

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.

and

SAMSUNG ELECTRONICS AMERICA, INC.,

Petitioners,

v.

SECURE WI-FI LLC,

Patent Owner.

Case IPR2024-01369
U.S. Patent No. 9,961,552

**PATENT OWNER'S
PRELIMINARY RESPONSE
UNDER 37 C.F.R. §42.107**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. The '552 patent presents a novel approach to securing wireless network connections, minimizing the risk of rogue attacks and protecting user privacy.	7
III. The Asserted References	9
A. <i>Vardi</i> embraces diminished security to create quicker and more efficient connections with non-authenticated access points.	9
B. Like <i>Vardi</i> , <i>IEEE802.11</i> does not disclose or suggest any fake MAC address or the claimed access point authentication.....	12
C. <i>Orava</i> teaches the use of a random MAC address for all data transmissions with an access point—including connection requests.	13
D. <i>Yun</i> describes two incompatible methods, neither of which teach or suggest transmitting an authentic device identifier in a connection request: first, a disparaged method and second a method that does not disclose an end device generating a fake MAC address or including any fake MAC address in a probe request.....	14
E. <i>Kholaiif</i> fails to cure the deficiencies of <i>Vardi-IEEE802.11-Orava-Yun</i>	16
IV. Institution should be denied because Petitioners have failed to demonstrate any reasonable likelihood of success on any challenged claim.....	17
A. <i>Vardi</i> , alone or in combination, fails to render obvious any challenged claim, rendering each ground meritless.	19
1. All grounds fail as Petitioners' proposed combination fails to teach or render obvious a "device" that determines whether an access point is an "authenticated"	

	access point, as required by all claims.....	21
2.	The proposed combination fails to render obvious how to determine whether an access point is “authenticated.”.....	28
B.	Petitioners cannot show that it would have been obvious to combine <i>Vardi-IEEE802.11</i> with <i>Orava</i> and/or <i>Yun</i> as proposed	29
1.	Petitioners cherry-pick portions of <i>Orava</i> and <i>Yun</i> , ignoring the references as a whole, including that both <i>Orava</i> and <i>Yun</i> disparage Petitioners’ proposed combination.....	32
2.	<i>Yun</i> teaches that its alleged fake MAC address cannot be used in the proposed combination with <i>Vardi</i>	39
3.	Petitioners rely on two discrete systems of <i>Yun</i> , without explaining how the systems could be combined.....	41
V.	Denial is warranted because Petitioners failed to provide any showing of the need, ranking, or explanation to justify the filing of two petitions.....	43
VI.	The Board should deny institution under <i>Fintiv</i>	43
A.	The Board need not address the merits of the Petition because the <i>Fintiv</i> factors favor denial.	45
1.	Factor 1 favors denial (likelihood of stay).....	45
2.	Factor 2 favors denial (timing of trial).....	46
3.	Factor 3 favors denial (investment in parallel proceedings).....	49
4.	Factor 4 favors denial (overlap of issues).....	51
5.	Factor 5 favors denial (overlapping parties).....	54
6.	Factor 6 favors denial because Petitioners have failed to present a compelling unpatentability challenge.....	54

VII. Conclusion	55
-----------------------	----

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Apcon, Inc. v. Gigamon Inc.</i> , IPR2020-01579 (P.T.A.B. Mar. 16, 2021)	55
<i>Apple Inc. v. Contentguard Holdings, Inc.</i> , IPR2015-00442 (P.T.A.B. July 13, 2015)	38
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019 (P.T.A.B. Mar. 20, 2020)	passim
<i>Aylo Freesites Ltd. v. Dish Techs. L.L.C.</i> , IPR2024-00941 (P.T.A.B. Nov. 21, 2024)	43
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015).....	38
<i>Bentley Motors Ltd., Jaguar Land Rover Ltd.</i> , IPR2019-01539 (P.T.A.B. Mar. 10, 2020)	46
<i>Code200, UAB v. Luminate Networks, Ltd.</i> , IPR2020-01506 (P.T.A.B. Feb. 16, 2021)	51, 52
<i>eClinicalWorks, LLC v. Decapolis LLC</i> , IPR2022-00229 (P.T.A.B. Apr. 13, 2022).....	47
<i>E-One, Inc. v. Oshkosh Corp.</i> , IPR2019-00161 (P.T.A.B. May 15, 2019).....	47
<i>F5 Networks, Inc. v. WSOU Investments, LLC</i> , IPR2022-00238 (P.T.A.B. May 19, 2022).....	45
<i>Immersion Sys. LLC v. Midas Green Techs., LLC</i> , PGR2021-00104 (P.T.A.B. Jan. 31, 2022)	46
<i>In re Beasley</i> , 117 Fed. Appx. 739 (Fed. Cir. 2004).....	37

<i>In re Gurley</i> , 27 F.3d 551 (Fed. Cir. 1994).....	27
<i>InTouch Techs., Inc. v. VGo Comm'cns, Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014).....	38
<i>KSR International Co. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007).....	38
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005 (P.T.A.B. May 2, 2022)	47, 54
<i>Panduit Corp. v. Dennison Mfg. Co.</i> , 810 F.2d 1561 (Fed. Cir. 1987).....	38
<i>Samsung Elecs. Co. v. Clear Imaging Research, LLC</i> , IPR2020-01401 (P.T.A.B. Feb. 17, 2021)	45, 54
<i>Samsung Elecs. Co., Ltd. v. Mojo Mobility Inc.</i> , IPR2023-01092 (P.T.A.B. Jan 8, 2024).....	46, 48
<i>Sand Revolution II, LLC v. Continental Intermodal Grp.</i> , IPR2019-01393 (P.T.A.B. June 16, 2020).....	49
<i>Teso LT UAB v. Luminati Networks Ltd.</i> , IPR2021-00122 (P.T.A.B. Apr. 20, 2021).....	52, 53
<i>U.S. Venture, Inc. v. Sunoco Partners Marketing & Terminals L.P.</i> , IPR2020-00728 (P.T.A.B. Oct. 1, 2020)	53
<i>Univ. of Strathclyde v. Clear-Vu Lighting LLC</i> , 17 F.4th 155 (Fed. Cir. 2021).....	37
<i>W.L. Gore & Associates, Inc. v. Garlock, Inc.</i> , 721 F.2d 1540 (Fed. Cir. 1983).....	37
<i>WesternGeco LLC v. ION Geophysical Corp.</i> , 889 F.3d 1308 (Fed. Cir. 2018).....	52
<i>Xerox Corp. v. Bytemark</i> , IPR2022-00624 (PTAB Feb. 10, 2023)	25

Statutes

35 U.S.C. § 314(a)	1, 43, 54
--------------------------	-----------

Regulations

37 C.F.R. § 42.24	43
-------------------------	----

Patent Owner's Exhibit List	
EX2001	Order Denying Defendants' Motion to Stay Pending <i>Inter Partes</i> Review, <i>Secure Wi-Fi LLC v. Samsung Electronics, Co., Ltd., et al.</i> , No. 2:24-cv-CV-0047-JRG, dated October 16, 2024
EX2002	Docket Control Order, <i>Secure Wi-Fi LLC v. Samsung Electronics, Co., Ltd., et al.</i> , No. 2:24-cv-CV-0047-JRG, dated June 14, 2024
EX2003	Cover pleading to Defendants' Preliminary Invalidity Contentions, <i>Secure Wi-Fi LLC v. Samsung Electronics, Co., Ltd., et al.</i> , No. 2:24-cv-CV-0047-JRG, served July 10, 2024
EX2004	Judicial Caseload Profile (June 30, 2024): Table C-5, <i>U.S. District Courts—Civil Federal Judicial Caseload Statistics</i> ; Table T-3, <i>U.S. District Courts—Median Time from Filings to Trial for Civil Cases in which Trials were Completed</i>
EX2005	Docket Navigator, Median Time-to-Trial Statistics for Judge Rodney Gilstrap, dated December 2024
EX2006	Cambridge Advanced Learner's Dictionary & Thesaurus, 4th Edition, 2013 (Excerpts)
EX2007	Merriam-Webster's Dictionary, merriam-webster.com (Excerpts)
EX2008	The Authoritative Dictionary of IEEE Standards Terms, 7th Edition, 2000 (Excerpts)
EX2009	Newton's Telecom Dictionary, 12th Edition, 1997 (Excerpts)
EX2010	Civil Docket Report for <i>Secure Wi-Fi LLC v. Samsung Electronics, Co., Ltd., et al.</i> , No. 2:24-cv-CV-0047-JRG

I. Introduction

The Board should deny institution of *inter partes* review of U.S. Patent No. 9,961,552 (“the ’552 patent”) because (1) Petitioners fail to demonstrate any reasonable likelihood that any challenged claim is obvious, (2) Petitioners filed two Petitions against the ’552 Patent, but failed to submit a ranking, let alone provide any explanation to justify the “rare circumstances” that would necessitate the filing of two parallel petitions, and (3) the § 314(a) factors strongly favor discretionary denial.

The ’552 patent claims novel technology to increase “security for Wi-Fi wireless access technologies.” EX1001, 1:27-28. In particular, a method performed by a device (challenged independent claims 10, 15, 21) or a system (challenged independent claim 24) uses a “fake” device identifier, such as a fake MAC address, when transmitting a probe request to an access point. An authentic device identifier is then transmitted as part of the connection request to the access point, but only after determining the access point is authenticated.

As the inventor recognized, in searching for a wireless access point with which to connect, an end device (e.g., a mobile device) may transmit probe requests to elicit responses from nearby access points. *Id.*, 3:4-39. The probe requests may be received by any number of access points near the end device. *Id.* And as probe requests traditionally included authentic device identifiers, sending probe requests

to unknown and possibly unscrupulous access points could expose location information to “devices to which the end device does not want to disclose the present location information.” *Id.* Thus, the inventor developed a novel and more secure method and device wherein a device uses a “fake” device identifier to include when broadcasting a probe request. *See, e.g.*, claims 10, 15, 21 and 24. After receiving a probe response from an access point, the device determines whether the access point is authenticated, including by determining that the access point is an access point included in the authenticated access point list that is received from the server. Only after determining that an access point is authenticated, will the end device request to connect to the authenticated access point by transmitting an authentic device identifier. Thus, the inventor disclosed and claimed a safer, more secure method of anonymously identifying and authenticating wireless access points while still allowing a device’s authentic identifier to be provided to facilitate the connection process. By using both a “fake” device identifier in the probe request and an “authentic” device identifier in the connection request, the ’552 patent balanced security and anonymity for identifying access points, while still maintaining the benefits of providing authentic identifying information of a device during the connection process.

Petitioners’ primary reference for all grounds, *Vardi*, is the antithesis of the ’552 patent. *Vardi* teaches a process of connecting to access points using “shortcuts”

to “expedite[s] wireless network and Internet access,” and ensures “the connection time [is] minimized”—all at the expense of security, which *Vardi* describes as “cumbersome.” EX1007, 1:67-2:1, 12:9-23, 46-49, 13:4-12, 11:28-30. *Vardi* recognized that a given location may include numerous access points, some with “mediocre service.” *Id.*, 1:55-61. Thus, *Vardi* proposed a server-centric system of compiling in a database “preferred access points” by relying on reporting by any number of other unknown users, including strangers and potentially unscrupulous individuals. *See id.*, 3:6-10. Based on this “knowledge base” of others, when a user enters an area, it may select and request access to an access point based on the information provided by others. *See id.*, 6:50-54; *see also id.*, 7:7-8 (using “historical data discovered by the user community.”). While this system may allow a device to “expedite” a wireless connection and quickly identify “preferred access points,” it does so at the expense of security, as the device uses the unconfirmed “knowledge base,” which could have been created using information from unscrupulous individuals seeking to cause users to connect to fictitious or malicious access points.

The stark differences of the problems and solutions identified in the ’552 patent and *Vardi* result in the Petition’s numerous failures. For example, in *Vardi*, the end device does not determine whether an access point is “authenticated,” as required by all challenged claims, and certainly not based in the manner claimed by the challenged claims. EX1001, 4:18-36. Quite the contrary, the purpose of *Vardi* is

to identify access points for which the end device has *not* previously connected to “reduce[] connection time” which “allows for seamless connection switching (and roaming) without centralized control.” EX1007, 12:13-23. And because *Vardi* teaches to rely on the “knowledge base” of others, the access point is not authenticated at all. No other reference cures these deficiencies of *Vardi*, and Petitioners offer no argument to the contrary. Pet., 52-53. Moreover, because *Vardi* is wholly unconcerned with security or location leaking—indeed, a key purpose is to *share* location information for the benefit of others—it does not teach or suggest any use of a “fake” MAC address at all.

Attempting to cure these deficiencies, Petitioners suggest combining *Vardi-IEEE802.11* with the *Orava* and *Yun* references in an attempt to utilize *Orava* and *Yun*’s alleged fake MAC address in *Vardi*’s knowledge base system. However, the combination of *Vardi* and *Orava* and/or *Yun* does not teach or suggest all elements of the claimed inventions. Moreover, considering *Orava* and *Yun*’s teachings in full, both references teach to include the alleged fake MAC address for **both** a probe request and an alleged connection request, and thus teach **not** to use an “authentic” device identifier for connection requests to the authenticated access point, as described and claimed in the ’552 patent. *Orava* teaches the use of a random MAC address for every data transmission, in lieu of the authentic or “fixed” MAC address, instructing that the “temporary MAC address can thus be used instead of a fixed

address in all protocol messages,” and indeed to protect anonymity, “it is not desirable to use the fixed MAC address permanently allocated to the MT at the manufacturing stage.” EX1005, ¶¶ 25, 49. Similarly in *Yun*, even assuming an alleged disclosure of using an arbitrary MAC address for a connection request in a local network, *Yun* nevertheless teaches that this technique is not applicable for networks that “require the use of [a] real MAC address.” EX1004, ¶¶ 149-150. *Yun* therefore teaches that to protect a real MAC address, a station’s real MAC address should only be transmitted to an access point after actual connection to the access point, via a secure method. EX1004, ¶ 157. Thus, both *Orava* and *Yun* teach to not use an authentic device identifier in a connection request, as required by all challenged claims.

Contrary to the law of obviousness, Petitioners are thus left to cherry-pick *Orava* and *Yun*’s alleged fake MAC address for the probe request. But because Petitioners impermissibly use the challenged claims as a roadmap, Petitioners then ignore *Orava* and *Yun*’s teachings and revert to using *Vardi*’s real MAC address for the connection request. There is no motivation to both adopt and reject *Orava* and *Yun*’s teachings to arrive at the proposed combination. Indeed, *Vardi* does not contemplate a fake MAC address at all, and if a POSITA were to modify *Vardi* to include *Orava* or *Yun*’s fake MAC address for the purpose of achieving MAC address anonymity, the POSITA would have done so just as these references

describe: using a fake MAC address in place of a real MAC address for both probe and connection requests. Thus, even if *Vardi* and *Orava* and/or *Yun* could have been combined, the combination that would have been reached by a POSITA would not have taught or suggested Petitioners' proposed combination, namely, using a "fake" device identifier for probe requests and then an "authentic" device identifier for connection requests as disclosed and claimed in the '552 patent.

These failures are discernable from the Petition itself and cannot be cured by expert testimony. Even if they could be cured (they cannot), Dr. Bims' declaration—made up principally of verbatim copying of attorney argument from the Petition—fails to add anything to the proceedings. Not one of Petitioners' grounds has any reasonable likelihood of success, failing to meet Petitioners' evidentiary burden at the outset. Institution should be denied.

But the Board need not consider the merits. Applying discretionary denial under *Fintiv*, the district court will make the same decisions to resolve the same disputes of the same parties months before any final written decision by the Board. Indeed, the underlying district court litigation involves the same issues, the same parties, the same challenged claims, and the same asserted art. There is extensive overlap, and institution would needlessly waste party and Board resources through duplicate, parallel proceedings that create the potential for inconsistent results. Moreover, even before the institution decision, the parties and the district court have

and will have expended substantial time and resources in the parallel litigation. Currently, fact discovery is well underway, the district court has already expended time and resources denying Samsung's motion to stay and the parties are about to commence claim construction. These activities have and will all occur well before the Board's institution decision in March 2025. Compounding the case for discretionary denial, the district court already denied Samsung's motion to stay the parallel proceeding. Efficiency and integrity of the system are best served by denying institution.

II. The '552 patent presents a novel approach to securing wireless network connections, minimizing the risk of rogue attacks and protecting user privacy.

The '552 patent is titled "Schemes for Connecting to Wireless Network." The '552 patent discloses and claims inventions for securing wireless connections in public or semi-public environments, enhancing user privacy, and mitigating unauthorized network access risks. The '552 patent is generally related to "security for Wi-Fi wireless access technologies." EX1001, 1:27-28.

In searching for and identifying nearby wireless access points, such as Wi-Fi access points, an end device may broadcast "probe requests" to elicit probe responses from nearby access points. *Id.*, 3:4-18. The probe requests may be received by any number of access points or other devices near the end device. *Id.* The inventor of the '552 patent recognized that sending probe requests containing authentic end

device identifiers that are available to all nearby devices, including those of unknown and possibly unscrupulous individuals, could expose location information to “devices in which the end device does not want to disclose the present location information.” *Id.*

Recognizing these concerns, the '552 patent introduced a method and system where an end device uses a “fake” device identifier, e.g., a randomized MAC address, to use when broadcasting probe requests. EX1001, 1:32-2:3. In this way, the inventions of the '552 patent may dynamically use fake identifiers to protect device anonymity until an access point is authenticated as trustworthy. For example, by separating the initial probe process, using fake identifiers, from the actual connection request, using real identifiers once the access point is determined to be authentic, the invention provides an additional layer of security during probe requests, the invention provides an additional layer of security during probe requests, while allowing an authentic device identifier to be used in attempting to connect to authenticated access points.

As an example, claim 10 recites “transmitting, to at least one access point, the probe request frame that includes the received fake device identifier,” “determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point,” and “transmitting, to the at least one

access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.” EX1001, claim 10.

The claimed inventions further use a robust mechanism of access point authentication before revealing sensitive device information. As claim 10 recites, for example, the device determines “whether the at least one access point is an authenticated access point” “based at least, in part, on the information regarding the at least one access point” in the probe response before transmitting “an authentic device identifier.” EX1001, claim 10. In this way, the systems and methods of the ’552 patent protect the real device identifier from being exposed during broadcasting probe requests, thereby enhancing user privacy and reducing the risk of unwanted tracking or unauthorized access, while balancing the security concerns by providing an authentic device identifier for connection requests once an authenticated access point has been identified. *Id.*

III. The Asserted References

A. *Vardi* embraces diminished security to create quicker and more efficient connections with non-authenticated access points.

Rather than seeking to augment device security through the ’552 patent’s hybrid approach of only providing an authentic device identifier after authenticating an access point, *Vardi* embraces reduced device security by relying on the information of other users in the name of speed and efficiency. Indeed, unlike the

'552 patent, *Vardi* has nothing to do with using a “fake” device identifier, e.g., a randomized MAC address, when broadcasting probe requests for security purposes or indeed, has no teaching or suggestion of a “fake” device identifier at all. EX1001, 1:32-2:3; EX1007.

Vardi recognizes that a device at any given time may be in communications distance with numerous access points, some with “mediocre service.” EX1007, 1:55-61. *Vardi* further recognizes that given the rise in the number of access points, many with poor performance, it was difficult to identify, obtain information about, and connect to access points in and around where the user was located. EX1007, 2:4-19, 23-29. *Vardi* therefore proposes a server-centric system of compiling in a database information for access points by relying on reporting by any number of other unknown users. *See id.*, 3:6-10; *see also id.*, Fig. 3 (User “Joe” reporting for a particular access point that “strength is good, uncluttered.”). Based on this “knowledge base,” when a user enters an area, it may select an access point based on the information provided by others. *See id.*, 6:50-54; *see also id.*, 7:7-8 (using “historical data discovered by the user community.”). By “exploit[ing] the radio resource database information” collected from “other clients” in “the user community” and “[s]haring centralized radio resource information with each client,” such that client devices receive “*information gathered by other clients* that was sent to the server,” *Vardi*’s process for connecting to access points “allows shortcuts,”

“expedite[s] wireless network and Internet access,” and ensures “the connection time [is] minimized.” EX1007, 12:9-23, 12:46-49, 13:4-12, 11:28-30.

While *Vardi*’s scheme may allow a device to “expedite” a wireless connection and quickly identify “preferred access points,” it does so at the expense of security, as the device uses the unauthenticated “knowledge base.” EX1007, 6:49-54. Particularly, *Vardi* fails to disclose any mechanism to evaluate the trustability of *any* user or user information and lacking any mechanism to track whether its “preferred” access points are malicious or are what they are reported to be by other users. *Vardi* does not disclose or contemplate these mechanisms because they would be counter to the entire purpose of *Vardi*: to use information of others to provide fast and efficient connections to access points.

Far from determining an access point is authenticated based at least in part on an indication of the end device’s previous connection to that access point, *Vardi* makes “selecting the proper AP more easy and efficient” by relying on the radio resource database comprised of the unverified ratings, rankings, experience and informative comments about APs by other users. EX1007, 16:2-27, 13:4-23. That is, *Vardi*’s mobile device selects an AP connection by preferentially relying on AP information collected from the “user community” and stored in its radio resource database, such as “an AP’s rating generated from various clients’ reports” and

“comments and other information provided by other users.” *Id.*, 16:9-27, 13:4-23, 11:28-30.

B. Like *Vardi*, IEEE802.11 does not disclose or suggest any fake MAC address or the claimed access point authentication.

802.11 is a standard published by the Institute of Electrical and Electronics Engineers (“IEEE”). The standard is created and maintained by a Standards Committee of the IEEE and approved by the IEEE-SA Standards Board. EX1008, 3. As recognized by the ’552 patent, the IEEE 802.11 standard generally provides a standardized method for conveying wireless communications. EX1001, 7:41-46. The standard was created by the “IEEE 802.11 Working Group,” comprised of hundreds of academic and industry professionals across the globe. *See* EX1009, 7-10.

Despite being the culmination of discussions and voting of hundreds of industry professionals, the version of IEEE 802.11 relied upon by Petitioners has the same failures as *Vardi* in that it does not teach or suggest a fake MAC address or performing the access point authentication of the ’552 patent, and Petitioners make no argument to the contrary. Indeed, secondary references, such as *Orava* and *Yun*, recognize that using a fake, and potentially non-unique MAC address, would cause standard non-compliance. EX1005, ¶ 3 (“according to IEEE 802.11 specifications, IEEE allocates an OUI identifier ... to each manufacturer, on the

basis of which identifier the manufacturer can determine MAC addresses for the devices”); EX1004, ¶ 149 (noting “[t]he requirement to use the real MAC address” for certain standards requirements, such as 3GPP).

C. *Orava* teaches the use of a random MAC address for all data transmissions with an access point—including connection requests.

Orava teaches not to reveal a device’s real, or “fixed” MAC address for *any transmission*. For example, *Orava* warns that “the fixed MAC addresses determined by manufacturers cause a security risk: a MAC address can be picked up from *every message* transferred over the air interface[.]” EX1005, ¶ 3 (emphasis added). And “[w]hen the MAC address of the device is known,” *Orava* explains, “the movements of the device can be followed, and its traffic can be deliberately disturbed by causing collisions with packets by using a ‘stolen’ MAC address.” *Id.* To solve these security problems, *Orava*’s method uses a random MAC address for every data transmission from the user terminal to protect the user’s anonymity. *Id.*, ¶¶ 25-26. *Orava* explains that “it is not desirable to use the fixed [authentic] MAC address permanently allocated to the MT [terminal device] at the manufacturing stage.” *Id.*, ¶ 25. Without explanation or rationale, however, the Petition selectively rejects these express security teachings of *Orava* to use the random MAC address for *every* data transmission; this relied upon reference in fact teaches away from the

inventive hybrid system of the '552 patent which transmits a real MAC address in its connection request.

Orava highlights the importance of using random MAC addresses to protect against “stolen” MAC addresses, which “can be picked up from every message transferred over the air interface,” for example, instructing to use random MAC addresses for all transmissions. *Id.*, ¶¶ 3, 8, 25-27, 49. *Orava* touts the desirability of using random MAC addresses for all transmissions and goes on to identify the problem of “collisions” which may occur when “two terminals might request for temporary MAC addresses substantially simultaneously” and both terminals use the MAC address transmitted through the broadcast address in lieu of their ‘real’ addresses. *Id.*; see also *id.* at ¶ 4. *Orava* therefore teaches a separate server that assigns and tracks random MAC addresses issued to devices to minimize collision risk. *Id.*, ¶¶ 3, 7-8, 25-27, Fig. 2.

D. *Yun* describes two incompatible methods, neither of which teach or suggest transmitting an authentic device identifier in a connection request: first, a disparaged method and second a method that does not disclose an end device generating a fake MAC address or including any fake MAC address in a probe request.

The Petition fails to recognize or address that it is relying upon two disparate and incompatible methods of *Yun* for its proposed modification of *Vardi-IEEE802.11*. *Yun* explicitly discloses that alleged end devices, “stations,” “are required to use their actual MAC address for communication with access points.”

EX1004, ¶ 143. *Yun* then offers two distinct methods as proposed exceptions to this rule. First, *Yun* describes a method titled “MAC address anonymity,” spanning paragraphs 143-152. *Yun* then describes a second method, titled “Dynamic address only for BSS,” spanning paragraphs 153-162.

The first “MAC address anonymity” method can only be used in a “local network.” EX1004, ¶ 144. Here, *Yun* discusses using “an arbitrary MAC address,” an “AMID.” *Id.* A station provides a “trial AMID” to an access point. EX1004, ¶ 146. If the AMID is unique within the local network, the access point responds, which confirms that the AMID may be used; if the AMID is not unique, the access point does not respond, and the station may try again with a different trial AMID. *Id.*, ¶¶ 146-147.

It is important to note that this method is limited to a “local network.” *Id.*, ¶ 144. *Yun* teaches that outside of a local network, “Stations(12) are required to use their actual MAC address for communication with the access point(14).” EX1004, ¶ 143. *Yun* discloses that only “[w]ithin a local network, the station(12) is not required to use its MAC address as identifier.” *Id.*, ¶ 144. As this disclosure of *Yun* is limited to a local network, an access point can determine whether the AMID is unique to the network and, if so, “send a probe response to confirm the validation of the AMID,” i.e., to confirm that the AMID is unique within the local network. *Yun*, however, describes numerous problems with this approach, including that it

fails to comply with standard requirements. *Id.*, ¶¶ 149-150. “[T]o solve the above-described problem,” *Yun* instead teaches to use its “present invention,” the “Dynamic address only for BSS” method. *Id.*, ¶ 151.

In the second “Dynamic address only for BSS” method, a station does not generate or transmit a fake MAC address in a probe request at all. Instead, a station transmits to an access point a request *for the access point* to send a fake MAC address to the station (e.g., a “MAC address *request* such as the probe request (‘Dynamic MAC address request’).” *Id.*, ¶ 156 (emphasis added). The access point then transmits an arbitrary MAC address to the station in response to the request to use for connection. *Id.* Only *after* connection, and once securely encrypted data may be transmitted, the station then provides “Real MAC Address” for use. *Id.*, ¶¶ 157-158.

For both methods, *Yun* teaches to not use an authentic device identifier in a connection *request*. The first method uses no authentic device identifier at all, and the second method teaches not to use any authentic device identifier until *after* any connection to the access point actually occurs.

E. *Kholaif* fails to cure the deficiencies of *Vardi-IEEE802.11-Orava-Yun*.

Petitioners attempt to add a fifth reference, *Kholaif*, to the *Vardi-IEEE802.11-Orava-Yun* combination only for ground 2 in an attempt to show

“mobile device components and corresponding claimed operations” and only for claims 24-28 which recite allegedly “well-known components.” Pet. 20, 78-90. Petitioners rely on *Kholaif* as allegedly disclosing a “mobile station,” “processor,” “WLAN communication interface,” “antenna,” “transmitter,” and “memory.” Pet., 89-93. However, *Kholaif* fails to account for the failures of *Vardi-IEEE802.11-Orava-Yun* detailed in this preliminary response, and Petitioners offer no argument to the contrary.

IV. Institution should be denied because Petitioners have failed to demonstrate any reasonable likelihood of success on any challenged claim.

Should the Board consider the merits, it should deny institution because Petitioners have failed to establish any reasonable likelihood of demonstrating any challenged claim is unpatentable. Petitioners fail to establish their proposed combination (even if proper), would have rendered obvious any challenged claim. Petitioners’ leading reference, *Vardi*, is missing multiple elements of the challenged claims because *Vardi* embraces location exposure and reduced security to serve the goal of “shortcuts” to “expedite wireless network and Internet access,” and ensure “the connection time [is] minimized.” EX1007, 12:9-23, 12:46-49, 13:4-12, 11:28-30.

Vardi fails to teach or suggest the requirements of claim elements 10[e], 15[e], 21[e], and 24[f], requiring a device to determine that an access point is an

“authenticated” access point. And it further fails to teach doing so based on information regarding the access point “is included in the authenticated access point list” (claims 10[e], 15[e], 21[e], 24[g]). Indeed, these claim requirements would have made no sense in the context of *Vardi*, as a key purpose of *Vardi* is to identify and connect to access points without the expense of authentication, allow[ing] for seamless connection switching (and roaming) ***without centralized control.***” See, e.g., EX1007, 2:23-29 (aiming to allow “users to *locate* and connect to the best access point at their desired location.”), 12:20-23 (“when the AP is already part of a radio resource database” steps in a standard system can be eliminated, “thereby substantially reducing the average connection time”). No secondary reference cures these deficiencies of *Vardi*, and Petitioners offer no argument to the contrary. Thus, every ground fails.

Vardi further fails to teach or suggest claim elements 10[b]/10[c], “receiving, from a server, a fake device identifier for the device” / “transmitting... the probe request frame that includes the received fake device identifier.” See also claim 15[b]/15[c] and claim 21[b]/21[c]. *Vardi* is far afield from the ’552 patented invention.

Seeking to cure these deficiencies, Petitioners attempt to modify *Vardi-IEEE802.11* in view of *Orava* and *Yun*. But even if a POSITA would have combined these two references with *Orava* and/or *Yun*, the combination would nevertheless

fail to render obvious the claimed inventions including elements 10[b, c, e], 15[b, c, e], 21[c, e], and 24[c, f, g]. Moreover, a POSITA would not have found it obvious to combine the references as proposed, especially in view of Petitioners' cherry-picking of portions of *Orava* and *Yun* when it suits them while ignoring other portions when they are fatal to the Petition.

The Petition fails to establish any reasonable likelihood that any challenged claim is unpatentable. Thus, the Board should deny institution.

A. *Vardi*, alone or in combination, fails to render obvious any challenged claim, rendering each ground meritless.

Vardi, the primary reference for each ground, fails to disclose or suggest at least two limitations of the independent claims. First, *Vardi* fails to teach or suggest the following elements:

1. “determining ... whether the at least one access point is an authenticated access point” Claims 10[e], 15[e], 21[e]; and
2. “a determination unit to determine ... whether the at least one access point is an authenticated access point” Claim 24[f]-[g].

Vardi does not teach determining that an access point is authenticated at all, much less in the manner claimed. While the Petition adds references *IEEE802.11*, *Orava*, *Yun*, and *Kholaiif* to grounds 1 and 2, these references do not cure *Vardi*'s

lack of disclosure or suggestion on these elements, and Petitioners offer no argument or analysis to the contrary.

Second, *Vardi* fails to teach or suggest the following elements:

1. “receiving, from the server, a fake device identifier for the device” and “transmitting, to at least one access point, the probe request frame that includes the received fake device identifier”
Claim 10[b]/[c];
2. “generating, a fake device identifier for the device” and
“transmitting, to at least one access point, a probe request frame that includes the fake device identifier” Claim 15[b]/[c];
3. “generating a collection that includes at least one of one or more random numbers or one or more random characters to prove a fake device identifier for the device” and “transmitting ... the probe request frame that includes the fake device identifier”
Claim 21[b]/[c]; and
4. “a transmitter to transmit, to at least one access point ... a probe request frame that includes a fake device identifier for a device”
Claim 24[c].

Indeed, *Vardi* does not teach receiving / generating or transmitting a fake MAC address at all, much less transmitting one in a probe request. Petitioners

attempt to cure these deficiencies of *Vardi* by adding *Orava* and *Yun*. However, *Orava* and *Yun* do not cure these failures, and Petitioners' proposed combinations only compound *Vardi*'s failures by presenting additional failures.

Accordingly, Petitioners' failure to demonstrate any disclosure or suggestion of these elements applies to all grounds. And all grounds fail.

1. All grounds fail as Petitioners' proposed combination fails to teach or render obvious a "device" that determines whether an access point is an "authenticated" access point, as required by all claims.

Each independent claim requires that the claimed "device" or a determination unit of a system determine whether an access point is an "authenticated" access point. Claims 10[e], 15[e], 21[e], 24[f]-[g]. Rather than describe what it means for an access point to be "authenticated" and whether that is disclosed within the proposed combination, Petitioners instead seek to equate *Vardi* with Petitioners' accused products in the underlying litigation, products which have vastly different functionality. Pet., 52.

Petitioners thus fail to address that authentication is the process of verifying the identity of an entity, using known, trusted, and verifiable information, before granting access to a resource. *See* EX2006, Cambridge Advanced Learner's Dictionary (2013 Ed.) (defining "authenticate" as "to prove that something is real, true or what people say it is"); *see also* EX2007, Merriam-Webster's Dictionary

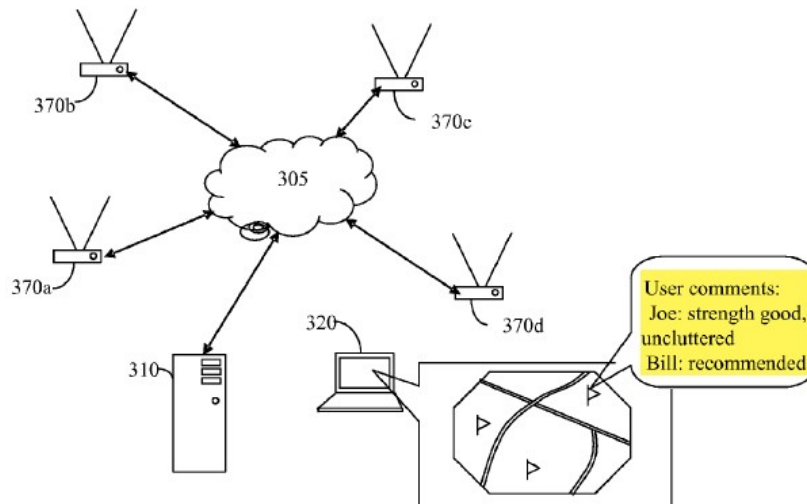
(defining “authenticate” as “to prove or serve to prove to be real, true, or genuine”); EX2008, The Authoritative Dictionary of IEEE Standards Terms (2000 Ed.) (defining “authentication” as “the process of validating a user or process to verify that the user or process is not counterfeit”); EX2009, Newton’s Telecom Dictionary (1997 Ed.) (defining “authentication” as “the process whereby a user or information source proves they are who they claim to be”). That is, “to prove that something is real, true, or what people say it is.” EX2006; *see also* EX2007-EX2009. Petitioners even ignore their own expert’s definition of “authentication,” and, to arrive at his conclusions of obviousness, so too does the expert. *See, e.g.*, EX1002, ¶ 55 (“to establish the identity of one station (STA) as a member of the set of STAs authorized to associate with another STA”) (quoting EX1009, 6.).

As discussed above, the ’552 patent teaches and claims methods and systems for enhancing the security of wireless networks, such as preventing spoofing attacks, protecting user data, and minimizing the risk of malicious targeting. For example, by verifying access points are *authenticated* before revealing an authentic device identifier, the ’552 patent teaches methods and systems that minimize providing authentic device information to unauthenticated access points. EX1001, claims 10, 15, 21, 24; 1:35-2:3. *Vardi*, by contrast, fails to disclose any authentication of an access point.

Vardi instead selects a “preferred AP” according to speed, ease and efficiency, prioritizing accumulated data from *other* users’ experience, comments and rankings, which is subsequently “distributed to user terminals (clients)” via a network server. EX1007, 16:12-22, 12:46-53, 13:4-23. The Petition identifies *Vardi*’s method “to determine whether the AP is a preferred AP” as allegedly disclosing or rendering obvious the required end device determining that the AP is an authenticated access point (Pet., 51-53). It is not. *Vardi*’s process for selecting “the most favorable access point for connection,” and likewise for “determin[ing] which APs are preferred for connection,” *id.*, 13:4-17, 14:52-57, are different both in kind and substance from the claims’ requirement that the end device determine that the access point is authenticated.

Particularly, Petitioners fail to show that *Vardi* would have rendered obvious the alleged end device determining whether an access point is an authenticated access point, i.e., verifying the identity of the access point, using known, trusted, and verifiable information. Pet. 51-53. *Vardi* instead proposes to connect using the alleged experience or comments of others, which are not verified and, indeed, may be provided by bad actors, including those seeking to trick a user into connecting to a malicious access point. EX1007, 16:9-22, Fig. 3. As the Cambridge Dictionary states, “authenticating” is proving “that something is real, true, or what people say it is.” EX2006. Indeed, the Authoritative Dictionary of IEEE Standards Terms

confirms “authentication” is “the process of validating a user” “to verify that the user ... is not counterfeit.” EX2008. In *Vardi*, the device simply relies on what people say it is, there is no proving or verifying it. *See, e.g.*, EX1007, Fig. 3.



Vardi likewise offers no mechanism to “establish the identity of one station (STA) as a member of the set of STAs authorized to associate with another STA” (EX1009, 6) before any alleged connection request. While IEEE802.11 does include an “Open System Authentication Request” and Response, Petitioners and their expert do not rely on this for this claim limitation, and instead rely on this as part of the alleged “connection request.” EX1003, ¶ 216.

By attempting to compare *Vardi* with their own accused products in the district court litigation, Petitioners also ignore the purpose of *Vardi* and incorrectly argue that *Vardi*’s radio resource database is “the claimed ‘authenticated access point list’ in memory.” Pet., 52-53. This statement is incorrect. To support it,

Petitioners cite only to their expert’s declaration at paragraphs 414-447. Pet. 53. However, Petitioners’ expert offers nothing more than circular reasoning which parrots the Petition—making a first conclusory assertion that *Vardi*’s preferred AP is the claimed “authenticated access point” (EX1002, ¶ 414), though *Vardi* merely selects an AP as a “favorite if it is part of radio resource database,” and that radio resource database is comprised of unverified user reports, none of which were “authenticated.” EX1007, 13:9-14, 6:50-54, 7:7-8. Dr. Bims takes this false premise and uses it to then conclude that the radio resource database of access point information distributed to client devices is the claimed “authenticated access point list,” though again, *none* of the APs comprising the radio resource database of *Vardi* have been *authenticated*. *Id.*; EX1002, ¶ 414. As such, there is no support for this assertion. *See Xerox Corp. v. Bytemark*, IPR2022-00624, Paper 12, at 2 (PTAB Feb. 10, 2023) (Director review designating institutional denial decision as precedential, where institution was denied when declaration merely parroted petition, “was conclusory and added little to the assertions the testimony was offered to support.”).

Indeed, Dr. Bims’ conclusions are incorrect, as *Vardi*’s preferred APs, its radio resource information database, and its “list of previously successfully used access points” all refer to access point information accumulated from numerous users and distributed—the whole purpose of *Vardi*. *See* EX1007, 12:33-13:26. As *Vardi* explains, “clients send connection reports” to a server and, after accumulating

the information from the numerous clients, “the server sends ... information to each client, relating to all APs in the vicinity of the client. In this manner, the mobile device can have ... information of APs to which *the mobile device was not connected before*[,] “allow[ing] for seamless switching (and roaming) *without centralized control*.” EX1007, 12:33-43, 12:9-23.

Thus, *Vardi*’s alleged end device does not connect to an access point by comparing AP information to a list of APs which have been authenticated. At best *Vardi*’s device utilizes a list of access points provided by the user community and connects to an access point based on that information. And, as the information provided by other unknown users is not proven to be what others say it is, the alleged end device makes no authentication determination, as required by the challenged claims. Rather than enhance security as taught in the ’552 patent, *Vardi* makes clear that its preferred APs are part of a “radio resource database,” with APs collected from other clients’ reports—which can of course include the same bad actors that the claimed inventions exclude. EX1007, 8:44-59; 12:46-49, 3:4-10.

While the Petition notes in passing that *Vardi* discloses a “cache memory” that stores “previously-connected APs,” Petitioners do not analyze that disclosure of *Vardi*. Pet., 27, 53. In fact, *Vardi* characterizes such a cache as “prior art,” and teaches *not* to use such a cache. EX1007, 12:24-39. Instead of using the cache, *Vardi*, unsurprisingly, teaches to upload the information to the server for accumulation with

information from other users, thus allowing the device to instead receive the accumulated information from the entire user community. *Id.*, 12:24-39. Indeed, *Vardi* boasts that its system does “enable fast connection,” i.e., by selecting the most favorable access point for connection from a “radio resource database” based on other users’ reporting, which has been “accumulated and processed at the network server” and then “distributed to user terminals (clients),” so that “the mobile device can have cache information of APs to which the mobile device ***was not connected before.***” *Id.*; see also *id.*, 12:24-49; *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994) (“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, ... ***would be led in a direction divergent from the path that was taken by the applicant.***”) (emphasis added). Thus, *Vardi* teaches away from the use of the described “prior art” “cache memory.”

The ’552 patent and *Vardi* operate differently. The ’552 patent teaches secure wireless network connections by “determining ... whether the at least one access point is an authenticated access point,” before revealing any “authentic device identifier” (see, e.g., claim 10). *Vardi* pools reports of access points from myriad users’ devices and its server sends that pooled data out to the entire user community in an attempt to ensure a speedy, easy and efficient connection, at the expense of security, with no mechanism to prove or verify that the access point information is what another says it is. *Vardi* fails to teach or suggest proving that an access point is

what the other unverified, untrusted users say it is (i.e., that it is an authenticated access point).

No secondary reference—*IEEE802.11*, *Orava*, *Yun*, or *Kholaiif*—cures these deficiencies of *Vardi*, and Petitioners offer no argument to the contrary. Thus, the Petition fails.

2. The proposed combination fails to render obvious how to determine whether an access point is “authenticated.”

In addition to failing to disclose “determining ... whether the at least one access point is an authenticated access point,” *Vardi* also fails to disclose how such authentication is determined as claimed: “based at least, in part, on the information” received in the probe response frame that indicates that “the at least one access point is included in the authenticated access point list that is received from the server.” Claims 10[e], 15[e], 21[e], and 24[f]-[g]. As discussed above, *Vardi*’s system, at best, accumulates and stores information provided by the user community using distinct. As there is no disclosure of any authentication of an access point in *Vardi*, there is no disclosure of such authentication being based at least in part on the information in the probe response frame that indicates that “the at least one access point is included in the authenticated access point list that is received from the server,” as recited in claims 10, 15, 21 and 24. Indeed, the whole purpose of *Vardi*

is to identify access points by relying on unauthenticated information of others, not based on any inclusion in a received list of access points that are authenticated.

No secondary reference cures these deficiencies of *Vardi*, and Petitioners offer no argument to the contrary. Thus, the Petition fails.

B. Petitioners cannot show that it would have been obvious to combine *Vardi-IEEE802.11* with *Orava* and/or *Yun* as proposed

Attempting to cure the failures of *Vardi-IEEE802.11*, Petitioners propose to add *Orava* and *Yun* to the combination. Pet., 24-86 (ground 1), 87-95 (ground 2). But adding either *Orava* or *Yun* (or both) would not cure any of the deficiencies described in Section IV.A, above. Neither *Orava* nor *Yun* teaches or suggests determining that an access point is “authenticated” or doing so by any of the claimed methods, and Petitioners offer no argument to the contrary. Pet., 52-53, 69, 75, 81-82. Accordingly, the combination of *Vardi-IEEE802.11* and *Orava* and/or *Yun* (with or without *Kholaiif*) does not cure *Vardi*’s deficiencies described above.

Even if a combination of *Vardi-IEEE802.11* with *Orava* and/or *Yun* taught all claimed elements (it does not), it would not have been obvious to combine *Vardi-IEEE802.11* with *Orava* or *Yun* as Petitioners propose. First, it is not proper for Petitioners to rely on two discrete and incompatible methods of *Yun* without explanation. Moreover, as demonstrated below, both *Orava* and *Yun* teach *not* to transmit an authentic MAC address as part of the connection request, as required by

Claims 10[e], 15[e], 21[e], 24[f]-[g]. *Orava* teaches the use of a random MAC address for every transmission, including the connection request, for example, instructing a method in which “instead of using a fixed MAC address, the method according to FIG. 2 is performed each time when setting up a data transmission connection from the MT to another terminal or an access point AP.” EX1005, ¶ 25; Fig. 2. Similarly, *Yun* uses a fake MAC address for the connection request and, contrary to the inventions of the ’552 Patent, *Yun* teaches sending an authentic device identifier only *after* an actual connection to the access point occurs, if at all. Petitioners are thus left to improperly cherry pick some disclosures of *Orava* and *Yun* while ignoring others. These deficiencies, among others, mean it would not have been obvious to combine *Vardi-IEEE802.11* with *Orava* or *Yun* as Petitioners propose.

As introduced above, the ’552 patent discloses a hybrid approach, allowing for security while ensuring successful connections with wireless access points. First, the patent describes transmitting a probe request that includes a fake MAC address. EX1001, 12:1-2 (claim 10[c]), 12:51-52 (claim 15[c]), 13:44-46 (claim 21[c]), 14:17-23 (claim 24[c]); *see also* Pet., 40-46 (discussing claim 10[c]). As the ’552 patent describes, broadcasting a fake MAC address distinct from the actual MAC address during the probe request, which is available to all nearby devices, increases security by preventing unauthenticated and malicious devices from receiving a

device's authentic device identifier, which would allow other devices to e.g., know and track the location of the end device. Second, the '552 patent describes transmitting a connection request to authenticated access points that includes not the fake MAC address, but an authentic device identifier for the device. EX1001, 12:17-20 (claim 10[e]), 13:4-7 (claim 15[e]), 14:1-4 (claim 21[e]), 14:45-49 (claim 24[h]); *see also* Pet., 51-53 (discussing claim 10[e]). This allows the access point to determine the end device's identity to, e.g., decide whether to connect to the device and/or enforce any rules or apply any functionality specific to that device.

For grounds 1 and 2, Petitioners propose to combine *Vardi-IEEE802.11* with *Orava* and *Yun* to arrive at the hybrid approach of the '552 patent. Pet., 24-92 Pet. 40 (discussing element 10[c]), Pet. 56-57 (element 10[f]); *see also* Pet., 67, 70 74, 75, 78, 82 (incorporating claim 10[c/f] analysis for claims 15[c/f], 21[c/f], and 24[c/h]). As described above, *Vardi* is wholly unconcerned with security, and indeed neither *IEEE802.11* nor *Vardi* includes any disclosure or suggestion of a fake MAC address, a fact that Petitioners cannot and do not dispute. *See* Pet., 35-40. As such, Petitioners must rely on *Orava* and/or *Yun* as allegedly disclosing a fake MAC address. *See, e.g.*, Pet., 16 (“Orava-Yun provides the random MAC address generation functionality to minimize location tracking in the Vardi communication system and method”). Petitioners propose “Configuring *Vardi*'s wireless system to substitute the ‘real’ MAC address for *Orava*'s temporary MAC address” in view of

Orava. Id., 15. The problem for the Petition, however, is that merely substituting *Orava*'s "temporary" or random MAC address would not result in the proposed hybrid combination; nor would it have been obvious. What Petitioners fail to acknowledge in their proposed combination is that *Orava* teaches "[t]he temporary MAC address can thus be used instead of a fixed address in all protocol messages." EX1005, ¶ 49. *Orava* expressly uses a random MAC address in the connection request, and explains that to maintain anonymity, "it is not desirable to use the fixed MAC address permanently allocated to the MT at the manufacturing stage." *Id.*, ¶¶ 25, 49, Figs. 2, 7. Likewise, the Petition seeks to combine *Vardi* in view of *Orava* and *Yun*, because *Yun*'s "transmitted packet on air uses an arbitrary MAC address, but Petitioners neglect to mention that *Yun* teaches **not** to use the "real MAC address" in a connection request contrary to their proposed combination.

1. Petitioners cherry-pick portions of *Orava* and *Yun*, ignoring the references as a whole, including that both *Orava* and *Yun* disparage Petitioners' proposed combination.

Neither *Orava* nor *Yun* ever teach to transmit a connection request that includes an authentic device identifier, as proposed in Petitioners' combination. Indeed, as described above, *Orava* expressly warns of the "security risk" caused by "the fixed MAC addresses determined by manufacturers": "a MAC address can be picked up from **every message** transferred over the air interface," allowing the authentic MAC address to be "stolen." EX1005, ¶ 3 (emphasis added). To solve this

security problem, *Orava* teaches the use of a random MAC address instead of the fixed or authentic MAC address. *Id.* at ¶¶ 3, 24-25, 49 (“[t]he temporary MAC address can thus be used instead of a fixed address in all protocol messages”). *Orava* does not use an authentic device identifier in *any* transmission, instead making clear that to maintain anonymity, “it is not desirable to use the fixed [authentic] MAC address permanently allocated to the MT [terminal device] at the manufacturing stage.” *Id.*

Likewise, in *Yun*’s first method, the “MAC address anonymity” method, teaches not to use an authentic device identifier at all. *Yun* instead discloses using an AMID (or EMID, both an “arbitrary MAC address”) “instead of the fixed MAC address.” EX1004, ¶¶144-146; *see also* Section III.D.

For the second, “Dynamic address only for BSS” method, *Yun* teaches not to transmit a “real MAC address” as part of the connection request. *See* Section III.D. Instead, *Yun* teaches that the real MAC address should not be sent until *after* “the station(12) is connected with the access point.” EX1004, ¶ 157. Here, *Yun* goes on to explain why it discloses to wait until after connection with the access point to provide the “real MAC address for the station”—because it can then do so using encryption, and thus not leak the real MAC address during any connection request. *Id.*, ¶ 158.

This reasoning is echoed by Petitioners' expert, Dr. Bims. For example, Dr. Bims recognizes *Yun*'s use of arbitrary MAC addresses prevents "third party attackers or unauthorized third parties from compiling a list of SSIDs and private location information based on previously used hotspots ... *Yun* teaches 'MAC address anonymity makes an identity of the station not presumed through the MAC address.'" EX1002, ¶ 114-115. Likewise, Dr. Bims acknowledges the "security risk" that *Orava* seeks to solve by generating and using fake MAC addresses in data transmissions, i.e., that "a MAC address can be picked up from every message transferred over the air interface." *Id.*, ¶¶ 109-110 (citing EX1005, ¶¶ 3-4, 29). Dr. Bims acknowledges that *Orava* uses temporary random MAC addresses "to arrange anonymity," and likewise *Yun*'s solution "prevent[s] MAC address disclosure and identification of the mobile device by devices receiving the probe request frame," and that both "*Orava* and *Yun* provide security control management to protect the mobile device's 'real' MAC address." *Id.*, ¶¶ 88-89, 110. Dr. Bims then draws the conclusion that in view of *Orava*, "a POSITA would have found it obvious to swap *Vardi*'s 'real' MAC address for *Orava*'s randomly generated Fake ID," and "a POSITA would have found it obvious to combine *Vardi*, *Orava* and *Yun* to transmit[] the received MAC address (*Orava*) in the probe request frame." *Id.*, ¶¶ 196, 204. But *Orava* teaches to use the fake ID for all data transmissions and warns of the "security risk" of using the real MAC address for all transmissions.

EX1005, ¶¶ 3 (“the fixed MAC addresses determined by manufacturers cause a security risk: a MAC address can be picked up from every message transferred over the air interface”), 25 (“the method according to Fig. 2 is performed each time when setting up a data transmission connection from the MT to another terminal or an access point AP”), 49 (“[t]he temporary MAC address can thus be used instead of a fixed address in all protocol messages”). Similarly, both of *Yun*’s methods make clear that a real MAC address should not be provided as part of a connection request, and instead provided after actual connection to the access point occurs. *Yun* provides the technical reasons why it does so. EX1004, ¶¶ 143-144, 157-158; *see* Section III.D., *supra*. These reasons are contrary to Petitioners’ proposed combination.

Petitioners offer no reason why a POSITA would modify *Vardi-IEEE802.11* in view of *Orava* or *Yun* to arrive at the proposed hybrid approach of the ’552 patent, including the end device generating a fake device identifier for use in probe requests and using an authentic device identifier in connection requests after verifying that the access point is authentic.

Petitioners’ motivation to combine theory hinges on unexplained cherry-picking from *Orava* and *Yun* to modify *some steps* of *Vardi*’s process, but then inexplicably ignoring both *Orava* and *Yun* where the references teach away from the proposed combination and approach of the ’552 patent. Specifically, the Petition alleges that a POSITA, desiring to improve security and privacy of IEEE 802.11

standard communications, would have been motivated **to follow** *Orava* and *Yun*’s teaching about the use of a generated random MAC address and a dynamic MAC address, rather than reveal authentic device identifiers. Pet., 35-40. However, Petitioners selectively apply this rationale only when attempting to meet claim limitations 10[b]-[c] / 15[b]-[c], 21[b]-[c] and 24[c]. Pet., 35-46; *see also id.*, 65-70, 74, 78 (incorporating 10[b]-[c] arguments for 15[b]-[c], 21[b]-[c] and 24[c]). By contrast, in their strained effort to meet *other* claim limitations, Petitioners inherently argue that a POSITA would **disregard** both *Orava* and *Yun*, which both teach *to avoid* transmitting the real MAC address *until after connection*. Pet., 53-60 (10[f]); *see also id.*, 69-70, 75, 82-83 (incorporating 10[f] for 15[f], 21[f] and 24[h]).

Without the benefit of using the claimed inventions of the ’552 patent as a guide, there is no reason why a POSITA would have arrived at the proposed combination by *sometimes* heeding *Orava*’s warnings about the security risk posed by using a real address: that a “MAC address can be picked up from every message transferred over the air interface” and “stolen,” nor any reason why a POSITA would have heeded *some* of *Yun*’s advice for “improving security and privacy,” but, without explanation, rejected the reference’s “secure method” of protecting the device’s real MAC address from disclosure until after connection. Neither hindsight, nor recasting the results of the inventive process as a motivation to combine, can operate to invalidate patent claims. “[T]he inventor’s own path itself never leads to a

conclusion of obviousness; that is hindsight.” *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 165 (Fed. Cir. 2021).

The claimed invention is not to be “used as a frame” on which “individual naked parts of separate prior art references were employed as a mosaic to recreate a facsimile of the claimed invention.” *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1552-53 (Fed. Cir. 1983) (“To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.”).

The main guardrail against hindsight in obviousness analysis is the requirement of showing a motivation, discussed or taught in the prior art references, to combine what is known from there. “Given the ‘subtle but powerful attraction of a hindsight-based obviousness analysis,’ [the Federal Circuit] require[s] a ‘rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references.’” *In re Beasley*, 117 Fed. Appx. 739, 743 (Fed. Cir. 2004). Because “claimed discoveries almost necessarily will be combinations of what, in some sense, is already known,” finding obviousness based on a combination of references requires “a reason that would have prompted a person of ordinary skill in the art to combine the elements.” *KSR International Co. v. Teleflex*,

Inc., 550 U.S. 398, 401 (2007); *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only could have made but would have been motivated to make the combinations or modifications of prior art to arrive at the claimed invention.”).

Because Petitioners bear the burden of proof on motivation to arrive at their proposed combination and they offer no rationale for a POSITA to cherry-pick some security teachings from *Orava* and *Yun*, while ignoring others, there is no merit and no reasonable likelihood of success in the Petition. *See, e.g., In re Enhanced Sec.*, 739 F.3d at 1355 (holding that it is insufficient to satisfy 103 by selecting “bits and pieces” from references in an attempt “to stitch together an obviousness finding from discrete portions of prior art references without considering the references as a whole.”) (discussing *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1582 (Fed. Cir. 1987)); *InTouch Techs., Inc. v. VGo Comm’ns, Inc.*, 751 F.3d 1327, 1349 (Fed. Cir. 2014) (It is improper to combine references “like separate pieces of a simple jigsaw puzzle” without “explain[ing] what reason or motivation one of ordinary skill in the art at the time of the invention would have had to place these pieces *together*.”); *Apple Inc. v. Contentguard Holdings, Inc.*, IPR2015-00442, Paper 9 at 11-12, 17 (P.T.A.B. July 13, 2015) (“analysis infected with impermissible hindsight cannot form the basis of an obviousness finding”).

2. *Yun* teaches that its alleged fake MAC address cannot be used in the proposed combination with *Vardi*.

Even if Petitioners' cherry-picking were appropriate under the law of obviousness, it nevertheless would not have been obvious to combine *Vardi-IEEE802.11-Orava* with either of *Yun*'s methods. Petitioners propose to "combine *Vardi*, *Orava*, and *Yun* to transmit the received MAC address (Orava) in the probe request message (*Vardi*/IEEE802.11)," to apply "Orava's randomly generated Fake ID and *Yun*'s anonymous probe request transmission" Pet., 11, 38-39. However, *Yun* teaches that "Stations(12) are required to use their actual MAC address for communication with the access point," absent two exceptions that cannot apply within *Vardi*'s system.

As discussed in Section III.D, the first exception is that an arbitrary MAC address may be used within a local network. For the first exception, *Yun* discloses that only "[w]ithin a local network, the station(12) is not required to use its MAC address as identifier." *Id.*, ¶ 144. As this disclosure of *Yun* is limited to a local network, an access point can determine whether the AMID is unique to the network and, if so, "send a probe response to confirm the validation of the AMID," which confirms that the AMID is unique within the local network and can be used for communications on the network without interfering with communications of other stations.

Vardi's system, however, is not for use in a local network. *Vardi* teaches mapping all access points near the devices of multiple users. EX1007, Abstract, 1:19-21. Indeed, *Vardi* teaches that devices may utilize “[v]arious broadband wireless services” in various places including homes, public establishments, airports, etc. *Id.*, 1:23-29. *Vardi* proposes to “map” access points for all these networks “allowing users to locate and connect to the best access point at their desired location.” *Id.* 2:23-26. To make this mapping, *Vardi* discloses that clients of various users “detect[] the APs in reach,” and “report to a server” information of the APs. *Id.*, 18:24-28. Thus, *Vardi*'s system is not limited to a “local” network. The purpose of *Vardi* is having its clients connect to all available and numerous networks in a given area, rather than a single local network. And *Yun* counsels that in these scenarios, “[s]tatements(12) are required to use their actual MAC address for communication with access point(14).” EX1004, ¶ 143. It would thus not have been obvious to use *Yun*'s “arbitrary MAC address” in *Vardi*'s system because *Yun* discloses that it could not have been done.

The second exception in *Yun* is the “Dynamic address only for BSS” method where an access point provides an arbitrary MAC address to the station. EX1004, ¶ 156. This method could not be used in *Vardi*'s system either. The purpose of *Vardi* is for the client to connect to unknown, unmapped, and uncontrolled access points throughout numerous geographical regions. *See, e.g.*, EX1007, 12:33-53. It

would not be feasible, or even possible, to modify each of these access points so that they could provide arbitrary MAC addresses to devices. Indeed, if a person implementing *Vardi*'s system could access all access points to modify them, there would be no need for *Vardi*'s system to map or gather information for the access points. More importantly, the Petition fails to present any theory of how *Vardi* could be modified to implement this functionality of *Yun*.

3. Petitioners rely on two discrete systems of *Yun*, without explaining how the systems could be combined.

As yet another obviousness failure, without any recognition or explanation, Petitioners rely on two distinct systems and methods of *Yun* without explaining how the separate embodiments could be combined or how the combination of the systems could be fit into *Vardi*. Petitioners rely on *Yun* at paragraphs 146 and 156 as allegedly teaching transmitting a fake MAC address in a probe request. Pet., 9, 38. But these disclosures are from two distinct and incompatible systems. The first system is titled "MAC address anonymity," spanning paragraphs 143-152, directed only to local networks. The second is titled "Dynamic address only for BSS," spanning paragraphs 153-162, and directed to solving problems of *Yun*'s first system when not operating in a local network. *See* Section III.D.

As described Section III.D, the "MAC address anonymity" disclosure teaches to use "an arbitrary MAC address." A station includes a "trial AMID" to an

access point. EX1004, ¶ 146. If the AMID is unique within the local network, the access point responds; if the AMID is not unique, the access point does not respond. *Id.*, ¶¶ 146-147.

In the “Dynamic address only for BSS” disclosure, a station transmits a “MAC address request such as the probe request (‘Dynamic MAC address request’)” to an access point. *Id.*, ¶ 156. The access point then transmits an arbitrary MAC address to the station in response to the request to use for connection. *Id.* After connection, and once securely encrypted data may be transmitted, the station then provides “Real MAC Address” for use. *Id.*, ¶¶ 157-158.

Petitioners fail to explain how these two separate systems can be combined and then inserted into *Vardi*’s system. Indeed, as discussed in Section IV.B.3, it would not have been obvious to include either embodiment in *Vardi*, much less some unexplained combination of *Yun*’s embodiments. Even if the two methods could be somehow combined in some way (that is unexplained), any possible combination would fail, as *Yun* teaches in both methods to **not** provide an authentic MAC address in a connection request, as required by the ’552 patent.

In sum, Petitioners failed to show that *Vardi*’s system can be properly combined with either *Orava* or *Yun*. The Board should thus deny institution.

V. Denial is warranted because Petitioners failed to provide any showing of the need, ranking, or explanation to justify the filing of two petitions.

The Board should exercise its discretion to deny institution because Petitioners filed two parallel petitions challenging the same patent, without attempting to make the required showing to justify the “rare” instance where two petitions could possibly be needed. *See* Patent Trial and Appeal Board Consolidated Trial Practice Guide at 59 (Nov. 2019); *see also Aylo Freesites Ltd. v. Dish Techs. L.L.C.*, IPR2024-00941, Paper 12 at 10-11 (P.T.A.B. Nov. 21, 2024). Petitioners ignored the Trial Practice Guide’s demand to identify (1) a ranking of the petitions, and further failed to provide the Trial Practice Guide’s required (2) “explanation of the differences between the petitions, why the issues addressed by the differences are material, and why the Board should exercise its discretion to institute additional petitions if it identifies one petition that satisfies petitioner’s burden under 35 U.S.C. § 314(a).” Consolidated Trial Practice Guide at 59-60. Instead, Petitioners merely split the challenged claims between the two parallel petitions, blatantly defying the word limits set by 37 C.F.R. § 42.24, but never providing any justification for their two petitions.

VI. The Board should deny institution under *Fintiv*

The Board should exercise its discretion to deny institution under § 314(a). To do so, the Board balances six factors:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the Petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board's exercise of discretion, including the merits.

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 at 5-6 (P.T.A.B. Mar. 20, 2020).

“These factors relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Id.* In evaluating these factors, the Board takes “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *Id.*

In addition, the USPTO Director issued an “Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court

Litigation” (“Interim *Fintiv* Procedure”) dated June 21, 2022, which is addressed below with respect to *Fintiv* factors 2 and 4.

A balance of the *Fintiv* factors warrants denial of institution.

A. The Board need not address the merits of the Petition because the *Fintiv* factors favor denial.

1. Factor 1 favors denial (likelihood of stay)

Factor 1—which considers whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted—favors denial of institution.

Petitioners’ request for a stay in the district court litigation has been denied. EX2001. The district “court’s denial of the motion to stay weights in favor of exercising authority to deny institution.” *F5 Networks, Inc. v. WSOU Investments, LLC*, IPR2022-00238, Paper 33 at 7 (P.T.A.B. May 19, 2022) (citing *Fintiv*, Paper 11 at 6-7). Indeed, the Board finds that factor 1 weighs in favor of exercising discretion to deny institution, even where a district court’s order denying a motion to stay permits the movant to renew its motion “should the PTAB issue a decision on institution or a final determination as to the validity of the asserted claims.” *See, e.g., Samsung Elecs. Co Ltd v. Clear Imaging Research*, IPR2020-01401, Paper 12 at 11 (P.T.A.B. Feb. 17, 2021) (denying institution, finding factor 1 favors denial following Judge Gilstrap’s denial of Samsung’s motion to stay).

Any stay, even if Samsung’s request is renewed, is also unlikely due to the significant case progression (discussed in factor 3) and scheduled jury trial preceding

any final written decision (discussed in factor 2). The first *Fintiv* factor therefore supports denying institution.

2. Factor 2 favors denial (timing of trial)

Fintiv factor 2 weighs in favor of denying institution because the district court is set to complete trial on November 3, 2025, nearly five months before the Board’s final decision would be due, on March 25, 2026. (EX2002). “If the court’s trial date is earlier than the projected statutory deadline, the Board generally has weighed this fact in favor of exercising authority to deny institution under *NHK*.” *Fintiv*, IPR2020-00019, Paper 11 at 9.

This timeline undisputedly favors denial, as the Board has previously held that a trial date which precedes a final written decision deadline by five, four and even one-to-two months favors discretionary denial. *See, e.g., Samsung Elecs. Co., Ltd. v. Mojo Mobility Inc.*, IPR2023-01092, Paper 11 at 11 (P.T.A.B. Jan 8, 2024) (denying institution, finding trial date, “about five months before the projected statutory deadline” favored discretion to deny); *Bentley Motors Ltd., Jaguar Land Rover Ltd.*, IPR2019-01539, Paper 9 at 14 (P.T.A.B. Mar. 10, 2020) (denying institution where trial set to occur five months before final written decision); *Immersion Sys. LLC v. Midas Green Techs., LLC*, PGR2021-00104, Paper 15 at 11 (P.T.A.B. Jan. 31, 2022) (jury trial four months prior favored discretionary denial); *see also, NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00552, Paper 18 at 8-9 (P.T.A.B.

May 2, 2022) (finding two-month period between trial date and deadline for final decision weighed in favor of discretionary denial); *E-One, Inc. v. Oshkosh Corp.*, IPR2019-00161, Paper 16 at 6-9 (P.T.A.B. May 15, 2019) (finding one-month period between trial date and deadline for final written decision weighed in favor of discretionary denial); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12-13 (P.T.A.B. May 13, 2020) (factor disfavors institution when “the currently scheduled District Court trial is scheduled to begin two months before our deadline to reach a final decision”); *eClinicalWorks, LLC v. Decapolis LLC*, IPR2022-00229, Paper 10 at 9 (P.T.A.B. Apr. 13, 2022) (determining denial favored where beginning of jury trial was “roughly one to two months” before final decision was due).

Additionally, the USPTO’s Interim *Fintiv* Procedure provides that the “[p]arties may present evidence regarding the most recent statistics on median time-to-trial for civil actions in the district court in which the parallel litigation resides for the PTAB’s consideration ... the PTAB will also consider additional supporting factors, such as the speed and availability of other case dispositions.” *See* Interim *Fintiv* Procedure, 8-9. Here, the median time-to-trial is 21.6 months and the median time from filing to case disposition in the Eastern District of Texas is 7.6 months. EX2004, Judicial Caseload Profile, Table T-3 at 2, Table C-5 at 2 (June 2024). Considering the 7.6-month median time for disposition in the Eastern District of

Texas, the parallel litigation will likely be disposed of in early 2025, over a year before the March 2026 statutory deadline for the final decision. *Id.*, Table C-5 at 2; *see also* EX2010 (showing January 2024 complaint filing). Moreover, the median time-to-trial statistics for the district predict a trial date of October 2025 (EX2004), and for Judge Gilstrap in particular, the trial would be six to eight months prior to the institution date, in July or September 2025 (EX2005) (showing 20-month average time-to-trial, excluding transfers, and median time-to-trial of 19 months). That Judge Gilstrap’s time-to-trial statistics predict an even earlier trial date lends credibility to the November 2025 scheduled jury trial and weighs significantly in favor of denial. *Samsung Electronics*, Paper 11 at 11-12 (statistics predicting even earlier trial date “confirm[] that the schedule set by the district court is credible and should be given weight”).

Judge Gilstrap has already set the jury trial, and that jury trial will conclude well before the Board’s projected statutory deadline. EX2002. Additionally, because of the stage of the underlying case and the speed with which the Eastern District of Texas reaches case dispositions, there are likely to be district court determinations relating to the validity of the ’552 Patent in advance of the Board’s projected statutory deadline. EX2004; EX2005. Thus, *Fintiv* factor 2 favors discretionary denial.

3. Factor 3 favors denial (investment in parallel proceedings)

Factor 3 weighs in favor of denial because both Secure Wi-Fi and Samsung will have expended considerable resources in the parallel litigation, including on the merits of Samsung's invalidity positions, by the time the Board issues an institution decision. *See Sand Revolution II, LLC v. Cont'l Intermodal Grp.*, IPR2019-01393, Paper 24 at 10 (P.T.A.B. June 16, 2020) (noting that investment in invalidity contentions is relevant to this factor).

For factor 3, the Board considers "the amount and type of work already completed in the parallel litigation by the court and the parties at the time of the institution decision." *Fintiv*, IPR2020-00019, Paper 11 at 9. "This investment factor is related to the trial date factor, in that more work completed by the parties and the court in the parallel proceeding tends to support the arguments that the parallel proceeding is more advanced, a stay may be less likely, and instituting would lead to duplicative costs." *Id.* at 10.

Here, the Board is projected to issue an institution decision on March 25, 2025. Secure Wi-Fi served its infringement contentions on May 15, 2024, and on July 10, 2024, Samsung served its invalidity contentions, over seven months before the projected institution decision. EX2002. Samsung's invalidity contentions include claim charts addressing the same references asserted by Samsung in every ground of its Petition for every claim challenged in the co-pending litigation. *E.g.*,

EX2002. Secure Wi-Fi and Samsung will have expended substantial resources in the parallel litigation, including on the merits of Samsung's invalidity positions, where—as detailed below—there is significant overlap of issues.

Additionally, discovery will have been open for over nine months at the time of the institution decision. *See* EX2002 (discovery opened June 19, 2024). The parties have already exchanged interrogatory responses and document productions. Secure Wi-Fi's expert has spent days, and will continue to spend time, reviewing millions of files and gigabytes of source code data for various versions of the Android operating system running on the accused products. *Id.* Moreover, the March 31, 2025 deadline to substantially complete document production and serve privilege logs is a mere six days after the institution decision. *See* EX2005. Finally, Secure Wi-Fi has sought and negotiated third-party discovery from five different third parties, as well as the entry of a supplemental protective order to account for third-party confidentiality concerns.

The parties further will have exchanged proposed claim terms and proposed constructions, will have submitted the Joint Claim Construction Statement, and will have completed claim construction discovery. EX2002. Secure Wi-Fi's deadline to file its opening claim construction brief and technical tutorial is March 31, 2025. By the time the Board issues an institution decision, the district court and Secure Wi-Fi will have spent time and resources dealing with preparations for the *Markman*

hearing—scheduled to proceed shortly after the institution decision deadline. This factor favors denial.

4. Factor 4 favors denial (overlap of issues)

Factor 4 weighs in favor of discretionary denial because there is substantial overlap between the claims, arguments, and evidence raised in the Petition and in Samsung’s invalidity contentions in the parallel district court proceeding. The Petition challenges each asserted claim in the district court litigation (i.e., claims 1-4, 6-15, 17-20, and 22-24). Pet., 3. In the district court litigation, Samsung’s invalidity contentions challenge the same claims using at least the same asserted references of its Petition—*Vardi*, *IEEE802.11*, *Yun*, *Orava*, and *Kholaiif*. Pet., 17; EX2003, 11, 16-24 (invalidity contentions identifying prior art references and obviousness grounds, including the five references cited in the Petition). Therefore, Samsung’s common prior art challenges to the claims renders the “overlap in issues between the two proceedings [] substantial.” *Code200, UAB v. Luminate Networks, Ltd.*, IPR2020-01506, Paper 10 at 11-12 (P.T.A.B. Feb. 16, 2021).

Moreover, Samsung failed to offer a *Sotera* stipulation. Petitioners’ lesser stipulation does not fully resolve concerns about overlap, duplicative efforts, and conflicting decisions—and does not prevent denial. *Int’l Bus. Machine*, Paper 7, 12. *Inter Partes* Review is intended to be a “quick and cost effective alternative[] to litigation,” not an avenue for Petitioners to argue invalidity a second time in a second

venue. *WesternGeco LLC v. ION Geophysical Corp.*, 889 F.3d 1308, 1317 (Fed. Cir. 2018) (quoting H. REP. NO. 112-98, at 40, 48 (2011)). Indeed, Samsung’s failure to offer a *Sotera* stipulation, despite the substantial overlap between the proceedings, only highlights the concerns of duplicative efforts and conflicting outcomes raised by *Fintiv* and the USPTO’s Interim *Fintiv* Procedure.

And Samsung’s district court assertion of *additional* prior art and *additional* combinations of art than those asserted here does nothing to alter the degree of overlap between the Petition and its invalidity contentions. *See, e.g., Fintiv*, IPR2020-00019, Paper 15 at 15 (finding Petitioner’s assertion of additional invalidity contentions “not relevant to the question of the degree of overlap for this factor”). Likewise, Petitioners incorrectly argue that the Petition’s challenge of three *additional* dependent claims of the ’552 Patent somehow weighs against discretionary denial, but the Board has repeatedly ruled that such a fact does nothing to mitigate “substantial” overlap in issues between the two proceedings where common prior art is presented and common independent claims are challenged. *Code200, UAB*, IPR2020-01506, Paper 10 at 11-12 (“In light of the common prior art asserted here and in the [] district court case, as well as the common challenge to the sole independent claim and all but two of the dependent claims of the [’552] patent, we agree with the Patent Owner that the overlap in issues between the two proceedings is substantial.”); *see also Teso LT UAB v. Luminati Networks Ltd.*,

IPR2021-00122, Paper 12 at 10 (P.T.A.B. Apr. 20, 2021) (denial of institution favored where Petition’s prior art references were all identified in the district court invalidity contentions, the same independent claims were challenged in both proceedings, and “the *additional* claims challenged in the Petition are all dependent claims”).

Therefore, with this substantial overlap between the Petition and the parallel proceedings, there are particularly strong “concerns of inefficiency and the possibility of conflicting decisions” if the IPR is instituted. *See, e.g., Fintiv*, IPR2020-00019, Paper 11 at 12 (finding “concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong” where there is substantial overlap).

Accordingly, factor 4 weighs strongly in favor of denial of institution. *See Teso LT UAB*, IPR2021-00122, Paper 12 at 10 (finding “the overlap in issues between the two proceedings is substantial” where common art and common challenges to the independent claim were presented in both proceedings); *see also eClinical Works*, IPR2022-00229, Paper 10 at 12 (finding factor 4 weighed in favor of denial where Preliminary Invalidity Contentions showed overlap of asserted claims, art and arguments asserted in the Petition); *U.S. Venture, Inc. v. Sunoco Partners Mktg. & Terminals L.P.*, IPR2020-00728, Paper 10 at 12-14 (P.T.A.B. Oct. 1, 2020) (finding overlap between primary references asserted in Petition and litigation weighed in favor of denial).

For each of these reasons, factor 4 strongly favors discretionary denial.

5. Factor 5 favors denial (overlapping parties)

Patent Owner is the plaintiff and Petitioners are the defendants in the parallel litigation (EX2002), and “because the petitioner and the defendant in the parallel proceeding are the same party, this factor weighs in favor of discretionary denial.” *Samsung Elecs. Co. v. Clear Imaging Research, LLC*, IPR2020-01401, Paper 12 at 21-22 (P.T.A.B. Feb. 17, 2021) (quoting *Fintiv*, IPR2020-00019, Paper 15 at 15).

6. Factor 6 favors denial because Petitioners have failed to present a compelling unpatentability challenge.

The Board need not address the merits of the Petition because the *Fintiv* factors favor denial and the flaws in the Petition are numerous and preclude a compelling challenge. In such circumstances, the Board has found that it “need not decide whether the merits of Petitioner’s asserted grounds are particularly strong because it would not impact [the] ultimate determination under Section 314(a)” and “the merits do not outweigh the other *Fintiv* factors.” *NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00552, Paper 18 at 12-13 (P.T.A.B. May 2, 2022) (finding that where factor 1 was neutral and factors 2-5 favored or slightly favored denial, factor 6 was neutral because it “would not impact [the] ultimate determination”); *Samsung Electronics Co., Ltd. v. Clear Imaging Research, LLC*, IPR2020-01401, Paper 12 at 23-25 (P.T.A.B. Feb. 17, 2021) (finding that where factors 1 and 4 slightly favored denial, factors 2 and 3 strongly favored denial, and factor 5 weighed in

favor of denial, those factors outweighed any merits of the case considered in factor 6); *Apcon, Inc. v. Gigamon Inc.*, IPR2020-01579, Paper 9 at 26 (P.T.A.B. Mar. 16, 2021) (finding that the merits of the petitioner’s grounds do not outweigh the other factors in light of the strength of factor 2); *see also Fintiv*, IPR2020-00019, Paper 11 at 15 (“if the merits of the grounds raised in the petition are a close[] call, then that fact has favored denying institution when other factors favoring denial are present”). Here, the Petition presents no compelling case. As one of multiple failures discussed above, Petitioners fail to substantively address the meaning of “authenticated” or describe why or how the proposed combination would have rendered obvious this claim requirement.

VII. Conclusion

As shown above, the Petition fails to establish a reasonable likelihood of success as to any challenged claim. Further, the Board should exercise its discretion to deny Petitioners’ unexplained, multiple, parallel IPRs against the ’552 patent. Moreover, the *Fintiv* factors and Interim *Fintiv* Procedure warrant the Board’s exercise of discretionary denial. Institution should be denied.

Dated: December 26, 2024

Respectfully submitted,

/Jerry D. Tice II/

Jerry D. Tice II

Reg. No. 73,582 (Lead counsel)

BUNSOW DE MORY LLP

701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
jtice@bdiplaw.com

Counsel for Patent Owner

37 C.F.R. §42.24(d) CERTIFICATION

The undersigned hereby certifies that this submission, excluding the table of contents, table of authorities, exhibit list, certificate of word count, and certificate of service, contains 12,774 words, as determined using the standard word counting feature of the Microsoft Word program.

Dated: December 26, 2024

/Jerry D. Tice II/
Jerry D. Tice II
Reg. No. 73,582 (Lead counsel)

CERTIFICATE OF SERVICE

Petitioners have consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that on December 26, 2024, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

BLANK ROME LLP - samsung-swf-iprs@blankrome.com
Walter D. Davis, Jr. - walter.davis@blankrome.com
Dipu A. Dosh - dipu.doshi@blankrome.com
Jonathan W.S. England - jonathan.england@blankrome.com
Sean D. Damon - sean.damon@blankrome.com
Arun Paradkar - arun.paradkar@blankrome.com

Dated: December 26, 2024

/Jerry D. Tice II/
Jerry D. Tice II
Reg. No. 73,582