

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

HOME DEPOT U.S.A., INC.,
Petitioner

v.

RAVENWHITE SECURITY, INC.,
Patent Owner

Case IPR2024-01316
U.S. Patent No. 10,594,823

**PATENT OWNER PRELIMINARY RESPONSE
UNDER 37 C.F.R. § 42.107(a)**

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-145

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '823 PATENT	3
A.	The '823 patent provides novel techniques for enhancing the ability of websites to identify client devices.	3
B.	Level of Ordinary Skill in the Art	6
C.	Claim Construction	7
III.	OVERVIEW OF THE CITED ART	7
A.	Hinton describes session cookies for authenticating a user across domains, which are established and valid only during the user's current session.....	7
B.	Varghese describes capturing device identity information within cookies stored outside of a user's web browser storage.	9
IV.	GROUND 1: HINTON DOES NOT RENDER OBVIOUS INDEPENDENT CLAIMS 1 AND 6.....	12
A.	The Petition fails to establish that Hinton renders obvious elements [1.b.iv] and [6.a.iv] ("wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session").....	12
B.	The Petition fails to establish that Hinton renders obvious elements [1.b.v] and [6.a.v] ("wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area").	16
V.	FOUNDATIONS 2 AND 3: VARGHESE DOES NOT RENDER OBVIOUS INDEPENDENT CLAIMS 1 AND 6.....	18
A.	The Petition fails to establish that Varghese renders obvious elements [1.b.v] and [6.a.v] ("wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area").	19

1.	The independent claims of the '823 patent require storing “the first cookie” and “the second cookie” in two “browser storage area[s].”	19
2.	Varghese’s flash cookies are not stored in any “browser storage area.”	21
3.	The Office already considered flash cookies during prosecution of the '823 patent, causing the applicant to narrow the phrase “client device storage area” to “client device browser storage area.”	24
B.	The Petition fails to establish that Varghese renders obvious elements [1.b.iv] and [6.a.iv] (“wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session”).....	26
VI.	THE BOARD SHOULD DENY THE PETITION IN VIEW OF THE PARALLEL LITIGATION.....	29
VII.	CONCLUSION.....	33

PATENT OWNER'S EXHIBIT LIST

Exhibit No.	Description
2001	Docket Control Order, <i>RavenWhite Licensing LLC v. The Home Depot, Inc.</i> , Case No. 2:24-cv-00688 (E.D. Tex.)
2002	Complaint, <i>RavenWhite Licensing LLC v. The Home Depot, Inc.</i> , Case No. 2:23-cv-00423 (E.D. Tex.)
2003	“A Dictionary of Computing,” Sixth Edition, Oxford University Press (2008)
2004	“Computer Memory,” GeeksforGeeks, accessed at https://www.geeksforgeeks.org/computer-memory/ (Aug. 3, 2023)
2005	Herrman, J., “What Are Flash Cookies and How Can You Stop Them?,” Popular Mechanics, accessed at https://www.popularmechanics.com/technology/security/how-to/a6134/what-are-flash-cookies-and-how-can-you-stop-them/ (Sept. 23, 2010)
2006	“What are Flash Cookies and how do they Work?,” CookieScan, accessed at https://www.cookiescan.com/what-are-flash-cookies-how-do-they-work/

I. INTRODUCTION

U.S. Patent No. 10,594,823 (“the ’823 patent”) provides novel techniques that allow websites to identify client devices while addressing security concerns typically associated with traditional cookies. EX1001, 2:66-3:4. The ’823 patent accomplishes these goals through use of “cache cookies that the server can use to identify the client device (or user),” “[e]ven if the browser is blocking cookies” or “has deleted its cookies.” *Id.*, 2:66-3:4, 6:49-53. The Office thoroughly evaluated the claims of the ’823 patent, ultimately determining that “the prior art does not teach or suggest the specially ordered and enumerated features of the independent claims.” EX1003, 310.

Here, Petitioner presents two obviousness grounds challenging independent claims 1 and 6 of the ’823 patent: one based on Hinton (EX1005) and one based on Varghese (EX1004). But Petitioner fails to establish that either Hinton or Varghese teaches the features of independent claims 1 and 6. In fact, the same claim features are missing from both Hinton and Varghese.

With respect to Hinton, Petitioner fails to establish that Hinton teaches “*a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*” (elements [1.b.iv] and [6.a.iv]). Petitioner purports that Hinton discloses two cookies: a “domain identity cookie (DIDC)” and an “‘e-Community Cookie’ (eCC).” Pet., 12, 18. But

Hinton's e-community cookie is generated and valid only during the *current* network session—not a “*previous network session*,” as required by the independent claims. EX1005, ¶¶137, 249. Petitioner also fails to establish that Hinton teaches “*the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area*” (elements [1.b.v] and [6.a.v]). Although Hinton describes a “persistent cookie store” and a “browser cookie memory,” the Petition does not establish that these are two different “*browser storage area[s]*,” as the claims require.

With respect to Varghese, Petitioner similarly fails to establish that Varghese teaches “*the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area*” (elements [1.b.v] and [6.a.v]). Petitioner points to Varghese's “flash cookie” as the recited “*second cookie*,” Pet., 48, but Petitioner's own evidence shows that flash cookies are *not* stored in a “*browser storage area*.” EX1002, ¶168; EX1014, 2. Moreover, the Office already evaluated (and used as a basis for rejection) Varghese's flash cookies during prosecution. EX1003, 81, 84-89, 97-103, 151-155, 162-164, 167-168, 204-213, 216-218. Petitioner also fails to establish that Varghese teaches “*a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*” (elements [1.b.iv] and [6.a.iv]). Varghese discloses that its cookies—both

its “standard cookie[s]” and “flash cookie[s]”—are replaced “upon each login.”

EX1004, 24:33-35, 26:4-11, 26:13-29. Petitioner, therefore, does not establish that Varghese’s purported cookies are stored in different “*previous network session[s]*,” as required by the claims.

Aside from the merits, the Board should discretionarily deny the Petition in view of the parallel district-court litigation. The parties have already invested significant effort and resources into the parallel litigation, Petitioner asserts the same art in the parallel litigation as it does here, and Petitioner has not filed any stipulation to reduce duplicative efforts across tribunals. As trial is set to begin less than one month following a Final Written Decision here, institution of this proceeding would lead to duplication of work and increased costs for both parties.

Accordingly, the Board should deny institution of this proceeding.

II. THE ’823 PATENT

A. The ’823 patent provides novel techniques for enhancing the ability of websites to identify client devices.

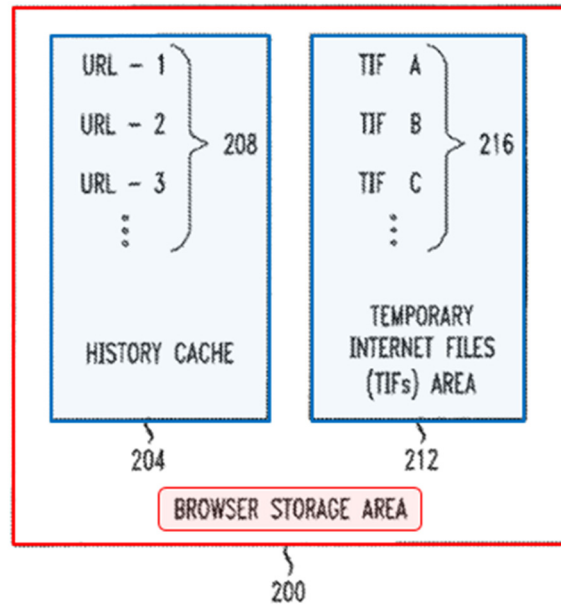
The ’823 patent generally relates to “causing a browser to store information in a browser storage area of a client device” that can later be used for “identification of a user.” EX1001, 1:31-34, 2:5-6. The ’823 patent explains that “[a] Web page . . . may request user information from the user when the user first accesses the page, such as a user’s name, password, address, interests, etc.” *Id.*, 1:39-42. “When the user accesses the same Web page at a later time, the server

may use the information previously entered by the user to customize the Web page for the user.” *Id.*, 1:42-45.

The ’823 patent further explains that “[t]his customization of a Web page is typically the result of cookies,” which are “message[s] transmitted to a browser by a server.” EX100, 1:46-48. “The message can include user-specific identifiers or personal information about the user,” and “[t]he message (i.e., cookie) is then sent back to the server each time the browser requests a Web page from the server.” *Id.*, 1:48-52. However, “[d]espite the benefits associated with customizing a Web page, cookies also present drawbacks.” *Id.*, 2:11-13. “As a result, some people block or clear cookies,” which results in organizations such as “banks [to] lose another technique to identify the user.” *Id.*, 2:24-40.

As the ’823 patent explains, to circumvent issues associated with traditional cookies, “one or more servers instead ‘write’ and ‘read’ a cache cookie to and from a browser storage area associated with a browser requesting a Web page from the server(s).” EX1001, 2:66-3:3. The patent describes exemplary embodiments in which “[t]he browser storage area may include a history cache and/or a Temporary Internet Files (TIFs) area.” *Id.*, 3:3-4. These two storage areas are illustrated in Figure 2.

FIG. 2



EX1001, FIG. 2 (annotated).

The “history cache 204 [] contains Uniform Resource Locators (URLs) 208 recently visited by the browser (also called browser history).” EX1001, 6:4-8. “A server can ‘write’ any of a wide variety of cache cookies,” e.g., URLs “recently visited by the browser,” “in the history cache 204 to, for instance, facilitate the identification of a client device (or user).” *Id.*, 6:4-8, 6:22-24. Then, “when the user revisits” a URL, “the server can ‘read’ the history cache 204 of the client device to determine what Web pages the browser has recently visited.” *Id.*, 6:42-45. “The server can use the pattern of URLs stored in the browser's history cache 204 to, e.g., identify the client device (or user).” *Id.*, 6:47-49. And “[e]ven if the browser is blocking cookies (or has deleted its cookies . . .), the history cache 204 still

contains the cache cookies that the server can use to identify the client device (or user).” *Id.*, 6:49-53.

“The browser storage area 200 can also include a Temporary Internet Files (TIFs) area 212 for storing TIFs 216,” which “are files containing information embedded in Web pages.” EX1001, 6:54-57. When a user returns to a URL, “[t]he server can use [a] determination (i.e., of which specific image files the browser retrieves from its local TIF area 212) to identify the browser.” *Id.*, 7:25-32. The patent explains that “[a]s a result, the TIFs stored in the TIF area 212 of a browser are an embodiment of cache cookies” that “persist indefinitely.” *Id.*, 6:64-67, 7:33-34.

Thus, by employing “cache cookie[s],” the ’823 patent addresses issues associated with traditional cookies, while still allowing websites to identify client devices. EX1001, 2:66-3:4.

B. Level of Ordinary Skill in the Art

For purposes of this Preliminary Response, Patent Owner applies Petitioner’s definition of a person of ordinary skill in the art (“POSITA”). Pet., 6. Patent Owner, however, does not waive its right to present a different definition at a later stage.

C. Claim Construction

All claim terms must be given their ordinary and customary meaning as understood by a POSITA at the time of the invention in light of the specification and the patent's prosecution history. 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-1313 (Fed. Cir. 2005) (en banc). At this preliminary stage, no term needs explicit construction to resolve any controversy between the parties. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

III. OVERVIEW OF THE CITED ART

A. Hinton describes session cookies for authenticating a user across domains, which are established and valid only during the user's current session.

Hinton (EX1005) is directed to “cross-domain log on technologies and technologies which create and manage virtual communities of online users.” EX1005, ¶7. “Each Internet user is served by a ‘home domain’, which is a domain in which a user is ‘registered’.” *Id.*, ¶9. “[T]he home domain itself may have ‘long term’ relationships with other domains,” such as “e-community domains, where one domain (e.g. the home domain) is responsible for user registration issues.” *Id.*, ¶10.

Hinton further explains that “[o]ften, a user will access resources in different (‘participating’) domains on behalf of their home domain,” and “the user will have to resubmit to a log in or authentication process as he or she moves from the home

domain to another domain.” EX1005, ¶11. Hinton sought to address this issue through “a cross-domain single-sign-on system and method which allows an Internet user to establish a long-term relationship with participating domains, and which gives the user the ability to go directly to participating domains, via bookmarks or direct URL’s for example, without having to go through a home domain first.” *Id.*, ¶15.

Hinton’s process requires users to enroll into an “e-community.” EX1005, ¶70. “As a result of enrollment into the e-community, a user will have a ‘domain identity cookie’ (‘DIDC’) established by each of the participating e-community domains,” which provides for “single-sign-on functionality.” *Id.* Following establishment of the DIDC, “[i]f a user requests a protected resource in another domain, then authentication information must be transferred across the e-community.” *Id.*, ¶129. The DIDC allows the user’s home domain to “vouch[] for a user’s identity,” and “[a]s a result of authentication, the SSO plug-in generates an ‘e-Community Cookie’ (an eCC or e-community cookie).” *Id.*, ¶¶130, 136.

“[A] user has one e-community cookie set for each domain at which it has a current, authenticated (or vouched-for) session.” EX1005, ¶132. And, importantly, “[a]n eCC is valid for only for [sic] the duration of a browser session, and it is expired when a user invokes logout functionality.” *Id.*, ¶249. In other words,

Hinton's eCC is established and valid only within a user's current network session—it is never reused in a subsequent session. *Id.*

B. Varghese describes capturing device identity information within cookies stored outside of a user's web browser storage.

Varghese (EX1004) is directed to “providing protection against identity theft over a computer network.” EX1004, 1:16-18. Varghese's purported “invention includes secure cookies, flash objects and other technologies to recognize and to fingerprint [] from which device a user access an application, whether it is a computer, laptop, mobile device or any other.” *Id.*, 5:64-67. “These user devices thus become additional authentication factors without requiring any change in user behavior” and “[i]nformation concerning these user devices is fingerprinted and stored into a device token or device id for one-time use.” *Id.*, 5:67-6:4.

Figure 4A of Varghese illustrates “exemplary embodiments of the device fingerprinting process 400 of the system and method of the present invention.” EX1004, 24:33-35.

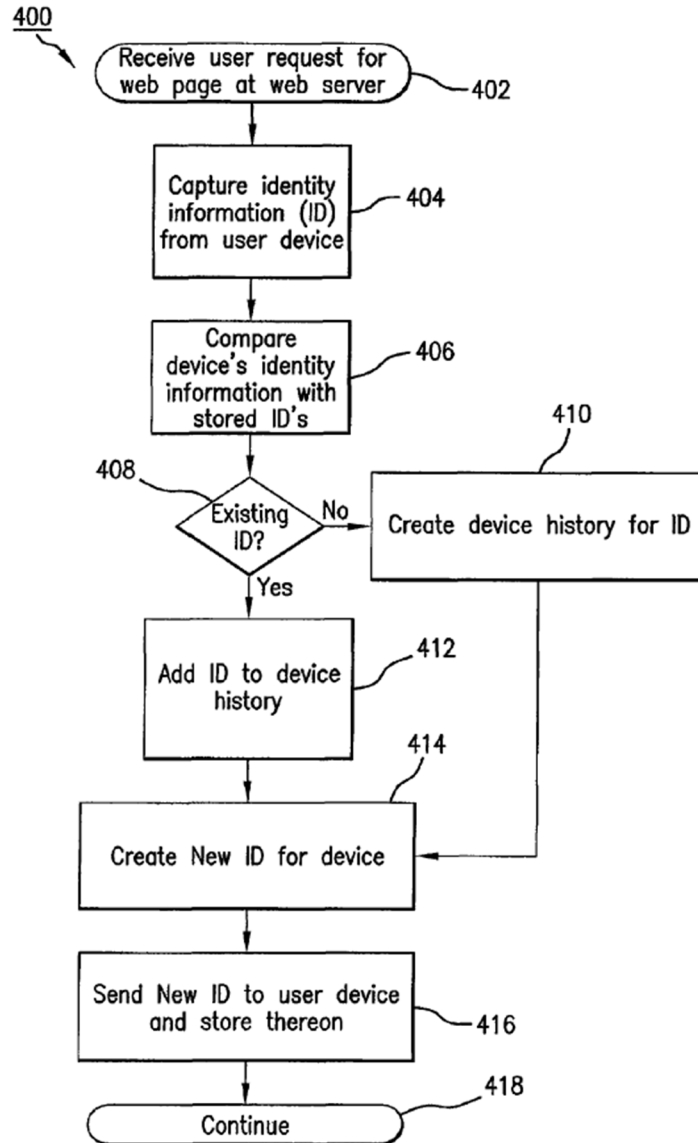


FIG.4A

EX1004, FIG. 4A.

Varghese describes, “[i]n Step 402, a request is received at a service provider server from a user device.” EX1004, 24:40-42. “The fingerprinting process is invoked and information describing the request is transferred.” *Id.*, 24:42-44. Then, “[i]n Step 404, device identity information for the user device is

captured . . . by a client program already resident on the user device,” such as “a web browser.” *Id.*, 24:50-53.

Varghese explains that captured device information can be stored in the form of “cookies.” EX1004, 25:7-42. “One such technique is known as ‘secure cookies,’” which is “a data packet sent by a web server to a web browser for saving to a file on the host machine,” and that “has been secured against modification or tampering.” *Id.*, 25:22-32. “Another such technique is known as ‘flash cookies’.” *Id.*, 25:33. In this case, “Flash” “software can create local shared objects, known as ‘flash cookies’, for maintaining locally persistent data on a user’s device akin to the standard ‘cookies’ stored by web browsers.” *Id.*, 25:34-43.

Of note, because flash cookies are stored outside of browser storage in a “special directory” associated with “Flash” software, EX1014, 2, Varghese explains that they “have the advantage [of] not being as easily removed from the user’s device as are standard cookies,” EX1004, 25:40-43. Nonetheless, a significant disadvantage is that Varghese’s system requires that the end-user install and maintain additional software (Flash software) on the host machine, and that the supplier of the software continue supporting and not discontinue that additional software. *See* EX1004, 25:34-37 (requiring installation of “software applications and/or plug-ins from Macromedia” for use of “flash cookies”); EX1014, 2

(installation of Macromedia “Flash Player” software required for use of flash cookies); EX2006, 3-4 (same).

IV. GROUND 1: HINTON DOES NOT RENDER OBVIOUS INDEPENDENT CLAIMS 1 AND 6.

As detailed in the sections below, the Petition fails to establish that Hinton renders obvious at least the following elements of independent claims 1 and 6: (1) *“wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session”* (elements [1.b.iv] and [6.a.iv]); and (2) *“wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area”* (elements [1.b.v] and [6.a.v]). The Petition, therefore, does not establish a reasonable likelihood that Hinton renders obvious independent claims 1 and 6.

A. The Petition fails to establish that Hinton renders obvious elements [1.b.iv] and [6.a.iv] (“wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session”).

Each of independent claims 1 and 6 recites, *“a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session.”* EX1001, 15:47-50, 16:41-44 (emphasis added). The Petition fails to show that Hinton teaches this claim element.

The Petition alleges that Hinton’s “domain identity cookie (DIDC)” is the recited “*first cookie*” of the independent claims, and that Hinton’s “‘e-Community Cookie’ (eCC)” is the recited “*second cookie.*” Pet., 12, 18. Hinton’s e-community cookie, however, is not “*stored at the client device during a second **previous** network session.*” EX1001, 15:47-50, 16:41-44 (emphasis added). Rather, Hinton’s e-community cookie is generated and valid only during the *current* network session. EX1005, ¶¶137, 249.

Hinton’s system “allows an Internet user to transfer directly to a domain that is participating in the e-community, by means such as a Bookmark or a directly-typed URL, without the necessity of returning to a home domain prior to transferring to the participating domain.” EX1005, ¶23. “As a result of enrollment into the e-community, a user will have a ‘domain identity cookie’ (‘DIDC’) established by each of the participating e-community domains,” which provides for “single-sign-on functionality.” *Id.*, ¶70.

Following establishment of the DIDC, “[i]f a user requests a protected resource in another domain, then authentication information must be transferred across the e-community.” EX1005, ¶129. In particular, the Petition alleges that “[d]uring a session subsequent to the session that created the DIDC, when a user requests access to an affiliated domain, the affiliated domain generates an eCC for that domain and causes the eCC cookie to be stored at the user’s device by sending

the eCC cookie to the user.” Pet., 19 (citing EX1005, ¶137). Petitioner ignores, however, that the “session subsequent to the session that created the DIDC,” Pet., 19, is the *current* network session—not “*a second previous network session*,” as required by the independent claims.

Specifically, Hinton explains that “a user has one e-community cookie set for each domain at which it has **a current, authenticated (or vouched-for) session.**” EX1005, ¶132 (emphasis added). This “**eCC is valid for only for** [sic] **the duration of a browser session**, and it is expired when a user invokes logout functionality.” EX1005, ¶249. Thus, the e-community cookie could not have been “*caused to be stored at the client device during a second previous network session*,” as required by the independent claims. EX1001, 15:47-50, 16:41-44 (emphasis added).

Hinton provides an example of this operation, explaining that an e-community cookie is established and used within “a current, authenticated session”—not a previous session:

As an example, consider a hypothetical site “www.acme.com” that is partitioned so that there is a distinct security policy server set of replicas protecting each of the engineering, accounting, and human resource departments. In this situation, if a user authenticates (or is vouched for) first to engineering, **they will have a domain-wide e-community cookie set** by the engineering security policy server. **When this user then goes to the accounting server, this e-community cookie**

indicates that the user has a current, authenticated session, and that the accounting server need not re-authenticate the user.

EX1005, ¶134 (emphasis added). Thus, Hinton does *not* disclose that an e-community cookie is stored in a “*previous network session*” and reused in a subsequent session. *Id.*, ¶¶132, 134, 249.

Tellingly, the Petition does not even allege that Hinton’s eCC “*was caused to be stored at the client device during a second **previous** network session,*” as required by the claims. Pet., 18-19 (emphasis added). Instead, Petitioner merely contends that “Hinton’s system discloses saving the eCC cookie in a **different** session than the DIDC cookie.” Pet., 19 (emphasis added). Indeed, the Petition relies on the *same* request to access an “affiliated domain” to satisfy both the claimed current “*network resource request*” and a “*previous network session.*” *Compare* Pet., 12 (“Hinton’s affiliated domain receives a request from user 100 to access contents of its domain, which a POSITA would have understood to be a network resource request”) (citing EX1005, ¶137), *with* Pet., 19 (“when a user requests access to an affiliated domain, the affiliated domain generates an eCC”) (citing EX1005, ¶137). Petitioner’s analysis thus confirms that Hinton’s e-community cookie is established and used only within the current network session, not a “*previous network session,*” as required by the independent claims.

Accordingly, the Petition fails to establish that Hinton renders obvious elements [1.b.iv] and [6.a.iv].

- B. The Petition fails to establish that Hinton renders obvious elements [1.b.v] and [6.a.v] (“wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area”).**

Each of independent claims 1 and 6 recites, “*wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area.*” EX1001, 15:50-54, 16:44-49. The Petition fails to establish that Hinton teaches “*a second client device browser storage area different from the first client device browser storage area.*” *Id.*

Hinton describes, “the user’s browser extracts (62) the DIDC and stores it in the **browser’s persistent cookie store**, such as storing it in a cookie folder on a hard disk drive.” EX1005, ¶88 (emphasis added). Hinton further describes that its “[e]-community cookie (eCC) . . . resides in the user's **browser cookie memory.**” EX1005, ¶248 (emphasis added). Pointing to this disclosure, Petitioner asserts, “[a]s Hinton expressly discloses that the storage areas for the two cookies have different names, a POSITA would have understood that the two storage areas are different browser storage areas.” Pet., 20.

The Petition further contends that “because the browser’s cookie store is persistent and the browser cookie memory is temporary, they are different storage areas for the browser.” Pet., 20. But Petitioner provides no support for the proposition that the term “memory,” by itself, indicates “temporary” storage. *Id.* Hinton provides no further details of how its cookies are stored, and the term memory may refer to *both* persistent and temporary memory. For example, the Oxford Dictionary of Computing explains that the term “memory” simply refers to “[a] device or medium that can retain information for subsequent retrieval.” EX2003, 311-312; *see also* EX2004, 4-5 (explaining that “secondary memory,” such as a “magnetic disk,” “is a non-volatile memory and used to store a large amount of data or information”). “The term [‘memory’] is **synonymous with storage and store . . .**” EX2003, 311-312 (emphasis added). Thus, the Petition fails to establish that the phrases “browser cookie **memory**” and “browser’s persistent cookie **store**,” EX1005, ¶¶88, 248 (emphasis added), refer to two different browser storage areas in Hinton.

The Petition also provides no reason why a POSITA would have sought to use two different browser storage areas. Pet., 20. And Petitioner’s expert merely repeats the Petition verbatim, providing no further reasoning or evidence. EX1003, ¶94; *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (P.T.A.B. Aug. 24, 2022) (holding that testimony that “merely repeats, *verbatim*, the conclusory

assertion for which it is offered to support . . . is entitled to little weight.”); *TQ Delta, LLC v. Cisco Systems, Inc.*, 942 F.3d 1352, 1359 (Fed. Cir. 2019) (“This court’s opinions have repeatedly recognized that conclusory expert testimony is inadequate to support an obviousness determination . . .”).

Therefore, the Petition’s analysis (or lack thereof) is insufficient to establish that Hinton renders obvious elements [1.b.v] and [6.a.v]. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (“[O]bviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.”) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

V. GROUNDS 2 AND 3: VARGHESE DOES NOT RENDER OBVIOUS INDEPENDENT CLAIMS 1 AND 6.

The Petition fails to establish that Varghese renders obvious at least the following elements of independent claims 1 and 6: (1) “*wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area*” (elements [1.b.v] and [6.a.v]); and (2) “*wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*” (elements [1.b.iv] and [6.a.iv]). The Petition, therefore, does not establish a reasonable likelihood that Varghese renders obvious independent claims 1 and 6.

- A. The Petition fails to establish that Varghese renders obvious elements [1.b.v] and [6.a.v] (“wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area”).

As noted with respect to Ground 1, each of independent claims 1 and 6 recites, “*wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area.*” EX1001, 15:50-54, 16:44-49. The Petition fails to establish that Varghese teaches this element because Varghese’s “flash cookie”—relied on for the claimed “*second cookie*,” Pet., 48-49—is not stored in a “*browser storage area*,” as required by the independent claims.

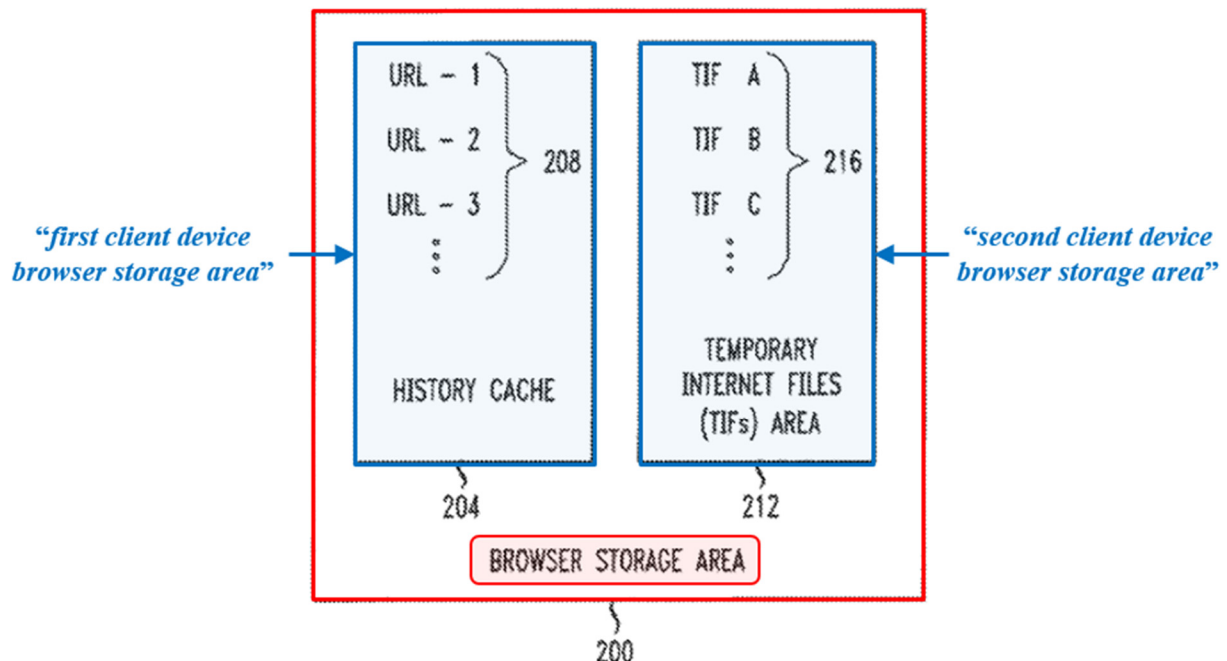
1. The independent claims of the ’823 patent require storing “the first cookie” and “the second cookie” in two “browser storage area[s].”

Each independent claim recites two storage areas that are specifically associated with the client device browser: “*a first client device browser storage area*” and “*a second client device browser storage area.*” EX1001, 15:50-54, 16:44-49. The ’823 patent explains, for example, “[w]hen a browser displays a Web page for the first time, the browser typically downloads one or more files (e.g., images, text, style sheets, etc.) to its browser storage area (e.g., browser cache).” EX1001, 4:60-63 (emphasis added). “The next time the browser visits the

same Web page, **the browser determines what is stored in its browser storage area** and displays the local copy of the files rather than downloading the same files again.” EX1001, 4:66-5:3 (emphasis added).

Example “*client device browser storage area[s]*” are described with respect to Figure 2 of the ’823 patent. Specifically, Figure 2 illustrates “a browser storage area 200” including “a **history cache 204** that contains Uniform Resource Locators (URLs) 208 recently visited by the browser (also called browser history)” and “a **Temporary Internet Files (TIFs) area 212** for storing TIFs 216.” EX1001, 6:4-8, 6:54-56 (emphasis added); *see also id.*, 3:3-4 (“The browser storage area may include a history cache and/or a Temporary Internet Files (TIFs) area.”).

FIG. 2



EX1001, FIG. 2 (annotated).

“[T]he URLs written to the history cache 204 by the server” and “the TIFs stored in the TIF area 212 of a browser” are “embodiment[s] of cache cookies” stored in browser storage areas. EX1001, 6:39-41, 7:33-34. And the ’823 patent further explains that these browser storage areas are specifically associated with the user device’s browser: “[O]ne or more servers [] ‘write’ and ‘read’ a cache cookie to and from **a browser storage area associated with a browser** requesting a Web page from the server(s).” EX1001, 2:66-3:3 (emphasis added).

Thus, the ’823 patent claims and discloses storing cookies in two “***browser storage area[s]***”—for example, “a history cache 204” and “a Temporary Internet Files (TIFs) area 212,” EX1001, 6:4-8, 6:54-56 (emphasis added)—not simply two storage areas on the client device.

2. Varghese’s flash cookies are not stored in any “browser storage area.”

Petitioner alleges that “Varghese discloses the use of two cookies – secure cookies and flash cookies.” Pet., 36. Petitioner equates Varghese’s “secure cookie” to the recited “*first cookie*” and Varghese’s “flash cookie” to the recited “*second cookie*.” Pet., 48. But, as demonstrated by Petitioner’s own evidence, Varghese’s flash cookies are not stored in a “***browser storage area***,” as required by the independent claims.

Specifically, Petitioner's expert explains that "[s]ecure cookies are standard cookies known to be **saved by the Web browser in browser-maintained files,**"

but, "[i]n contrast, **Flash cookies are stored in a separate storage area.**"

EX1002, ¶168 (emphasis added). Petitioner's expert further explains that flash cookies not stored in browser storage at all; rather, they "are stored on the client machine as Local Shared Objects: 'Windows C:\Documents and Settings\[username]\Application Data\Macromedia\Flash Player; Macintosh OSX /Users/[username]/Library/Preferences/Macromedia/Flash Player; GNU-Linux ~/.macromedia.'" EX1002, ¶168 (citing EX1014, 2).

In other words, Varghese's flash cookies are stored in a "special directory" on the user's hard disk that is associated with Macromedia Flash Player software—not with the user's Web browser. EX1014, 2. Petitioner provides no reason to store Varghese's flash cookies in a "**browser storage area,**" merely contending that "it was obvious to a POSITA to organize different types of files in different folders." Pet., 48-49. Such analysis fails to address the claim language. *Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249, 1257 (Fed. Cir. 2010) ("Claims must be interpreted with an eye toward giving effect to all terms in the claim.") (internal citations omitted)).

Indeed, Varghese explains that because flash cookies are *not* stored in a "**browser storage area,**" they "have the advantage [of] not being as easily removed

from the user's device as are standard cookies." EX1004, 25:40-43. That is—consistent with Petitioner's own expert's testimony—flash cookies are specifically designed to persist *outside* of browser storage. *See* EX2005, 2 ("[T]he Flash plug-in is able to store data locally just like your browser does, **but in a different location on your hard drive**. 'And since Flash is an add-on component,' . . . 'built-in browser controls over standard cookies don't apply to Flash cookies.'") (emphasis added); EX2006, 2 (same), 3 ("**Because these cookies are stored outside the browser** you cannot protect yourself by using a different browser") (emphasis added); EX1002, ¶168. Thus, storing Varghese's flash cookies in a "**browser storage area**" would not only run contrary to Varghese's express teachings, but to the purpose of flash cookies themselves. Varghese's express teachings thus demonstrate that a POSITA would not have been motivated to store flash cookies in a browser storage area.

On the other hand, the '823 patent's use of browser storage areas provides a significant advantage over flash cookies. Specifically, the patented invention does not require end-users to separately install and maintain Flash software on their host machines. EX1004, 25:34-37; EX1014, 2; EX2006, 3-4. Nor does the '823 patent rely on an additional third party to continue supporting (and not discontinue) Flash software in order to store flash cookies. EX1004, 25:34-37; EX1014, 2; EX2006, 3-4.

Accordingly, because Varghese’s flash cookies are not “*stored in a second client device **browser storage area**,*” Varghese does not render obvious elements [1.b.v] and [6.a.v].

3. **The Office should exercise its discretion under § 325(d) because it already considered flash cookies during prosecution of the ’823 patent, causing the applicant to narrow the phrase “client device storage area” to “client device browser storage area.”**

While the Board should deny on the merits for the reasons just discussed, it would also be on solid ground to exercise discretion under 35 U.S.C. § 325(d) because the same arguments regarding flash cookies were considered and overcome during prosecution, and Petitioner has not identified any error. *Advanced Bionics v. Med-El Elektromedizinische Geräte GMBH*, IPR2019-01469, Paper 6, 8-11 (P.T.A.B. Feb. 13, 2020) (designated precedential Mar. 24, 2020).

During prosecution of the ’823 patent, the Office repeatedly rejected the claims as obvious in view of a reference titled “Local Shared Objects – ‘Flash Cookies’” (hereinafter Flash). EX1003, 81, 84-89, 97-103, 151-155, 162-164, 167-168, 204-213, 216-218. Significantly, the Examiner asserted that Flash discloses “wherein a second cookie of a second type different from the first type was caused to be stored at the client device during the previous network session, and **wherein the first and second cookies are stored in different client device storage areas of the client device,**” pointing to the same storage location as Petitioner’s expert

here. *Compare* EX1003, 167-168 (emphasis added), *with* EX1002, ¶168 (citing EX1014, 2). Indeed, Petitioner’s expert relies on the same evidence already used to reject the claims during prosecution—Exhibit 1014. EX1003, 81 (showing Exhibit 1014 in Notice of References Cited).

Ultimately, in response to these rejections, the applicant amended the claims to narrow the phrases “first client device storage area” to “first client device browser storage area,” and “second client device storage area” to “second client device browser storage area.” EX1003, 346. Thus, the same arguments (based on cumulative art) were previously presented to, and thoroughly considered by, the Office during prosecution. *Advanced Bionics*, IPR2019-01469, Paper 6 at 8.

Petitioner provides no explanation as to why the Office should reconsider the same evidence and arguments already considered and overcome during prosecution. Petitioner merely states, “[s]hould the challenges herein be found to be based on *prior art* that is the same as or cumulative to *prior art* considered by the examiner during prosecution, the examiner has made a clear error in allowing the claims over such prior art” because “the challenges in this Petition satisfy the compelling merits standard.” Pet., 71 (emphasis added). But Section 325(d) is not limited to prior art; it also considers the arguments that were previously before the Office. And such a generic statement does not “point[] out sufficiently how the examiner erred in its evaluation of the asserted prior art” or arguments, especially

given that flash cookies formed the basis of multiple rejections during prosecution. *See Advanced Bionics*, IPR2019-01469, Paper 6 at 9 n.10 (quoting *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8, 17-18 (P.T.A.B. Dec. 15, 2017) (precedential: § III.C.5, first paragraph)). Petitioner does not even address how flash cookies are stored in a “**browser storage area**”—which would contradict the express teachings of Varghese—defeating any claim of compelling merits. *See* Pet., 48-49 (asserting only that cookies would be stored in “different folders”).

The Board, therefore, need not (and should not) reconsider the evidence and arguments presented during prosecution of the ’823 patent. *Advanced Bionics*, IPR2019-01469, Paper 6 at 8-10.

B. The Petition fails to establish that Varghese renders obvious elements [1.b.iv] and [6.a.iv] (“wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session”).

Each of independent claims 1 and 6 requires that the “*first cookie . . . was caused to be stored to the client device during a **first previous network session**,*” and the “*second cookie . . . was caused to be stored at the client device during a **second previous network session**.*” EX1001, 15:36-50, 16:31-44 (emphasis added). As noted in Section V.A.2, Petitioner equates Varghese’s “secure cookie” to the recited “*first cookie*” and Varghese’s “flash cookie” to the recited “*second cookie*.” Pet., 48. But the Petition fails to establish that Varghese teaches storing these

cookies in two different “*previous network session[s]*,” as required by the independent claims.

To meet this limitation, Petitioner asserts that Varghese “discloses that secure cookies can be removed from the browser’s memory when the user clears the browser’s cookies,” and “that the cookies are routinely replaced with each login (*i.e.*, new network session).” Pet., 46-47 (citing EX1004, 26:13-14). From these statements, Petitioner concludes, “[t]hus, a POSITA would have understood and found obvious that Varghese discloses a scenario in which the flash cookie was created and stored in a second previous session than the secure cookie (e.g., the user cleared the browser’s cookies).” *Id.*, 47.

Varghese, however, provides no support for Petitioner’s hypothetical scenario. Indeed, the passage of Varghese relied on by Petitioner supports the opposite conclusion—that *both* secure cookies and flash cookies would be replaced upon each login, regardless of whether a user cleared the browser’s secure cookies.

As part of Varghese’s “device fingerprinting process,” Varghese explains that “a new Device ID token is created for the device,” which is “sent to the user device and stored thereon, e.g., **as a standard cookie or as a flash cookie.**” EX1004, 24:33-35, 26:4-11 (emphasis added). Referring to these cookies, Varghese further explains that “[a] feature of the invention relates to the **replacement of the cookie on the user’s machine upon each login**” so that

“stolen fingerprints, tokens, or device ids cannot be fraudulently reused.” *Id.*, 26:13-29 (emphasis added). In other words, Varghese discloses replacing cookies—including *both* secure cookies and flash cookies—upon each login. Thus, in Petitioner’s hypothetical scenario in which a user cleared the browser’s cookies, Varghese’s system would still replace *both* the secure cookie and flash cookie on the next login (i.e., during the *same* session).

Petitioner and its expert also provide no reason to modify Varghese to generate and store secure cookies and flash cookies in different network sessions. Pet., 46-48; EX1002, ¶166. To the contrary, as noted above, Varghese counsels against doing so to prevent “stolen fingerprints, tokens, or device ids” from being “fraudulently reused.” *See* EX1004, 26:13-29.

Petitioner’s citation to Varghese’s Table 8 does not salvage its argument. Petitioner contends, with no explanation, “Varghese contemplates the cookies being created in different network sessions when only one of the secured cookie or the flash cookie is present.” Pet., 47 (citing EX1004, Table 8); EX1002, ¶166 (repeating Petition verbatim). Nowhere does Varghese describe or suggest this operation.

Varghese’s Table 8 merely depicts “exemplary security evaluation in the form of decision tables.” EX1004, 19:28-30, Table 8. For example, Varghese explains how security decisions are made based on the existence of certain data,

such as when a flash cookie exists but a secure cookie does not. *Id.*, 19:55-20:10, Table 8. But nowhere does Varghese teach that a secure cookie or flash cookie is created upon performing a security check. *Id.* Rather, “[i]f the retrieved data tokens that were previously stored on a device by this invention, **e.g., a secure cookie, a Flash cookie, or Flash data, are not present, a further pattern check is performed,**” which “examines the particulars of the pattern of the location and device criteria and assigns an appropriate score.” *Id.*, 19:62-67 (emphasis added).

That is, when a cookie is missing (e.g., if a user were to clear the browser’s cache), Varghese simply assesses other device characteristics to make a security decision. Varghese’s description with respect to Table 8 in no way supports that Varghese’s secure cookie and flash cookie would be created in two different “*previous network session[s]*,” as required by the independent claims.

Accordingly, the Petition fails to establish that Varghese renders obvious elements [1.b.iv] and [6.a.iv].

VI. THE BOARD SHOULD DENY THE PETITION IN VIEW OF THE PARALLEL LITIGATION.

In *Apple Inc. v. Fintiv, Inc.*, the Board articulated six nonexclusive factors for determining whether to institute an AIA post-grant proceeding where there is parallel district-court litigation. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (“*Fintiv*”). On June 21, 2022, Director Vidal issued a Memorandum re: Interim Procedure for Discretionary Denials in AIA Post-Grant

Proceedings with Parallel District Court Litigation (“*Fintiv* Memo”) clarifying the procedure that the Board should follow when evaluating the six *Fintiv* factors.

Here, the Board should exercise its discretion to deny the Petition because (1) *Fintiv* factors one through five support discretionary denial; and (2) the Petition does not provide a compelling, meritorious challenge (*Fintiv* factor six).

Fintiv factor one: As Petitioner notes, no stay has been requested in the parallel litigation, and there is no indication that the court would grant in the event this proceeding were instituted. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12 (P.T.A.B. May 13, 2020) (“*Fintiv II*”) (in similar circumstances finding that “[t]his factor does not weigh for or against discretionary denial”). This factor, therefore, is neutral.

Fintiv factor two: Trial in the parallel litigation is scheduled to begin April 20, 2026. EX2001, 1. If trial were instituted in this proceeding, a Final Written Decision would be due around the same time (March 25, 2026). The close proximity of trial to the projected Final Written Decision deadline should, at a minimum, be considered neutral and “implicate other factors . . . such as the resources that have been invested in the parallel proceeding.” *Fintiv*, 9.

Fintiv factor three: Petitioner asserts that the parallel “litigation was just initiated on August 21, 2024, and there is no schedule yet entered for that matter.” Pet., 69. Petitioner ignores that the parties have been litigating for almost a year

and a half. An initial complaint against Petitioner was filed on September 18, 2023. EX2002. That case was ultimately dismissed without prejudice, and a new complaint against Petitioner was filed August 21, 2024.

Since September 18, 2023, the parties have made significant investment into litigating the '823 patent. Discovery began in November with RavenWhite's mandatory production of documents relevant to all claims and defenses. And by March 25, 2025 (the institution decision deadline), the parties will have prepared and exchanged infringement and invalidity contentions (including subject-matter eligibility contentions). EX2001, 4-5. These facts weigh at least "somewhat in favor of discretionary denial." *Fintiv II*, 14.

Moreover, Petitioner waited until the second-to-last day it was allowed to file its petition—almost exactly one year after being served with a complaint—and provides no explanation as to its filing delay. Pet., 67-71 (discussing *Fintiv* factors); 35 U.S.C. § 315(b). This fact weighs heavily in favor of discretionary denial. *Fintiv*, 11-12 ("If, however, the evidence shows that the petitioner did not file the petition expeditiously, . . . these facts have favored denial.").

Fintiv factor four: *Fintiv* factor four weighs heavily in favor of discretionary denial. "Fintiv factor four looks at the overlap between the issues raised in the IPR petition and in the parallel proceeding in order to evaluate 'concerns of inefficiency and the possibility of conflicting decisions.'" *Fintiv*

Memo, 7; *Fintiv*, 12. Aside from noting the estoppel provisions of 35 U.S.C.

§ 315(e)(2), Petitioner has not provided a *Sotera* stipulation stating that it will not, in the parallel litigation, pursue the same grounds as in the Petition or any grounds that could have reasonably been raised in the petition. Pet., 69. Petitioner, in fact, has not provided any stipulation that would reduce overlap between the issues in this proceeding and the parallel district-court litigation. *Id.* Therefore, the same issues are likely to be litigated in district court, at least up until the time a Final Written Decision is issued, failing to mitigate concerns of inefficiency or conflicting decisions.

Factor 4, therefore, weighs in favor of denial. *Fintiv* Memo, 7 (“If the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial.”); *Fintiv*, 12.

Fintiv factor five: As Petitioner notes, Petitioner is the defendant in the parallel district-court litigation. *See* EX1007. And the plaintiff in the parallel proceeding is the exclusive licensee of the ’823 patent, also a real party-in-interest in this proceeding. *See* Paper 8, 1. This factor, therefore, weighs in favor of discretionary denial. *Fintiv II*, 15.

Fintiv factor six: Director Vidal’s *Fintiv* Memo explains that “[c]ompelling, meritorious challenges are those in which the evidence, if unrebutted in trial,

would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” *Fintiv* Memo, 4. As explained in the arguments above, the Petition fails to establish that multiple claim elements are taught by the prior art. *See* Sections IV-V. Petitioner’s expert largely repeats the Petition verbatim without providing additional analysis or corroborating evidence. *Id.*; *Bytemark*, IPR2022-00624, Paper 9 at 15. Therefore, Factor six favors denial of institution. *Fintiv*, 15.

* * *

At bottom, the same invalidity issues are likely to remain at issue in district court at the same time that a Final Written Decision is due here, and trial is set to begin less than one month later. Institution of trial, therefore, would not provide a “quick and cost-effective alternative[] to litigation,” causing duplicate effort and costs for both parties. *Fintiv* Memo, 3 (citing H.R. Rep. No. 112–98, pt. 1, at 48). The Board should exercise its discretion to deny the Petition in view of the parallel litigation.

VII. CONCLUSION

For at least the foregoing reasons, the Board should deny institution of this proceeding.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

Richard M. Bemben
Registration No. 68,658
Attorney for Patent Owner

Date: December 26, 2024

1101 K Street, NW, 10th Floor
Washington, DC 20005
(202) 371-2600

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

1. This Patent Owner Preliminary Response complies with the type-volume limitation of 14,000 words, comprising 7,070 words, excluding the parts exempted by 37 C.F.R. § 42.24(a)(1).

2. This Patent Owner Preliminary Response complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman font.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

Richard M. Bemben
Registration No. 68,658
Attorney for Patent Owner

Date: December 26, 2024

1101 K Street, NW, 10th Floor
Washington, DC 20005
(202) 371-2600

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

I certify that the above-captioned **PATENT OWNER PRELIMINARY RESPONSE UNDER 37 C.F.R. § 42.107(a)** and associated Exhibits 2001-2006 were served in their entirety on December 26, 2024, upon the following parties via electronic mail:

Jennifer Librach Nall (Lead Counsel)
Nicholas G. Papastavros (Back-up Counsel)
Safraz W. Ishmael (Back-up Counsel)
Joseph Wolfe (Back-up Counsel)
DLA PIPER LLP (US)
Jennifer.nall@us.dlapiper.com
Nick.papastavros@us.dlapiper.com
Safraz.ishmael@us.dlapiper.com
Joseph.wolfe@us.dlapiper.com
DLA-HD-RW@us.dlapiper.com

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX PLLC

/Richard M. Bemben/

Richard M. Bemben
Registration No. 68,658
Attorney for Patent Owner

Date: December 26, 2024

1101 K Street, NW, 10th Floor
Washington, DC 20005
(202) 371-2600