Trials@uspto.gov
571-272-7822

Paper No. 9
Entered: August 24, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

XEROX CORP., ACS TRANSPORT SOLUTIONS, INC., XEROX TRANSPORT SOLUTIONS, INC., CONDUENT INC., AND NEW JERSEY TRANSIT CORP.,
Petitioner,

v.

BYTEMARK, INC.,
Patent Owner.

IPR2022-00624
Patent 10,360,567 B2

Before BENJAMIN D. M. WOOD, BARRY L. GROSSMAN, and JAMES A. TARTAL, *Administrative Patent Judges.*

WOOD, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Xerox Corp., ACS Transport Solutions, Inc., Xerox Transport Solutions, Inc., Conduent Inc., and New Jersey Transit Corp. (collectively, "Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–16 of U.S. Patent No. 10,360,567 B2 (Ex. 1001, "the '567 patent"). Bytemark, Inc. ("Patent Owner") filed a Preliminary Response (Paper 7, "Prelim. Resp.").

We have authority under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a) (2018). Upon considering the Petition, we determine that Petitioner has not shown a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we determine not to grant the Petition.

B. Related Proceedings

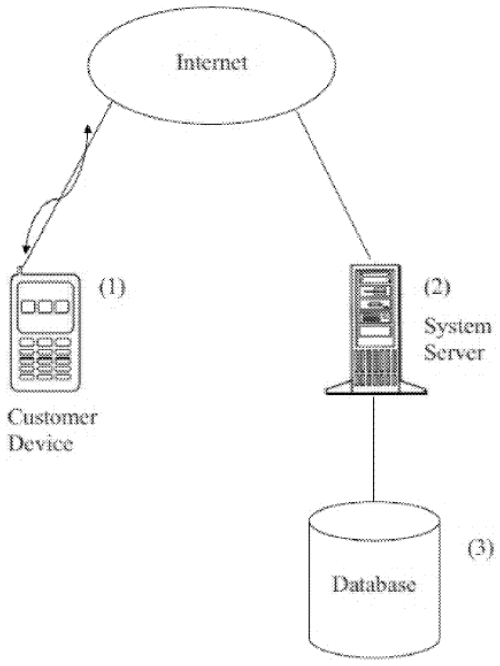
Petitioner states that Patent Owner has asserted the '567 patent against Petitioner in Case No. 17-CV-1803 pending in the United States District Court for the Southern District of New York. Pet. 56; *see* Ex. 1012 (Patent Owner's Third Amended Complaint). Petitioner also seeks *inter partes* review of a related patent, U.S. Patent No. 10,346,764 B2. *See Xerox Corp. et al. v. Bytemark, Inc.*, IPR2022-00621, Paper 1 (Feb. 18, 2022). Another related patent, U.S. Patent No. 8,494,967 ("the '967 patent"), was the subject of a previous *inter partes* review. *See Masabi Ltd. v. Bytemark, Inc.*,

IPR2017-01449, Paper 38 at 4 (PTAB Dec. 3, 2017) (Final Written Decision finding some of the claims of the '976 patent unpatentable).

C. The '567 Patent

The '567 patent issued July 23, 2019 from an application filed May 23, 2014, and is titled "Method and System for Distributing Electronic Tickets with Data Integrity Checking." Ex. 1001, codes (45), (22), (54). Electronic tickets are "procured electronically and stored on the user's device," e.g., a mobile phone. *Id.* at 2:13–14, 30–31.[1] When the ticket is presented, the ticket taker verifies the ticket by inspecting a "visual object that a human can perceive without a machine scanning it." *Id.* at 2:32–34.

Figure 1 of the '567 patent illustrates the "[b]asic architecture" of the electronic ticketing system of the invention, and is reproduced below.



[1] The '567 patent also refers to a "mobile ticket," which we understand to be synonymous with "electronic ticket." Ex. 1001, 11:5–11. The '567 patent defines the term "pass" used in claim 1 as a "mobile ticket." *Id.* at 11:17–18.

As illustrated in Figure 1 of the '567 patent, a customer can use mobile device 1 to purchase a ticket from a service, such as an on-line website, that operates system server 2 and database 3. Ex. 1001, 2:53–54, 3:51–53. The ticketing service sends to the user's device a unique number, referred to as a "token," that is also stored in the system database. *Id.* at 2:54–56. "Ticket holders that have purchased tickets have a data record in the system database that contains the unique token associated with the ticket and other relevant information, including the venueID [sic] and an identifier identifying the specific show the ticket is for." *Id.* at 4:5–9. When the time comes to present the ticket, the venue can select what visual indicator will be used as the designated validation visual object. *Id.* at 2:56–59. As the '567 patent explains:

> The user can then request the validation visual object. The user's device will have an application that launches a user interface. The user can select "validate" or some other equivalent command to cause the application to fetch and download from the ticketing system a data object referred to herein as a ticket payload, which includes a program to run on the user's device. . . . As a result, the application transmitted to the user's device is previously unknown to the user and not resident in the user's device. At that point the user's device can execute the program embodied in the ticket payload, which causes the validation visual object to be displayed on the user's device. The ticket taker knows what the validating visual object is and simply looks to see that the user's device is displaying the correct visual object.

Id. at 2:59–3:7.

In addition to using a validating visual object to assist in validating the electronic ticket when the ticket is presented, the '567 patent teaches "data integrity checking . . . to be sure that the pass data and the software

managing that pass data on the user's device has [sic] not been altered improperly." Ex. 1001, 13:21–23. For example, "if the pass data or other data is unrecognized by the server or is inconsistent with a separate locally generated key on the device, there is an anomaly." *Id.* at 13:24–26. "When these anomalies are detected the tickets and user account are locked down to stop fraudulent activity." *Id.* at 13:26–28; *see id.* at 4:11–16 (teaching that an application on the user's mobile device "fetches the stored ticket token and transmits that token to the system," which "looks up the token to check that the token is valid for the upcoming show. If the token is valid, then the system transmits back to the device a ticket payload."). The '567 patent further teaches that:

> If such suspicious activity is detected, the user account is flagged for further investigation if necessary, for example, by setting a status bit in a data record associated with the user to indicate a fraudulent transaction has occurred. When this logical condition is established, any passes that were previously locked to the device will no longer be available on any device. That is, the user's account data on the back office server is set so that each purchased pass has a status bit indicating that it is unavailable for use for security reasons.

Id. at 14:5–14.

D. The Challenged Claims

Petitioner challenges claims 1–16 of the '567 patent. Pet. 1. Claim 1 is the sole independent claim, and is reproduced below: [2]

[2] Claim 1 has been reformatted slightly to include Petitioner's limitation designations and for clarity.

1. [1p] A mobile ticketing system for detecting fraudulent activity of tickets using data integrity, comprising:

[1a] a mobile device in communication with a server;

[1b] a server adapted to receive authentication data for a user account from the mobile device via a data network, and

[1c] transmit data in the form of a ticket payload that contains code to the mobile device embodying a pass,

[1d] wherein the pass includes a validation visual object that a ticket taker can rely on as verification of the pass without using a scanning device and wherein the validation visual object is not accessible until a time selected to be close to the point in time where the ticket has to be presented;

[1e] wherein the server is further configured to:

receive the pass with the data from the mobile device and determine if there is any mismatch in the received data of the pass by comparing the received data with the data transmitted;

block the user account in an event of the received data is mismatched with the transmitted data and detected as a fraudulent activity; and

[1f] determine the occurrence of the fraudulent activity associated with the user account in connection with the mobile ticketing system and

store in a data record associated with the account a data value indicating the fraudulent activity and

[1g] in dependence on the data value indicating fraudulent activity, the code in the ticket payload makes the pass, including the validation visual object, no longer available on the device.

Ex. 1001, 17:50–18:12.

E. Asserted Grounds of Unpatentability

Petitioner contends that the challenged claims are unpatentable based on the following specific grounds (Pet. 12):

No.	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1	1–6, 8–10, 12–16	§ 103	Terrell,[3] Ritter[4]
2	7	§ 103	Terrell, Ritter, Masahiro[5]
3	11	§ 102	Terrell, Ritter, Laudermilch[6]

In support of its proposed grounds, Petitioner relies on the Declaration of Dr. Mark Jones (Ex. 1003).

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner asserts that one of ordinary skill in the art at the time of the invention "would have at least a Bachelor of Science Degree in Computer Science, Computer Engineering, or similar educational background, or equivalent on-the-job training, including approximately three years of experience in developing mobile applications." Pet. 11 (citing Ex. 1003

[3] WO 2009/141614 A1 (pub. Nov. 26, 2009) (Ex. 1008).

[4] US 7,114,179 B1 (Sept. 26, 2006) (Ex. 1011).

[5] JP 2006-201997A (pub. Aug. 3, 2006) (Ex. 1010). The first named inventor of this reference is Yukimi Watakabe. *Id.* code (72). Nonetheless, for purposes of this opinion, we use Petitioner's appellation.

[6] U.S. 8,259,568 B2 (Sept. 4, 2012) (Ex. 1009).

¶ 14). Patent Owner contends that "a POSITA in the timeframe of the invention would have a bachelor's degree in computer engineering or similar discipline and approximately two years of experience designing mobile applications." Prelim. Resp. 6.

The parties' positions are largely in agreement, differing only in the proposed length of experience in developing mobile applications. Because the outcome of this case would not differ under either definition, we need not resolve the difference. Further, we presume that the cited prior art references reflect the level of ordinary skill at the time of the invention. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

B. Claim Construction

We construe the claims "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005). Any special definitions for claim terms must be set forth in the Specification with reasonable clarity, deliberateness, and precision. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioner and Patent Owner agree that no claim term requires express construction, and indeed neither party offers constructions for any claim term. Pet. 13–14; Prelim. Resp. 6. In the absence of any proposed constructions, and as we have determined not to institute *inter partes* review, we decline to expressly construe any claim term in the first instance.

Accordingly, we proceed with the understanding that each term should be accorded its plain and ordinary meaning.

C. Ground 1: Claims 1–6, 8–10, 12–16—Obvious over Terrell and and Ritter or the knowledge of a POSITA

Petitioner alleges that claims 1–6, 8–10, and 12–16 would have been obvious over Terrell and "Ritter or the [k]nowledge of a POSITA." Pet. 19–45. Claim 1 is independent, and claims 2–6, 8–10, and 12–16 ultimately depend from claim 1. Ex. 1001, 17:50–19:12.

1. Terrell

Terrell describes methods and systems for electronic ticketing in which the electronic ticket contains an "eye-readable" image displayed by a mobile device "for inspection purposes," and machine-readable code defining at least a unique ticket number that can be used to authenticate the ticket. Ex. 1008, 2:7–13; *id.* at 4:18–20 (same). Figure 1 depicts Terrell's system, and is reproduced below:

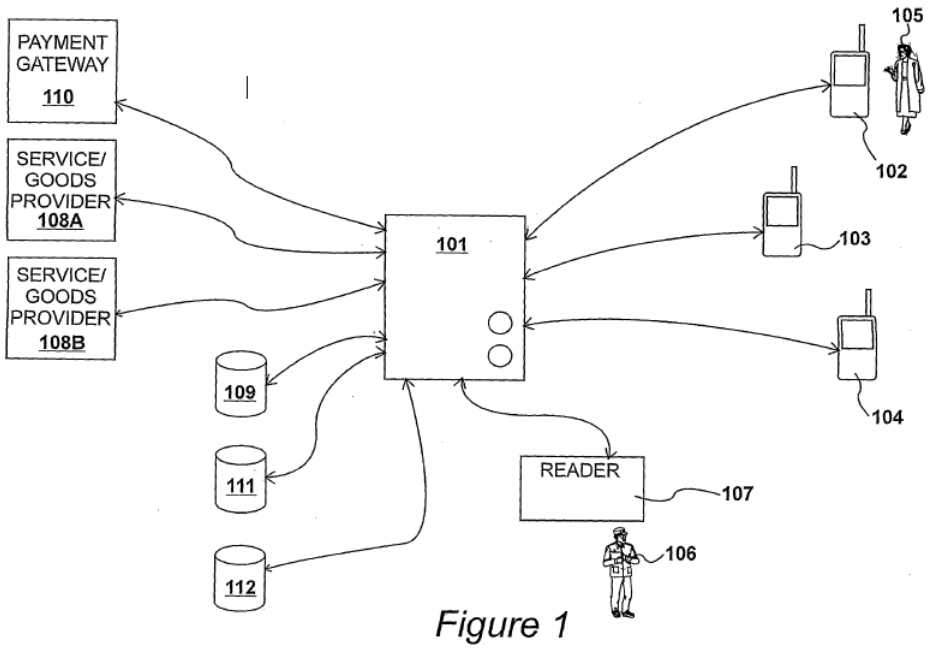


Figure 1

As depicted in Figure 1 of Terrell, a customer, such as user 105, may purchase an electronic ticket from service/goods provider 108A or 108B (e.g., a rail service provider) via wireless application server 101 using a mobile device such as mobile phone 102. Ex. 1008, 4:5–29. Server 101 provides the ticket, with a unique ticket number, to mobile device 102, and stores details of the ticket, including the ticket number, in verification database 111. *Id.* at 5:1–4, Figs. 7, 11. The ticket number is displayed on the ticket and also converted to a barcode displayed on the ticket, so the barcode may be read and compared to the displayed ticket number, "thus providing a very simple check of the ticket's authenticity." *Id.* at 14:5–9, Fig. 11. Further, "[w]here a database of the unique ticket numbers is available, this ticket number can also be checked against a database to ensure that it is valid." *Id.* at 14:9–11. Such an inspection of the ticket number may also be logged on verification database 111 by server 101. *Id.* at 14:11–13. Thus, "if two separate uses of the ticket are logged, this may be identified by the server 101 and the ticket's further use may be blocked." *Id.* at 14:13–15. "Alternatively, the purchaser of the ticket could be blocked from further use of the system or pursued in respect of their potential fraud." *Id.* at 14:15–17.

2. Ritter

Ritter "relates to a method and a system for ordering, loading and using admission tickets for access to access-controlled devices," such as "means of public transportation, secured buildings, halls or exhibition grounds." Ex. 1011, 1:4–6, 2:52–54. Figure 1 of Ritter depicts the described invention, and is reproduced below:

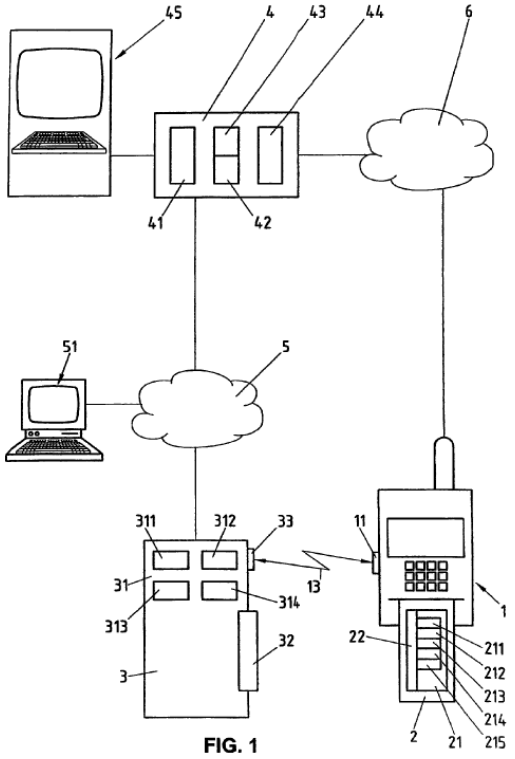


FIG. 1

As illustrated in Figure 1 of Ritter, a user may order an admission ticket from reservation center 4 by means of mobile communications terminal 1, e.g., a "mobile radio telephone," using mobile network 6. Ex. 1011, 5:5–14, 51–53. Reservation center 4 then transmits the admission ticket over network 6 to the user's mobile terminal; the ticket may include a ticket number, the location of the event for which access is sought, and "special codes which indicate a special service" and "are processed in accordance with the special code according to a special procedure." *Id.* at 5:62–6:1, 6:17–21. The transmitted ticket is received by mobile terminal 1 and stored in memory module 21, e.g., SIM card 2. *Id.* at 4–7. Admission tickets can be loaded "in the form of small programs applications, so-called applets on chipcards 2" (in particular SIM card 2). *Id.* at 6:13–14, 30–32. According to Ritter, "such applets . . . can be automatically erased during marking as used." *Id.* at 6:34–35.

To use the admission ticket, mobile terminal 1, with the ticket stored in its memory, is placed near reading device 31 of access-controlled service device 3. Ex. 1011, 6:37–41. Ticket data, such as the ticket number, is transmitted to reading device 31, which compares the data to current access data, and access is authorized based on the comparison. *Id.* at 7:13–41. Ritter teaches that "access tickets that have been used for authorized access to a respective access-controlled device 3, can be marked as used, for example through updating of the access data stored in the reservation center 4, which has been informed by the reading device 31." *Id.* at 7:42–46.

3. Principles of Law

"A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in [35 U.S.C. § 102], if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." 35 U.S.C. § 103. Obviousness is a question of law based on underlying findings of fact. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). The underlying factual considerations "include the scope and content of the prior art, the differences between the prior art and the claimed invention, the level of ordinary skill in the art, and any relevant secondary considerations" of non-obviousness, including commercial success of the patented product or method, a long-felt but unmet need for the functionality of the patented invention, and the failure of others who have unsuccessfully attempted to accomplish what the patentee has achieved. *Id.* at 17–18. The obviousness analysis should not be conducted "in a narrow, rigid manner,"

but should instead focus on whether a claimed invention is merely "the result[] of ordinary innovation," which is not entitled to patent protection. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

4. Discussion

Sole independent claim 1 requires the server to be configured to, *inter alia*, "store in a data record associated with the user account a data value indicating the fraudulent activity." Ex. 1001, 18:6–8. Regarding this limitation, Petitioner notes Terrell's teaching that "after fraudulent activity is detected, 'the purchaser of the ticket could be blocked from further use of the system or pursued in respect of their potential fraud.'" Pet. 28 (quoting Ex. 1008, 14:15–17). Petitioner asserts that "[a] POSITA would understand that such a blocking would require recording the blocking in a data record associated with that user's account." *Id.* (citing Ex. 1003 ¶ 54). Petitioner also contends that "[a] POSITA would find it obvious that blocking the account of the purchaser from further use of the system would include storing a data value indicating the fraudulent activity in a data record associated with the user account, for example, in Terrell's registration details database 112 or its database 111." *Id.* Further, according to Petitioner:

> This is especially true in light of Terrell's teaching that "if two tickets were found to have the same unique ticket number, the scanner would be configured to provide an alert to the inspector," and that "all barcode scan records may be centrally collated and analyzed to identify potential fraudulent use."

Id. at 28–29 (quoting Ex. 1008, 14:30–15:3; citing Ex. 1003 ¶ 54).

Patent Owner responds, *inter alia*, that "[t]he Petition fails to show that the Terrell/Ritter combination teaches or suggests storing a data value indicating fraudulent activity." Prelim. Resp. 8. Patent Owner asserts that

"Terrell, at most, teaches blocking a ticket purchaser from further use of the Terrell system based on potential fraud." *Id.* at 8–9. Patent Owner contends that "[t]here is no indication anywhere in Terrell . . . that this is achieved using a data value indicating fraudulent activity, as opposed to some other manner of blocking a user, such as deleting the user's account or reporting the user for fraud." *Id.* at 9. Patent Owner further submits that Petitioner's argument "that a POSITA's 'understanding' would find this limitation obvious . . . is an improper attempt to use a POSITA's common knowledge to supply a wholly missing claim limitation without evidentiary support or satisfying the 'searching' standard required by the Federal Circuit." *Id.* Instead, according to the Patent Owner, Petitioner's "entire analysis consists of conclusory statements." *Id.* at 10.

Petitioner does not allege, and we do not find, that Terrell expressly teaches a server configured to "store in a data record associated with the user account a data value indicating the fraudulent activity." Pet. 28. Instead, Petitioner relies on Terrell's teaching that "the purchaser of the ticket could be blocked from further use of the system or pursued of their potential fraud," and asserts that: (1) such a blocking would "require" recording the blocking in a data record associated with the user's account; and (2) a POSITA "would find it obvious" that "blocking the account of the purchaser" would including "storing a data value indicating the fraudulent activity in a data record associated with the user account." *Id.* But Petitioner does not provide sufficient evidence or persuasive reasoning to support either of these assertions.

First, Terrell does not teach "blocking the *account* of the purchaser," as the second assertion noted above implies. Rather, Terrell teaches

blocking the *purchaser*. Ex. 1008, 14:15–17. Thus, it is far from clear that blocking the purchaser would "require" recording the blocking in a record in the purchaser's account, as opposed to—as Patent Owner suggests (Prelim. Resp. 9)—deleting the purchaser's account altogether.

Petitioner's only evidence in support of its assertion that blocking the purchaser would require recording the blocking in a record in the user's account is the opinion of its Declarant, Dr. Jones. Pet. 28 (citing Ex. 1003 ¶ 54). We have reviewed this excerpt from Dr. Jones' declaration and note that it merely repeats, *verbatim*, the conclusory assertion for which it is offered to support. *See* Ex. 1003 ¶ 54 (Dr. Jones declaring that "[a] POSITA would understand that such a blocking would require recording the blocking in a data record associated with that user's account."). Dr. Jones does not cite to any additional supporting evidence or provide any technical reasoning to support his statement. Thus, the cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."); *Upjohn Co. v. Mova Pharm. Corp.*, 225 F.3d 1306, 1311 (Fed. Cir. 2000) ("Lack of factual support for expert opinion to factual determinations, however, may render the testimony of little probative value in a validity determination.") (quoting *Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 281, 294 (Fed. Cir. 1985)); *Carella v. Starlight Archery & Pro Line Co.*, 804 F.2d 135, 138 (Fed. Cir. 1986) ("Although in some circumstances unsupported oral testimony can be sufficient to provide prior knowledge or use, it must be regarded with suspicion and subjected to close scrutiny.").

Similarly, Petitioner's only support for the assertion that "[a] POSITA would find it obvious that blocking the account of the purchaser from further use of the system would including storing a data value indicating the fraudulent activity in a data record associated with the user account" is Dr. Jones' Declaration. Pet. 28.[7] Again, however, Dr. Jones offers only a *verbatim* restatement of the assertion being supported, without any supporting evidence or technical reasoning. Neither Petitioner nor Dr. offers a construction for the terms "data value" or "data record," for example.

This is particularly problematic in cases where, like here, expert testimony is offered not simply to provide a motivation to combine prior-art teachings, but rather to supply a limitation missing from the prior art. *See KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007) (stating that a "factfinder . . . must be cautious of arguments reliant upon *ex post* reasoning"); *Arendi S.A.R.L. v. Apply, Inc.*, 832 F.3d 1355, 1361–62 (Fed. Cir. 2016) (holding that reliance on common sense in an obviousness analysis is "typically invoked to provide a known motivation to combine, not to supply a missing claim limitation") (emphasis omitted). Although doing so might be permissible when "the limitation in question [is] unusually simple and the technology particularly straightforward" (*id.* at 1362), Petitioner has not alleged that to be the case here, much less provided support for such an allegation.

[7] Again, Terrell does not teach blocking the *account* of the ticket purchaser (but rather teaches blocking the purchaser itself), so even if accepted as true this assertion would not necessarily support a finding that Terrell teaches the limitation in question.

Finally, we are not persuaded that Terrell's teachings that "if two tickets were found to have the same unique ticket number, the scanner would be configured to provide an alert to the inspector," and "all barcode scan records may be centrally collated and analyzed to identify potential fraudulent use," supports a finding that Terrell teaches the limitation in question. Petitioner does not explain how it is "especially true," in light of these statements, that a POSITA would find it obvious that blocking the account of the purchaser from further use of the system would include storing a data value indicating the fraudulent activity in a data record associated with the user account. *See* Pet. 28–29. These statements do not, on their face, refer to blocking or modifying a user account, much less blocking a user. The only evidence offered to support a connection between these statements and the limitation in question is the declaration testimony of Dr. Jones, to which, for the same reasons discussed above, we give little weight.

For the above reasons, we are not persuaded that Petitioner has sufficiently shown that claim 1, as well as dependent claims 2–6, 8–10, and 12–16, would have been obvious over Terrell and Ritter. Therefore, we are not persuaded that Petitioner is reasonably likely to prevail with respect to at least one of the claims challenged in the Petition, and decline to institute *inter partes* review of these claims.

D. Remaining Grounds

Petitioner additionally contends that (1) claim 7 would have been obvious over Terrell, Ritter, and Masahiro; and (2) claim 11 would have been obvious over Terrell, Ritter, and Laudermilch. Pet. 45–51. As claims 7 and 11 depend from claim 1, these proposed grounds of unpatentability

rely on the combination of Terrell and Ritter rendering unpatentable claim 1. Ex. 1001, 18:27–37, 52–56; Pet. 45–51. Therefore, because we are not persuaded that Petitioner is reasonably likely to prevail in showing that claim 1 would have been obvious over Terrell and Ritter, we decline to institute inter partes review of claims 7 and 11.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not shown that there is a reasonable likelihood that it would prevail with regard to at least one of the claims challenged in the Petition. Accordingly, we decline to institute *inter partes* review. 35 U.S.C. § 314(a).

IV. ORDER

For the reasons given, it is

ORDERED that the Petition for *Inter Partes* Review is denied.

PETITIONER:

Ashley N. Moore
Scott W. Hejny
McKool Smith P.C.
amoore@mckoolsmith.com
shejny@mckoolsmith.com

PATENT OWNER:

James T. Carmichael
Minghui Yang
Carmichael IP, PLLC
jim@carmichaelip.com
mitch@carmichaelip.com