Trials@uspto.gov
571-272-7822

Paper 12
Entered: February 28, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2021-01448
Patent 10,698,989 B2

Before THU A. DANG, KEVIN F. TURNER, and DAVID C. McKONE, *Administrative Patent Judges.*

MCKONE, Administrative Patent Judge.

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

I. INTRODUCTION

A. Background and Summary

Samsung Electronics America, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–9 of U.S. Patent No. 10,698,989 B2 (Ex. 1001, "the '989 patent"). Pet. 5. Proxense, LLC ("Patent Owner") filed a Preliminary Response (Paper 10, "Prelim. Resp.").

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2016); 37 C.F.R. § 42.4(a) (2020). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), 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." For the reasons explained below, we decline to institute an *inter partes* review of the '989 patent.

B. Related Matters

The parties advise us that Patent Owner has asserted the '989 patent and four other patents against Petitioner in *Proxense, LLC v. Samsung Electronics, Co., Ltd.*, No. 6.21-CV-00210 ("the Texas case"). Pet. 3; Paper 5, 2. Petitioner also advises us that it has filed petitions for *inter partes* review challenging the other four patents asserted in the Texas case, including U.S. Patent No. 8,352,730 ("the '730 patent"), a parent of the '989 patent (*see* Ex. 1001, code (63)). Pet. 3.

C. The '989 Patent

The '989 patent relates to computerized authentication responsive to biometric verification of a user being authenticated. Ex. 1001, 1:35–38. Figure 2, reproduced below, illustrates an example:

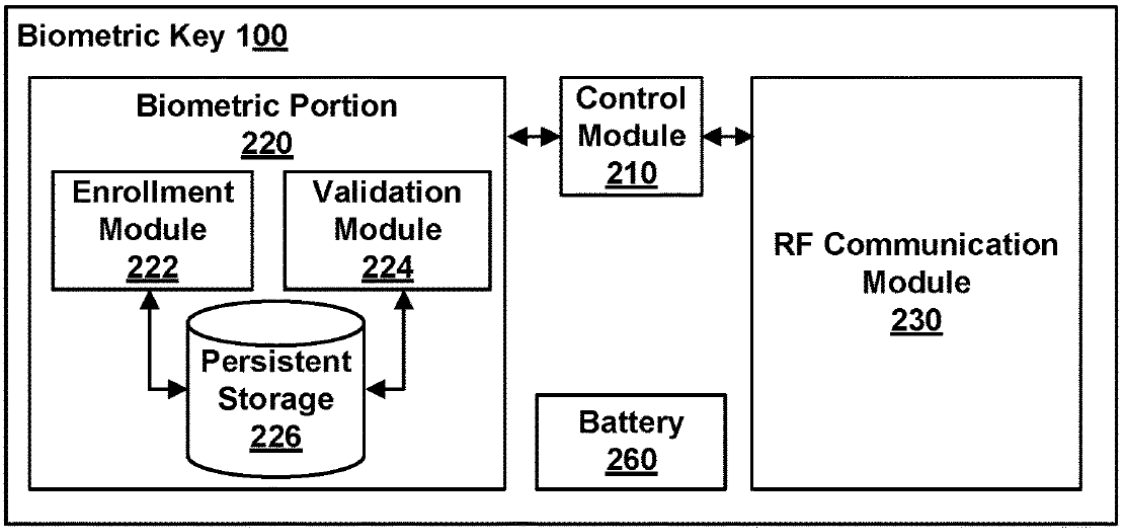

FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key. *Id.* at 3:47–49. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at 5:18–21, 5:31, 5:40–42. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can provide a code to biometric key 100. *Id.* at 5:22–26. The code is stored in persistent storage 226. *Id.* at 5:57–59. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user's fingerprint and compares the scanned data to the stored

fingerprint to determine whether the scanned data matches the stored data. *Id.* at 5:27–37.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below:

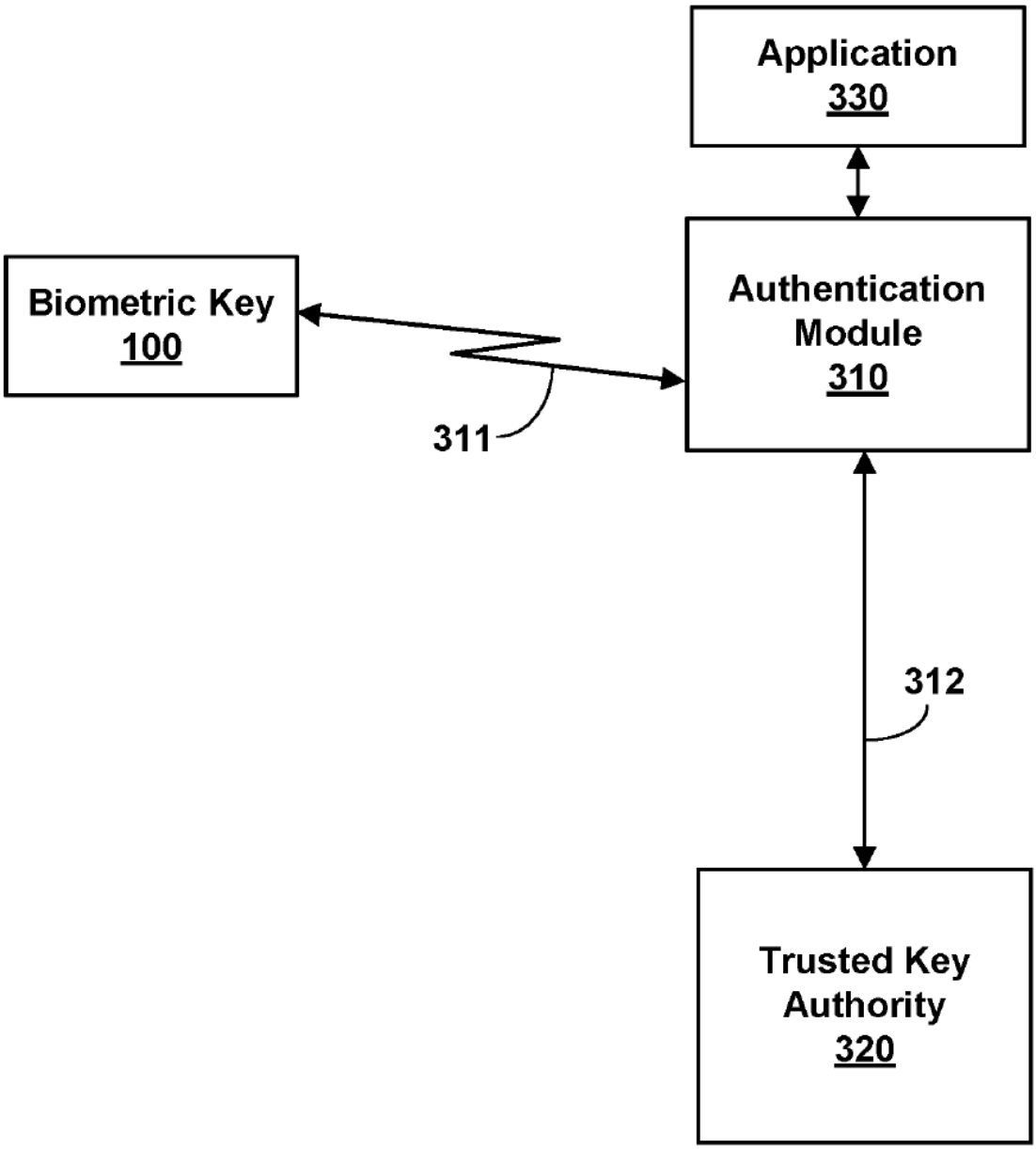

Figure 3 is a block diagram of a system for providing authentication information for a biometrically verified user. *Id.* at 3:30–52. Authentication module 310 is coupled to biometric key 100 via line 211 (a wireless

medium) and with trusted key authority 320 via line 312 (a secure data network such as the Internet). *Id.* at 6:23–27. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at 6:27–33. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at 6:33–37; *see also id.* at 6:61–67 ("In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. . . . In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key"). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at 6:37–40.

"Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like." *Id.* at 6:41–47. Trusted key authority 320 can be operated by an agent such as a government official, a notary, an employee of a third party, or other form of witness, and can follow standardized procedures such as requiring a state issued drivers license or federally issued passport to establish the true identity of the user. *Id.* at 7:58–64.

Claim 1, reproduced below,[1] is illustrative of the claimed subject matter:

1. A method comprising:

[1A] receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;

[1B] persistently storing biometric data and the ID code on the smartphone, [1C] wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;

[1D] receiving, at the smartphone, scan data from a biometric scan using the smartphone;

[1E] comparing, using the smartphone, the scan data to the biometric data;

[1F] determining whether the scan data matches the biometric data; and

[1G] responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority, [1H] a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code, [1I] wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

[1] We add bracketed numbering corresponding to the numbering Petitioner uses in the Petition. *See, e.g.*, Pet. iv.

D. Evidence

Petitioner relies on the references listed below.

Reference		Date	Exhibit No.
Scott	WO 99/56429	Nov. 4, 1999	1005
Lapsley	US 2001/0000535 A1	Apr. 26, 2001	1007
Berardi	US 7,239,226 B2	July 3, 2007	1010
Shreve	US 2002/0109580 A1	Aug. 15, 2002	1012
Kinoshita	US 2003/0055792 A1	Mar. 20, 2003	1013

Petitioner also relies on the Declaration of Andrew Wolfe, Ph.D. (Ex. 1003, "Wolfe Decl.").

E. The Asserted Grounds

Petitioner asserts the following grounds of unpatentability (Pet. 5):

References	Basis	Claim(s) Challenged
Scott, Lapsley	§ 103(a)[2]	1–9
Berardi, Shreve, Kinoshita	§ 103(a)	1–9

II. DISCRETIONARY DENIAL

Institution of *inter partes* review is discretionary. *See Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2140 (2016) ("[T]he agency's decision

[2] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103. Because the '989 patent has an effective filing date before the effective date of the relevant provision of the AIA, we cite to the pre-AIA version of § 103.

to deny a petition is a matter committed to the Patent Office's discretion."); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) ("[T]he PTO is permitted, but never compelled, to institute an IPR proceeding."); 35 U.S.C. § 314(a).

Patent Owner contends that we should deny the Petition based on the advanced state of the Texas case, pursuant to *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential). Prelim. Resp. 4–6. Because we deny the Petition for the reasons given below, we do not reach whether we should exercise our discretion to deny the Petition based on *Fintiv*.

III. ANALYSIS

A. Claim Construction

We construe a claim

> 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) (2019); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Petitioner submits that no express constructions of any claim terms are necessary to resolve the parties' dispute and that the claim terms should be given their plain and ordinary meaning. Pet. 7–8. According to Patent Owner, however, Petitioner argued in the Texas case that a "third-party" is "an entity with a responsibility separate from executing the transaction

itself." Prelim. Resp. 2 (quoting Ex. 2001 (Petitioner's Opening Claim Construction Brief in the Texas case), 7).

In the Texas case, Petitioner argued, as to the term "third-party trusted authority," that no construction was needed and that "[t]he intrinsic evidence does not suggest a party or component numbered after a second party." Ex. 2001, 6–7. This was in response to its articulation of Patent Owner's position, namely, that a "third-party trusted authority" is "[a] third component that provides a second level of authentication." *Id.* at 6.[3]

However, as to Petitioner's view of how a skilled artisan would have understood this term, Petitioner further argued that "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation," and that "[t]he applicant emphasized the prior art 'disclose[d] two parties: the user and the institution.'" *Id.* at 7 (quoting remarks made by the applicant for the '730 patent, a parent of the '989 patent, accompanying an amendment and addressing the same claim term (alterations by Petitioner)). Petitioner argued that "the intrinsic evidence suggests 'third party' relates to a specific class of entity occupying the aforementioned particular relationship." *Id.* Petitioner then pointed out that "the specification explains the agent for the trusted authority 'can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.'" *Id.* (citing description in the '730 patent

[3] In its responsive brief, Patent Owner changed its position to "[n]o construction needed" and stated that it "no longer seeks to submit this term for construction." Ex. 2002, 12. The Texas court's Claim Construction Order does not include a construction for this term. Ex. 3001.

corresponding to Ex. 1001, 7:58–61). According to Petitioner, "[t]his 'witness' role further aligns with prosecution history where the applicant explained 'sending a code to a receiver of a **door that the user is trying to access**' does not satisfy the 'third party' limitation." *Id.* (quoting an amendment in the '730 patent file history).

Petitioner further offered expert testimony to support an argument that "[c]ommon industry use of 'trusted third party' identifies 'third party' as an entity with a responsibility separate from executing the transaction itself." *Id.* at 7–8 (citing a declaration of Seth James Nielson (Ex. 2003) ¶¶ 70–74 and a book, Cryptographic Libraries for Developers).[4] Dr. Nielson appears to best articulate the distinction Petitioner was drawing between a third component and a third entity: "the prosecution history, and common industry usage all suggest a 'third party' refers to an entity outside of the transaction or a witness thereto rather than a 'third component.'" Ex. 2003 ¶ 74.

In light of Petitioner's arguments in the Texas case, Patent Owner contends that the parties "agree that a 'third-party trusted authority' is an institution or entity that is outside of the multi-party system (user and application or vendor) that is being authenticated." Prelim. Resp. 3.

We agree with Patent Owner. The plain meaning of "third-party trusted authority" suggests an entity or party separate from the principal parties to a transaction. *See e.g.*, THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004) ("third party n. . . . 2. One other than the principals involved in a transaction.") (Ex. 3002).

---

[4] Neither Petitioner nor Patent Owner has included in our record the file history of the '730 patent or the Cryptographic Libraries for Developers book.

This is consistent with the description in the Specification. For example, Figure 3, reproduced above, depicts trusted key authority 320 as an entity separate from biometric key 100, authentication module 310, and application 330. As the Specification states, "[t]rusted key authority 320 is a third-party authority that is present in some embodiments to provide enhanced security." Ex. 1001, 6:59–61. Examples of trusted key authorities include "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at 7:56–61. Petitioner's citations to the applicant's statement during the prosecution of the parent '730 patent are also consistent with a third-party trusted authority being an entity separate from the principal parties to a transaction, as is the Declaration of Dr. Nielson. Ex. 2001, 6–8; Ex. 2003 ¶¶ 70–74. Thus, we construe "third-party trusted authority" to mean a trusted authority that is an entity separate from the parties to a transaction.

Patent Owner also argues that "a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code" (claims 1, 5) and "a transaction is completed responsive to successful authentication of the ID code" (claim 7) require a message to be sent from the third-party trusted authority. Prelim. Resp. 3. We need not further construe this term to resolve the parties' dispute. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that "we need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Based on the record before us, we do not find it necessary to provide express claim constructions for any other terms.

B. Obviousness of Claims 1–9 over Scott and Lapsley

Petitioner contends that claims 1–9 would have been obvious over Scott and Lapsley. Pet. 19–37. For the reasons given below, Petitioner has not made a sufficient showing.

A claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are "such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." We resolve the question of obviousness on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) if in evidence, objective evidence of nonobviousness, i.e., secondary considerations.[5] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

1. Level of Skill in the Art

Petitioner contends that a person of ordinary skill in the art "would have had a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent)" and "that more education could compensate for less experience and vice versa." Pet. 4. Patent Owner does not challenge Petitioner's proposed level of skill or propose an alternative. For purposes of this Decision, we adopt Petitioner's proposed level of skill.

[5] The record does not include allegations or evidence of objective indicia of nonobviousness.

2. Scope and Content of the Prior Art

a) Overview of Scott

Scott describes "a portable personal identification device for providing secure access to a host facility," in which the device "includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and provides a biometric signal indicative thereof." Ex. 1005, 2:5–8. Figure 1, reproduced below, illustrates an example:

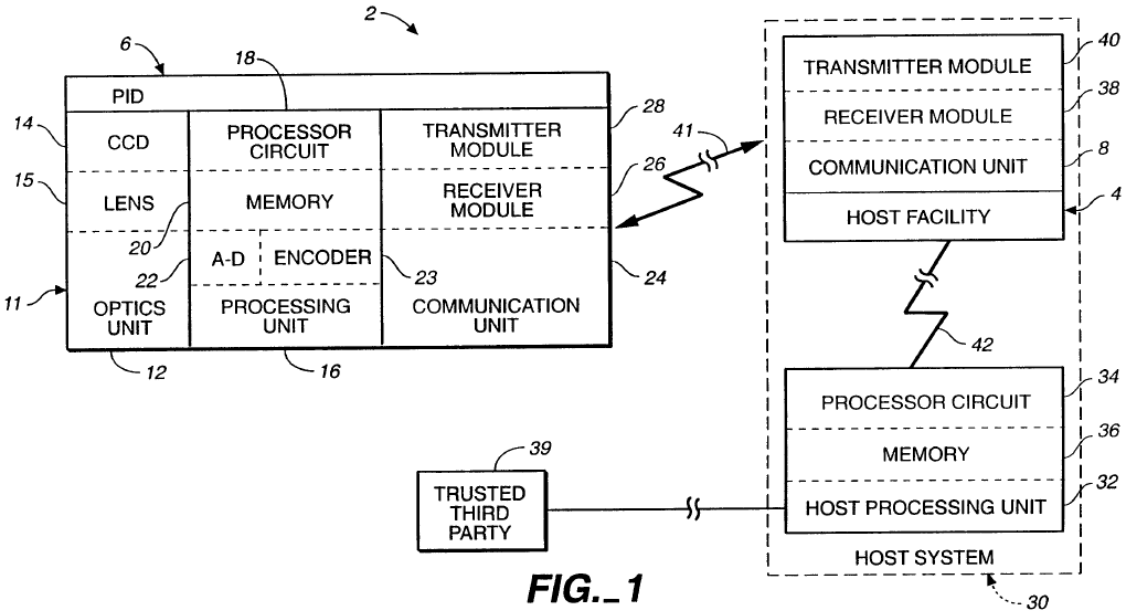

FIG._1

Figure 1 is a block diagram of security system 2 that provides access to host facility 4 (e.g., a bank, store, military base, computer system, automobile, home security system, or gate). *Id.* at 10:1, 10:24–28.

A registered person carries battery powered personal identification device (PID) 6 (e.g., similar in size to a hand-held pager), which includes biometric sensor 11. *Id.* at 10:28–11:5. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. *Id.* at 11:11–13. The owner of PID 6 enrolls into the unit by scanning a finger using biometric sensor 11 to create an image that is stored as the fingerprint template in memory 20. *Id.* at

11:14–20, 15:30–16:6. PID 6 communicates wirelessly via transmission signal 41 with host facility 4. *Id.* at 12:14–16.

Host facility 4 is part of host system 30 (e.g., a bank ATM system or point of sale system), which also includes host processing unit 32. *Id.* at 11:30–12:2. "Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42." *Id.* at 12:3–5. Memory 36 stores ID codes of enrolled individuals who have registered with host system 30. *Id.* at 12:6–7.

Figure 7 is reproduced below:

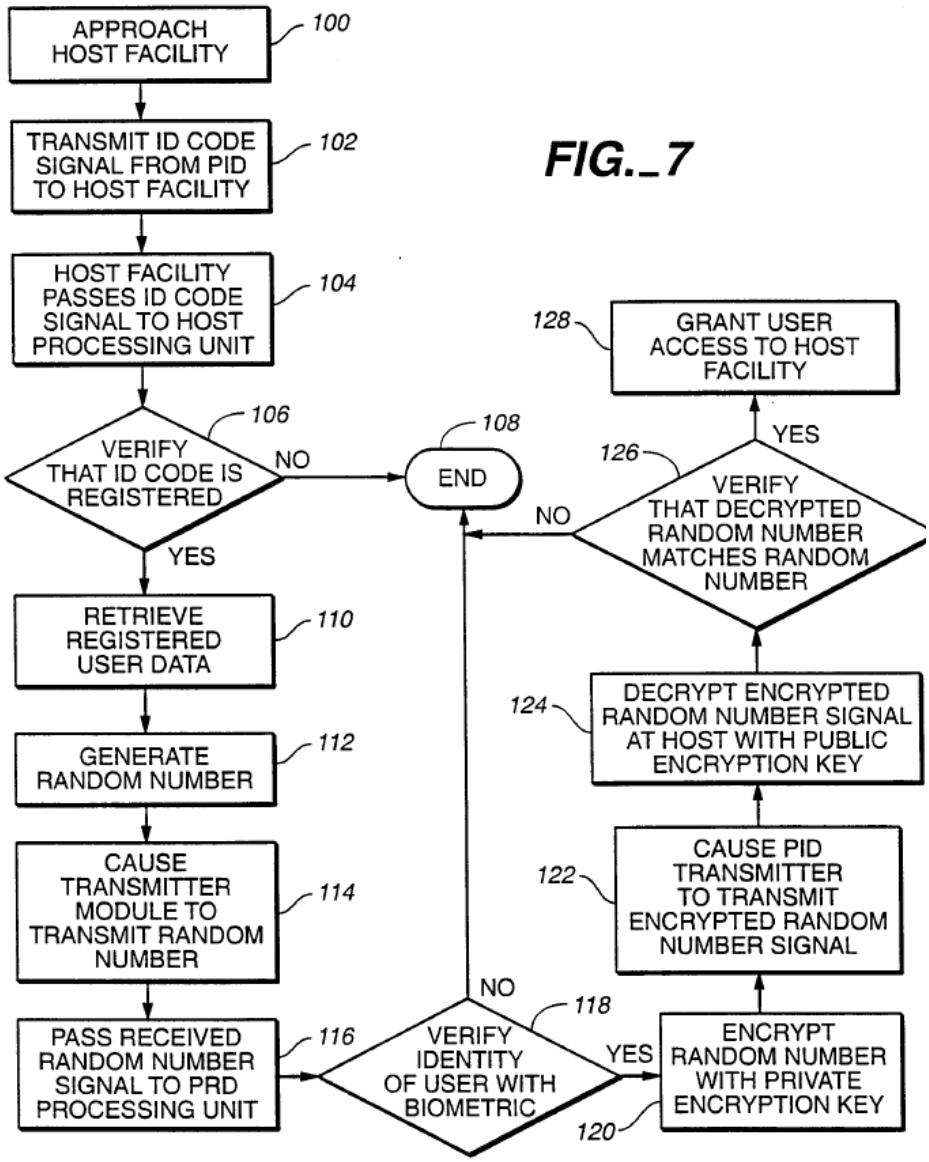

FIG._7

Figure 7 is a flow diagram of a method of accessing a host facility with a personal identification device. *Id.* at 10:13–14.

A user with PID 6 approaches host facility 4 (e.g., an ATM machine) and transmits the ID code to host receiver module 38, which passes it to host processing unit 32. *Id.* at 17:20–27 (steps 100–104). Host processing unit 32 verifies that the received ID code represents a registered ID code and, if so, the account or user information is located. *Id.* at 17:27–30 (steps 106, 110). Host processing unit 32, via transmitter module 40, sends a random

number to PID 6, in response to which PID 6 performs a user verification. *Id.* at 18:1–4 (steps 112–118). PID 6 verifies the user's fingerprint when the user places their finger on platen 15 of biometric sensor 11 by comparing the fingerprint signal to the stored fingerprint template. *Id.* at 16:19–29. If PID 6 successfully verifies the user's fingerprint, PID 6 encrypts the random number and sends it back to host processing unit 32, which decrypts the random number and verifies that it matches the random number it sent to PID 6. *Id.* at 18:5–14 (steps 120–126). If the random number is a match, host processing unit 32 grants the user access to host facility 4. *Id.* at 18:14–15 (step 128).

b) Overview of Lapsley

Lapsley describes "a system and method of using biometrics for processing electronic financial transactions such as on-line debit, off-line debit and credit transactions without requiring the user to directly use or possess any man-made tokens such as debit or credit cards or checks." Ex. 1007 ¶ 2. Figure 2, reproduced below, illustrates an example:

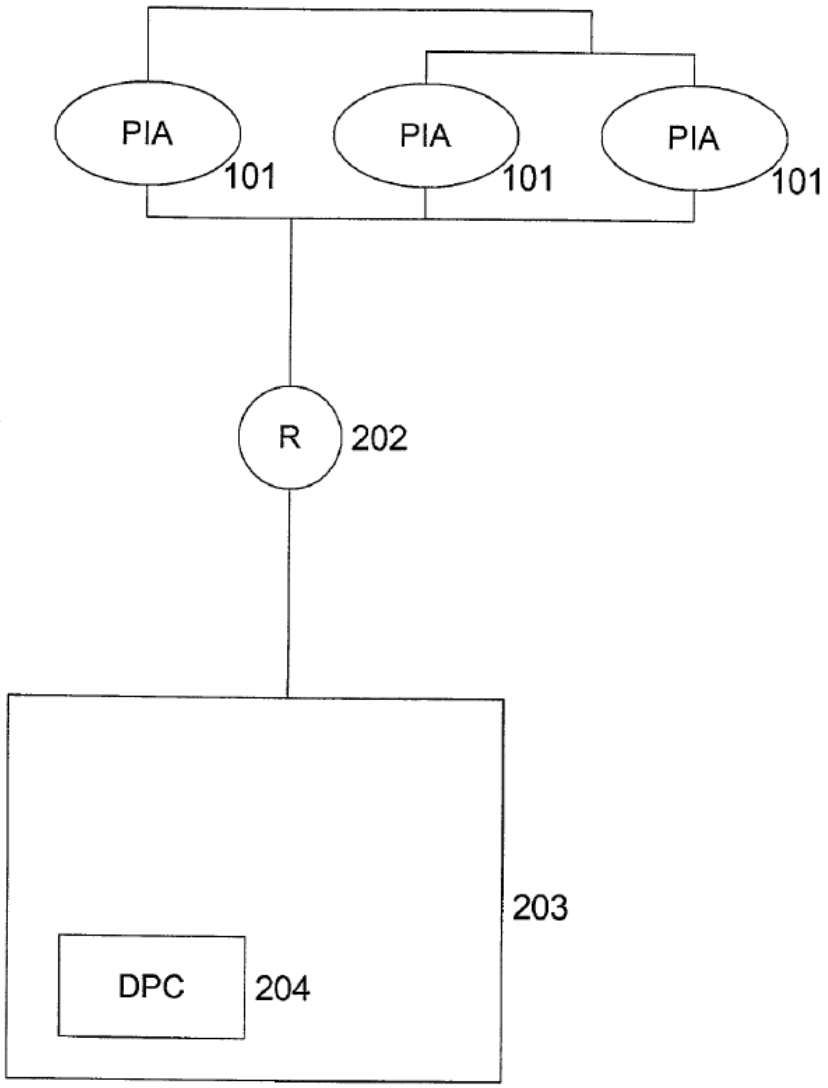

FIG. 2

Figure 2 is a block diagram showing the connections among Party Identification Devices (PIAs) 101, router 202, and Network Operations Center (NOC) 203. *Id.* ¶ 47. Figure 2 is in the context of a supermarket chain or other multi-lane retail chain with multiple PIAs 101 connected via

an in-store local area network to local router 202, which is connected to NOC 203 via frame relay lines. *Id.* ¶ 98. NOC 203 includes Data Processing Center (DPC) 204. *Id.*

Each PIA 101 has a hardware identification code that is assigned to it and registered with DPC 204 at the time of manufacture, making the PIA uniquely identifiable to DPC 204 in transmissions from the PIA. *Id.* ¶¶ 85, 161. An entity uses the PIA hardware identification code to identify itself to the DPC. *Id.* ¶ 158.

Figure 7 is reproduced below:

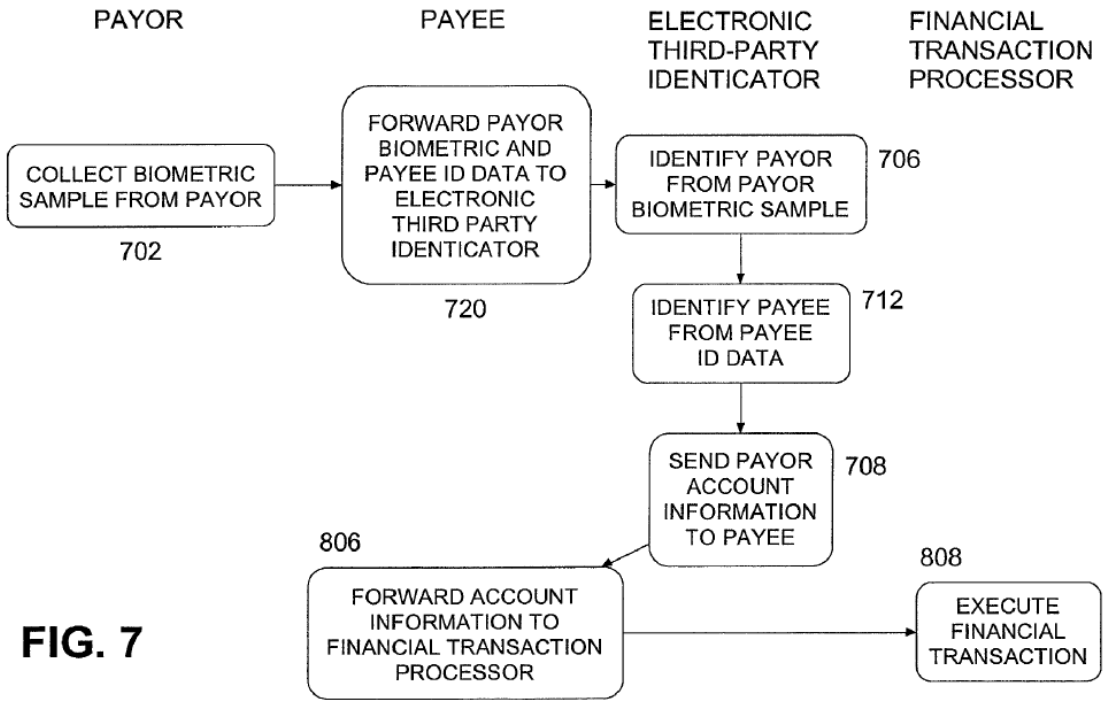

FIG. 7

Figure 7 is a flow diagram showing a transaction flow among the participants in a retail point-of-sale transaction. *Id.* ¶¶ 52, 166.

The customer/payor originates an electronic payment at a point-of-sale by submitting a bid biometric sample obtained by a biometric sensor of the PIA controlled by a payee/seller. *Id.* ¶¶ 166–167 (step 702). The PIA determines that the sample is not fraudulent and sends the sample to the

DPC. *Id.* ¶ 167. The payor enters a PIN code into the PIA, and the PIA transmits the biometric data, PIN, and hardware identification code of the PIA to the DPC. *Id.* ¶ 168 (step 720). The DPC identifies the payer using the biometric sample, retrieves a list of financial accounts that the payor has registered with the system, and transmits the list to the PIA. *Id.* (steps 706, 708). The DPC identifies the payee using the PIA hardware identification code. *Id.* ¶¶ 166, 168. The payor selects a financial account at the PIA and the PIA transmits the financial information to the payee's in-store payment system (e.g., point-of-sale terminal or electronic cash register). *Id.* ¶¶ 169–170. The in-store payment system authorizes the transaction. *Id.* ¶ 170.

3. Differences, if any, between Claims 1–9 and the Prior Art; Reasons to Modify or Combine

a) Claim limitation 1A

Petitioner contends that Scott's PID 6 teaches "a smartphone," as recited in claim limitation 1A. Pet. 20. Specifically, Petitioner argues that, "[w]hile Scott does not explicitly disclose the use of a smartphone," a smartphone would have been obvious in light of Scott's disclosure that its PID 6 could be a portable hand-held device similar in size and shape to a cell phone and that telephone and computer lines are used to communicate with PID 6. *Id.* (citing Ex. 1005, 4:22–24, 8:23–24, 9:16–22, 13:16–26, 22:6–8; Ex. 1003 ¶ 41).

Petitioner contends that Scott discloses that its PID 6 is manufactured with a unique ID code, which teaches "the ID code uniquely identifying the smartphone among a plurality of smartphones," as recited in claim limitation 1A. Pet. 20 (citing Ex. 1005, 9:23–25). Scott describes that "the units are manufactured with unique ID codes." Ex. 1005, 9:24–25.

As to whether Scott's ID code is "receiv[ed], at a smartphone . . . from a third-party trusted authority," Petitioner argues that "a [person of ordinary skill in the art] would have found it obvious that these ID codes would have come from a third party trusted authority as in Lapsley." Pet. 20. In support, Petitioner cites to Dr. Wolfe's testimony and generally to Petitioner's analysis of claim limitation 1G. *Id.* (citing Ex. 1003 ¶ 40; "[1G] *infra*"). Dr. Wolfe merely copies this argument in his testimony, without providing an additional evidence or any specificity as to where Lapsley might provide a teaching of receiving an ID code from a third-party trusted authority. Ex. 1003 ¶ 40.

Petitioner's analysis of claim limitation 1G does not purport to provide an identification of where Lapsley teaches receiving an ID code from a third-party trusted authority. Pet. 23–27. In making other arguments, Petitioner cites to paragraphs 8, 9, 27, 29, 54, 82, 85, 103, 104, 158, 161, and 166–168 of Lapsley. *Id.* at 25–27. Paragraph 29 states that "the payee would register with the [electronic third party identicator (ETPI)] payee identification data, which optionally comprises, a payee hardware ID code." Ex. 1007 ¶ 29. This does not state that a device receives the ID code from an ETPI. *Id.*

Paragraph 85 states that "[a]ach PIA preferably has a hardware identification code that is registered with the DPC at the time of manufacture. This makes the PIA uniquely identifiable to the DPC in all transmissions from that device. This hardware identification code is stored in write-once or read-only memory 110." Ex. 1007 ¶ 85. Paragraph 104 states that a DPC's "transaction processor uses the decryption module (DM) 428, which utilizes the hardware identification code of the PIA to identify the encryption code[] that is required to decrypt the message from the PIA."

Id. ¶ 104. Paragraph 158 states that "[a]n entity may either register at least one digital certificate, or use at least one PIA hardware identification code to identify itself to the DPC." *Id.* ¶ 158. Paragraph 166 states that "the payee is identified through the PIA's hardware identification code." *Id.* ¶ 166. Paragraph 168 states that "the PIA transmits the biometric-PIN to the DPC for identification, along with the PIA hardware identification code," and that "[t]he DPC identifies the payee using the hardware identification code that was previously registered by the payee." *Id.* ¶ 168. None of these statements suggests that a PIA receives the identification code from the DPC. *Id.* ¶¶ 85, 104, 158, 166, 168.

Paragraphs 8, 9, 27, 54, 103, 161, and 167 do not mention the hardware identification code. At most, Lapsley describes a PID that is assigned a code at the time of manufacturing, but it does not state what entity assigns or sends the code to the PID. In short, Petitioner does not provide an express identification of where Lapsley teaches receiving an ID code from a third-party trusted authority, and none of the paragraphs in Lapsley that Petitioner cites for other purposes provide such a teaching.

Thus, Petitioner has not shown sufficiently that Scott and Lapsley teach "receiving, at a smartphone, an identification (ID) code from a third-party trusted authority," as recited in claim limitation 1A. Independent claim 5 similarly recites "a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority"; and independent claim 7 similarly recites "the ID code is received from a third-party trusted authority." Petitioner refers to its analysis of claim limitation 1A for these features of claims 5 and 7. Pet. 30, 34. For the same reasons, Petitioner has not shown sufficiently that Scott and Lapsley teach these limitations. For this reason, Petitioner has not shown a reasonable likelihood

that it would prevail in showing that claims 1–9 would have been obvious over Scott and Lapsley.

b) Claim limitation 1G

Petitioner maps Scott's disclosure of storing a fingerprint template and ID code in memory 20 to "persistently storing biometric data and the ID code on the smartphone," as recited in claim limitation 1B. Pet. 21 (citing Ex. 1005, 4:1–18, 6:28–7:23, 8:13–22, 11:11–20, 13:10–15, 15:30–16:6, 19:30–32). As to claim limitation 1C, Petitioner notes that Scott's biometric data include fingerprint data. *Id.* at 22 (citing Ex. 1005, 1:14–23, 2:5–16, 3:21–22, 15:30–16:6). Petitioner contends that Scott's PID 6 receives a fingerprint scan and compares it to a stored biometric template, which Petitioner argues teaches "receiving, at the smartphone, scan data from a biometric scan using the smartphone," "comparing, using the smartphone, the scan data to the biometric data," and "determining whether the scan data matches the biometric data," as recited in claim limitations 1D, 1E, and 1F. *Id.* at 22–23 (citing Ex. 1005, 3:21–22, 15:30–16:29).

The parties dispute whether Scott and Lapsley teach "responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," as recited in claim limitation 1G. As to "responsive to a determination that the scan data matches the biometric data, wirelessly sending from the smartphone, the ID code for comparison by the third-party trusted authority," Petitioner contends that, in response to the comparison made in the discussion of claim limitations 1D and 1E, above, Scott's PID 6 transmits to host facility 4 an

encrypted message with the ID code. Pet. 23–24 (citing Ex. 1005, 4:6–18, 5:22–6:24, 6:28–7:23, 12:14–18, 13:10–15, 19:30–32; Ex. 1003 ¶ 48).

As to "comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," Petitioner contends that "Scott discloses that the third-party trusted authority host processing unit 32 stores a list that includes an ID code and a public key for each registered PID 6," and that host processing unit 32 compares the device ID code received from PID 6 to this list to authenticate PID 6 as a legitimately registered device. *Id.* at 24–25 (citing Ex. 1005, 5:10–21, 6:11–21, 7:24–8:4, 8:18–22, 9:23–25, 11:12–13, 12:6–13, 13:10–15, 19:18–20, 19:30–32, Fig. 1; Ex. 1003 ¶ 50). Dr. Wolfe copies these arguments in his testimony. Ex. 1003 ¶ 50. Here, Petitioner and Dr. Wolfe identify Scott's host processing unit 32 as corresponding to the claimed "third-party trusted authority." In its analysis of claim limitations 1H and 1I, Petitioner makes clear that host facility 4 is the resource (e.g., ATM machine, POS device, etc.) that is accessed when the transaction is completed. Pet. 27–28 (citing Ex. 1005, 10:24–25 ("Referring to FIG. 1, a security system 2 provides access to one or more secure host facilities 4 only to registered persons."), 5:10–21, 8:5–12, 10:25–28, 11:31–32, 13:6–9, 14:6–12, 17:20–18:19, 20:27–30; Ex. 1003 ¶ 54).

Patent Owner argues that "host processing unit 32 is *part of* the system being accessed—it is not a third party." Prelim. Resp. 7 (citing Ex. 1005, 11:24–25, 11:30–12:1). As explained in Section III.A above, a "third-party trusted authority" is a trusted authority that is an entity separate from the parties to a transaction. Scott describes both host processing unit 32 (the alleged "third-party trusted authority") and host facility 4 (the alleged resource for "accessing one or more from a group consisting of a

casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account") as part of a single entity, host system 30. Ex. 1005, 11:31–12:5 ("Host facility 4 is part of a host system 30. Host system 30 will typically be bank ATM systems, point of sale systems, and the like. Host system 30 also includes a host processing unit 32, which has a processor circuit 34 and memory 36 . . . . Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42."). Host processing unit 32, because it is not an entity separate from host facility 4, is not a third-party trusted authority.

Petitioner further argues that, "[t]o the extent that Patent Owner argues that Scott's host processing unit 32 is not a third-party trusted authority, Lapsley . . . provides additional disclosure rendering this feature of the limitation obvious to a [person of ordinary skill in the art]." Pet. 25. Petitioner contends that Lapsley's Data Processing Center (DPC) is a trusted third-party authority that receives biometric data and a hardware identification code from a Party Identification Apparatus (PIA) and uniquely identifies the PIA by finding the identification code on a list the DPC maintains. *Id.* at 25–26 (citing Ex. 1007 ¶¶ 54, 85, 103, 104, 158, 161, 166–168).

Relying on Dr. Wolfe's testimony, Petitioner argues that a skilled artisan "would have been motivated to modify Scott's system such that authentication is performed by an external third-party trusted authority possessing a list of device ID codes that unique identify legitimate PIDs, as taught in Lapsley, to improve efficiency and flexibility of the system by consolidating ID codes to a central location at a secure third-party agent." *Id.* at 26 (citing Ex. 1003 ¶ 53). Dr. Wolfe repeats this argument in his

testimony, but does not state the basis for his opinion, rendering it of little value. *See* 37 C.F.R. § 42.65(a). Citing to Lapsley, Petitioner argues that a skilled artisan "would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction." *Id.* (citing Ex. 1007 ¶¶ 8, 9, 27, 29). Petitioner argues that a skilled artisan "would have further understood that it was common to have an ATM that is not owned by a bank use the bank as a third party for authorization and it was common for a store to use a bank or credit card exchange as a third party for authorization." *Id.* at 26–27. Petitioner does not cite any evidence for this argument.

Patent Owner responds that "Lapsley's DPC is part of the system providing access to a user's registered financial accounts, i.e., a cloud based digital wallet—not a *third party* trusted authority." Prelim. Resp. 8 (citing Ex. 1007 ¶¶ 102, 138, 139). Patent Owner contends that, "[i]n Lapsley, instead of using a personal fob or phone to access the DPC digital wallet, the user utilizes a Party Identification Apparatus located at a store." *Id.* (citing Ex. 1007 ¶¶ 167–169). According to Patent Owner, "[a]s the DPC is accessed with the PIA to retrieve a list of user financial accounts stored in the DPC, the DPC must be the system being accessed/authenticated. Consequently, Lapsley's DPC is not what the Petitioner and Patent Owner agree constitutes a 'third-party trusted authority.'" *Id.* at 9.

Petitioner has not explained sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what resource is being accessed. As Patent Owner points out (Prelim. Resp. 9), the DPC appears to be what is being accessed, as the payee and payor, with the PIA, access a list of financial accounts from the DPC. Ex. 1007 ¶¶ 167–170. Here, the DPC is the resource to be accessed, but it is

a party to the transaction, rather than a third party. This is similar to the situation Petitioner argues that the applicant distinguished during prosecution: "During prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." Ex. 2001, 7 (quoting remarks made by the applicant during prosecution of the '730 patent (alterations by Petitioner)).

Petitioner's reasons to combine are also conclusory and unsupported by persuasive evidence. In particular, Dr. Wolfe merely repeats Petitioner's arguments in his testimony, without further explaining them or identifying the basis for his opinions.[6] We agree with Patent Owner that Petitioner has not shown that Lapsley teaches a third-party trusted authority or that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Scott and Lapsley.

Because Petitioner does not show persuasively that either Scott or Lapsley teaches a "third-party trusted authority," as recited in claim 1, or that a skilled artisan would have combined the teachings of those references, Petitioner has not shown sufficiently that Scott and Lapsley teach "responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," as recited in claim limitation 1G.

[6] Moreover, as explained below, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight.

Independent claims 5 and 7 include similar recitations of sending an ID code to a third-party trusted authority for comparison to a stored ID code. Petitioner refers to its analysis of claim limitation 1G for these features of claims 5 and 7. Pet. 32, 35. For the same reasons, Petitioner has not shown sufficiently that Scott and Lapsley teach these limitations. For this additional reason, Petitioner has not shown a reasonable likelihood that it would prevail in showing that claims 1–9 would have been obvious over Scott and Lapsley.

C. Obviousness of Claims 1–9 over Berardi, Shreve, and Kinoshita

Petitioner contends that claims 1–9 would have been obvious over Berardi, Shreve, and Kinoshita. Pet. 37–53. However, Petitioner's allegations and citations to Berardi do not correspond to the disclosure of that reference. *See* Prelim. Resp. 10 ("With regard to Berardi, Petitioner references elements and paragraphs not contained within Berardi at all, i.e., in error.").[7]

For example, in alleging that Berardi teaches "responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," as recited in claim

[7] Patent Owner notes that Petitioner's errors "make[] it difficult to ascertain Petitioner's arguments" but argues that "a full reading of Berardi makes clear that it fails to disclose a 'third-party trusted authority.'" Prelim. Resp. 10. Patent Owner then presents substantive arguments as to Berardi, Shreve, and Kinoshita. *Id.* at 10–15. We deny the Petition as to this ground based on Petitioner's failure to present an understandable case as to Berardi and do not reach Patent Owner's additional arguments.

limitation 1G, Petitioner argues that "issuer system 1010," including "issuer account server (IAS) 1014 that processes fob identifying information," corresponds to the claimed "third-party trusted authority." Pet. 42. Berardi does not describe an "issuer system 1010" or "issuer account server (IAS) 1014." Petitioner cites to Exhibit 1010, 10:56–11:12, 22:1–41, and 28:50–67 in support of its arguments for claim limitation 1G. The cited material in columns 10 and 11 is inapposite (and does not discuss issuer system 1010 or IAS 1014), Berardi ends its disclosure at line 30 (not line 41) of column 22, and column 28 does not exist in Berardi. Additionally, following the normal numbering of elements in patent drawings, the highest number referenced in Berardi is "906," short of the elements "1010" and "1014," discussed by Petitioner.

Also in its analysis of claim limitation 1G, Petitioner states that "the fob 102 wirelessly transmits to RFID reader 104 (which transmits to POS Device 110/issuer system 1010) a message for authorization that includes fob identifying information which includes an account number unique to the fob . . . ." Pet. 42 (citing Ex. 1010, 10:56–11:12, 22:1–19, 28:50–67). We examined Petitioner's citations to discern whether Petitioner might have mistakenly referenced issuer system 1010 rather than POS Device 110. Column 10, line 56–column 11, line 12 discusses communication via RF antenna 106 and RF module 102, and does not discuss POS Device 110. Column 22, lines 1–19 spans a portion of the claims of Berardi and does not appear relevant. Column 28, lines 50–67 do not exist in Berardi. We conclude that Petitioner did not simply misidentify or mislabel the component of Berardi it sought to reference.

There are numerous similar errors. For example, Petitioner relies on column 28, lines 50–67, which does not exist in Berardi, for claim

limitations 1B and 1D–1F. Petitioner's citation to column 12, lines 36–41, in its analysis of claim limitations 1C and 1D does not correspond to biometric information, or anything else we can discern to be relevant to these claim limitations. Instead, it discusses RFID reader 104 authenticating fob 102. Ex. 1010, 12:36–41. We do not intend to list all such errors here. We decline to speculate as to what Petitioner might have intended to cite. The result of the errors in the Petition is that we are unable to understand Petitioner's allegations and Patent Owner cannot fairly be said to be on notice of Petitioner's challenge based on Berardi.

Petitioner contends that, to the extent Berardi fails to teach claim limitation 1G, Shreve provides additional disclosure. Pet. 42–43. Petitioner further contends that, if Berardi fails to teach claim limitation 1H, Kinoshita provides additional disclosure. *Id.* at 44. However, because Petitioner has not sufficiently explained its allegations as to Berardi, it is impossible to understand Petitioner's proposed combinations with Shreve and Kinoshita. Moreover, as explained above, Petitioner's showing for claim limitations 1B and 1D–1F are based largely on material that does not exist in Berardi. Thus, even if we were able to discern Petitioner's arguments for claim limitations 1G and 1H, Petitioner's cited evidence does not support its allegations for other elements of claim 1.

Petitioner's allegations for independent claims 5 and 7 largely track or refer back to its analysis of claim 1 and, thus, suffer from the same defects. Pet. 48–53. Petitioner's allegations for claims 2–4, 6, 8, and 9 do not shed any additional light on what Petitioner might have intended for claim 1, and

instead largely cite irrelevant or non-existent material in Berardi. *Id.* at 45–48, 53.[8]

In sum, we cannot discern Petitioner's allegations of obviousness based on Berardi, Shreve, and Kinoshita, nor can we say Patent Owner is on notice of those allegations. Accordingly, Petitioner has not shown a reasonable likelihood that it would prevail in showing that claims 1–9 would have been obvious over Berardi, Shreve, and Kinoshita.

IV. CONCLUSION

Petitioner has not shown a reasonable likelihood that it would prevail with respect to at least 1 of the claims challenged in the Petition.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review is denied as to claims 1–9 of the '989 patent.

[8] We are concerned with Dr. Wolfe's testimony. Paragraphs 89–137 of his Declaration (Ex. 1003) appears to be a near carbon copy of pages 37–53 of the Petition, and include the Petition's citations to obviously incorrect or non-existent material in Berardi. These circumstances suggest a lack of attention, as even a cursory review would have shown that his testimony regarding Berardi includes numerous references to irrelevant or non-existent material, rendering that testimony not useful. This is not an instance of one or even a few inadvertent errors that might go missed upon a diligent review. The entirety of Dr. Wolfe's testimony regarding Berardi is defective on its face. For these reasons the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight.

PETITIONER:

James Glass
Marissa Ducca
Sean Gloth
Richard Lowry
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
marissaducca@quinnemanuel.com
seangloth@quinnemanuel.com
richardlowry@quinnemanuel.com

PATENT OWNER:

David Hecht
HECHT PARTNERS LLC
dhecht@hechtpartners.com