

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

UNIVERSAL SECURE REGISTRY, LLC,
Patent Owner.

IPR2018-00809
Patent 9,530,137 B2

Before PATRICK R. SCANLON, GEORGIANNA W. BRADEN, and
JASON W. MELVIN, *Administrative Patent Judges*.

MELVIN, *Administrative Patent Judge*.

JUDGMENT

Final Written Decision

Determining All Claims Unpatentable

Denying Patent Owner's Motion to Amend

35 U.S.C. § 318(a)

Denying Petitioner's Motion to Strike

Denying Patent Owner's Motion to Strike

37 C.F.R. § 42.5

I. BACKGROUND

Petitioner, Apple Inc., requested *inter partes* review of claims 1, 2, and 5–12 of U.S. Patent No. 9,530,137 B2 (Ex. 1101, “the ’137 patent”). Paper 3 (“Pet.”). Patent Owner, Universal Secure Registry, LLC, timely filed a Preliminary Response. Paper 8 (“Prelim. Resp.”). We instituted review. Paper 9 (“Inst.” or “Institution Decision”). Because Patent Owner disclaimed claims 8, 10, and 11 (Ex. 2003), the instituted review does not include those claims. Inst. 6–7. Thus, we review claims 1, 2, 5–7, 9, and 12 (the “challenged claims”).

Patent Owner filed a Response (Paper 18 (“PO Resp.”)) and a Conditional Motion to Amend (Paper 19 (“MTA”)); Petitioner filed a Reply (Paper 25 (“Pet. Reply”)) and an Opposition to Patent Owner’s Contingent Motion to Amend (Paper 24 (“MTA Opp.”)); Patent Owner filed a Sur-reply (Paper 30) and a Reply to Petitioner’s Opposition (Paper 31 (“MTA Reply”)); and Petitioner filed a Sur-reply to the Contingent Motion to Amend (Paper 39 (“MTA Sur-reply”). We held a hearing on July 16, 2019, and a transcript is included in the record. Paper 49 (“Tr.”).

This is a final written decision as to the patentability of the challenged claims. For the reasons discussed below, we determine that Petitioner has shown by a preponderance of the evidence that the challenged claims are unpatentable. We also deny Patent Owner’s Conditional Motion to Amend.

A. RELATED MATTERS

As required by 37 C.F.R. § 42.8(b)(2), each party identifies various judicial or administrative matters that would affect or be affected by a decision in this proceeding. Pet. 2–3; Paper 7, 2 (Patent Owner’s Updated Mandatory Notices).

B. THE '137 PATENT

The '137 patent is titled “Method and Apparatus for Secure Access Payment and Identification” and describes ways to securely authenticate the identity of a plurality of users. Ex. 1101, codes (54), (57), 1:43–55.

The challenged patent describes a secure database called a “Universal Secure Registry” (USR), which can be used as “a universal identification system” and/or “to selectively provide information about a person to authorized users.” *Id.* at 4:8–11. The '137 patent states that the USR database is designed to “take the place of multiple conventional forms of identification.” *Id.* at 4:23–25. The '137 patent further states that various forms of information can be stored in the database to verify a user’s identity and prevent fraud: (1) algorithmically generated codes, such as a time-varying multi-character code or an “uncounterfeitable token,” (2) “secret information” like a PIN or password, and/or (3) a user’s “biometric information,” such as fingerprints, voice prints, an iris or facial scan, DNA analysis, or even a photograph. *See id.* at 14:1–7, 14:21–40, 44:54–61, Fig. 3.

The patent discloses a variety of embodiments including those in which a user is authenticated on a device using secret information (such a PIN code) and biometric information (such as a fingerprint), then the first device transmits information to a second device for further authentication. *See id.* at 29:21–44. The second device may verify the user’s information and return an enablement signal to the first device. *Id.* at 33:20–34. Accordingly, the '137 patent discloses that the system can be used to selectively provide authorized users with access to perform transactions

involving various types of confidential information stored in a secure database. *See, e.g., id.* at 4:8–15.

C. CHALLENGED CLAIMS

Challenged claims 1 and 12 are independent. Claim 1 is illustrative of the claimed subject matter and is reproduced below, including Petitioner's square-bracketed annotations that segment the claim when mapping it to the prior art (*see* Pet. 20–41):

1. [p] A system for authenticating a user for enabling a transaction, the system comprising:
 - [a] a first device including:
 - a first processor, the first processor programmed to authenticate a user of the first device based on secret information and [b] to retrieve or receive first biometric information of the user of the first device;
 - [c] a first wireless transceiver coupled to the first processor and programmed to transmit a first wireless signal including first authentication information of the user of the first device; and
 - [d] a biometric sensor configured to capture the first biometric information of the user;
 - [e] wherein the first processor is programmed to generate one or more signals including the first authentication information, an indicator of biometric authentication, and a time varying value in response to valid authentication of the first biometric information, and [f] to provide the one or more signals including the first authentication information for transmitting to a second device; and
 - [g] wherein the first processor is further configured to receive an enablement signal from the second device; and

[h] the system further including the second device that is configured to provide the enablement signal indicating that the second device approved the transaction based on use of the one or more signals;

[i] wherein the second device includes a second processor that is configured to provide the enablement signal based on the indication of biometric authentication of the user of the first device, at least a portion of the first authentication information, and second authentication information of the user of the first device to enable and complete processing of the transaction.

Ex. 1101, 45:27–61.

D. GROUNDS OF UNPATENTABILITY

Petitioner asserts the following grounds of unpatentability based on the following evidence of record:

Claim(s) Challenged	Statutory Basis	References
1, 2, 6, 7, 9, and 12	§ 103(a)	Jakobsson ¹ and Maritzen ²
5	§ 103(a)	Jakobsson, Maritzen, and Niwa ³

Pet. 20, 53, 63. Petitioner also relies on the Declaration of Dr. Victor Shoup (Ex. 1102). Pet. 9.

E. OBVIOUSNESS OVERVIEW

An invention is not patentable “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter

¹ International Patent Application Publication No. WO 2004/051585, published June 17, 2004 (Ex. 1113).

² U.S. Patent Application Publication No. 2004/0236632, published November 25, 2004 (Ex. 1114).

³ U.S. Patent No. 6,453,301, issued September 17, 2002 (Ex. 1117).

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.” 35 U.S.C. § 103(a).⁴ The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and, (4) where in evidence, so-called secondary considerations, including commercial success, long-felt but unsolved needs, and failure of others. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441, F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of elements produced a predictable result weighs in the ultimate determination of obviousness. *KSR*, 550 U.S. at 416–17.

II. DISCUSSION

A. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner and Patent Owner propose very similar statements of the level of ordinary skill in the art. In Patent Owner’s phrasing, a skilled artisan would have had “a Bachelor of Science degree in electrical engineering, computer science or computer engineering, and three years of work or research experience in the fields of secure transactions and encryption; or a

⁴ The America Invents Act included revisions to, *inter alia*, 35 U.S.C. § 103 effective on March 16, 2013. Because the ’137 patent claims benefit of filing date under § 120 to an application filed before March 16, 2013 (*see* Ex. 1101, 1:7–40), the pre-AIA version of 35 U.S.C. § 103 applies.

Master’s degree in electrical engineering, computer science or computer engineering, and two years of work or research experience in related fields.” PO Resp. 16–17 (citing Ex. 2004 ¶ 18). Petitioner’s statement includes only a bachelor’s degree and marginally less work experience. Pet. 5. Patent Owner states that its positions would be the same under either party’s proposal. PO Resp. 17. We agree with Patent Owner that the analysis and conclusions remain the same under either proposal. As a more-comprehensive definition for a skilled artisan, we adopt Patent Owner’s statement and note that it is consistent with the prior art of record.

B. CLAIM CONSTRUCTION

Before the Board, claims in an unexpired patent are interpreted according to their broadest-reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b) (2017); *Cuozzo*, 136 S. Ct. 2131, 2144–46 (2006).⁵ Under the standard applicable here, we generally give a claim term its “ordinary and customary meaning,” which is “the meaning that the term would have to a person of ordinary skill in the art in question” at the time of the invention. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). The specification may impose a specialized meaning, departing from the ordinary and customary meaning, by defining a term with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir.

⁵ A recent amendment to this rule does not apply here because the Petition was filed before November 13, 2018. *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b), effective Nov. 13, 2018).

1994). Further, a party may prove “the existence of a ‘clear and unmistakable’ disclaimer” that narrowed a term’s definition in the prosecution history of a challenged patent. *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1063–64 (Fed. Cir. 2016) (quoting *Elbex Video, Ltd. v. Sensormatic Elecs. Corp.*, 508 F.3d 1366, 1371 (Fed. Cir. 2007)).

Petitioner proposes constructions for three terms: “biometric information,” “secret information,” and “authentication information.” Pet. 14–20. Patent Owner asserts that resolving issues in dispute requires no construction for any of those terms. PO Resp. 12.

We agree with Patent Owner that no unpatentability dispute turns on the construction of the three terms Petitioner identifies. Thus, construing those terms would not benefit this proceeding, and we therefore decline to expressly construe them. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (affirming that the Board only need construe claims terms “to the extent necessary to resolve the controversy”) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Patent Owner, however, asserts also that the term “the one or more signals,” as used in both independent claims, should be construed to mean “one or more signals that include all of the following three types of information: (1) first authentication information, (2) an indicator of biometric authentication of the user of the first device, and (3) a time varying value.” PO Resp. 12–13 (citing Ex. 2001 ¶ 38–43). Petitioner primarily addresses whether the prior art teaches the limitation as expressed by Patent Owner. *See* Reply 1–2. Petitioner also states that “limitation 1[f] does not require that the authentication code include all three pieces of

information” (*id.* at 2) but that assertion does not address the antecedent basis for “one or more signals,” which Patent Owner relies on to argue multiple places in the claim require the signals include three distinct pieces of information (PO Resp. 12–13). As to the three pieces of information as recited in limitation 1[e], Petitioner appears to accept Patent Owner’s construction. *See* Reply 1–3.

Patent Owner argues that “independent claims 1 and 12 require the first device to transmit *three separate and distinct types of information* to a second device for processing because each is a ‘distinct component’ of the claimed invention.” Sur-reply 5 (quoting *Becton, Dickinson & Co. v. Tyco Healthcare Grp.*, 616 F.3d 1249, 1254 (Fed. Cir. 2010)). In particular, Patent Owner distinguishes a claim scope where the claimed signals are “derived from some of the three distinct types of information.” *Id.* Because, as discussed below (*see infra* at 12–16), we conclude that Jakobsson teaches multiple methods of assembling its authentication code, even Patent Owner’s sought construction does not eliminate Jakobsson’s disclosures from the claim scope. Accordingly, we conclude that we need not further address Patent Owner’s construction for the one or more signals.

We explained in the Institution Decision that we view the meaning of “transaction” as significant to the issues here. Inst. 7. As we discussed in a related proceeding, CBM2018-00022, “the written description describes the invention as being broader than a system for secure access payment and the authentication of a purchaser’s identify.” CBM2018-00022, paper 10, 12–13 (citing Ex. 1101,⁶ 13:42–14:7, 42:64–43:3, Figs. 3, 4). We also noted that

⁶ The ’137 patent appears as Exhibit 1101 in this proceeding and Exhibit 1001 in CBM2018-00022.

“[w]e do not consider the term ‘transaction’ by itself to be explicitly or inherently financial, because the ’137 patent indicates that a particular transaction is financial in nature by using the term ‘financial transaction.’” *Id.* at 13 (citing Ex. 1101, 6:59, 7:9, claim 11). We adopt that same understanding of “transaction” in this case.

We conclude there is no need to construe any other term to resolve the issues in this decision. *See Nidec Motor Corp.*, 868 F.3d at 1017; *Vivid Techs.*, 200 F.3d at 803.

C. UNPATENTABILITY OVER JAKOBSSON AND MARITZEN

Petitioner maps the limitations of claims 1, 2, 6, 7, 9, 10, and 12 onto Jakobsson’s and Maritzen’s disclosures. Pet. 20–41.

Jakobsson is a published international patent application directed to an identity-authentication system. Ex. 1113. In certain embodiments of Jakobsson’s system, a user is first authenticated on a user device using a PIN or biometric information; the user device then sends information to a remote verifier including user authentication, PIN, biometric data, and a time-varying code, so that the remote system may verify the information and return a signal to the user device. *See id.* ¶¶ 50, 59.

Maritzen is a published patent application directed to conducting a financial transaction, in one embodiment using communication “between a vehicle-accessed, payment-gateway terminal (VAPGT) and a pre-registered, key-enabled, personal transaction device (PTD).” Ex. 1114, code (57). Relevant here, Maritzen involves financial transactions in the form of payments. *Id.*

Patent Owner argues that the combination of Jakobsson and Maritzen fails to disclose: “the one or more signals” recited in claims 1 and 12

(PO Resp. 17–22); the “enablement signal” recited in claims 1 and 12 (*id.* at 23–28); the comparison recited in claim 5 (*id.* at 28–30); the encryption recited in claim 6 (*id.* at 30–31); and the memory recited in claim 7 (*id.* at 32). Patent Owner also argues a skilled artisan would have had no reason to combine: Jakobsson and Martizen. *Id.* at 32–37. Finally, Patent Owner argues that objective indicia of nonobviousness counsel a conclusion of no unpatentability. *Id.* at 38–44.

1. Claims 1 and 12

Petitioner maps the limitations of claim 1 onto Jakobsson’s disclosures, relying on Maritzen only for the preamble, in that Maritzen teaches authorization of financial transactions. Pet. 25 (“Accordingly, it would have been obvious to use the authentication system of Jakobsson to authenticate a financial transaction as disclosed in Maritzen.”). At least because we construe “transaction” as broader than just financial transactions, the preamble of claim 1 reads on Jakobsson’s disclosures. Ex. 1113 ¶ 39 (“Authentication can result in the performance of one or more actions including, without limitation, providing access or privileges, taking action, or enabling some combination of the two. Access includes, without limitation: access to a physical location, communications network, computer system, and so on; access to such services as financial services and records.”); see Pet. 20–21. Thus, although Patent Owner argues that a skilled artisan would not have been motivated to combine Maritzen with Jakobsson (PO Resp. 32–37), that argument does not impact Petitioner’s showing for claim 1.

*a. Transmitting and Processing “The One Or More Signals”
(Limitations 1[f], 1[h], and 12[f])*

Jakobsson discloses a variety of configurations for the authentication codes sent to a remote verifier, including that one code may be augmented with additional information to produce another code. Ex. 1113 ¶¶ 52, 59, 65–77. In particular, Jakobsson discloses using “the user data value (P) with the secret (K), the dynamic value (T), and the event state (E) to generate an authentication code A (K, T, E, P) 292.” *Id.* ¶ 73. It also discloses a user device that “first combines (K, T, E) to generate an authentication code A (K, T, E) 291” and “then combines the generated authentication code 291 with the PIN (P) to generate an authentication code 292 that is a function of (K, T, E, P).” *Id.* That latter arrangement Jakobsson discloses as one example of how “[t]he combination function 230 can combine these values (K, T, E, P) in any order (and with other values not mentioned) to generate the authentication code 292.” *Id.*

The Petition asserts that “the processor of user authentication device 120 [first processor] is configured to provide an authentication code [one or more signals] including a first authentication code [first authentication information].” Pet. 34 (emphasis omitted; bracketed material in original) (citing *id.* at 30–33 (discussing limitation 1[e]); Ex. 1102 ¶ 85).

Patent Owner argues that Petitioner fails to show Jakobsson teaches transmitting signals including “the first authentication information, an indicator of biometric authentication, and a time varying value,” as recited in limitation 1[f]. PO Resp. 17–22. Patent Owner points to Petitioner’s assertion that Jakobsson discloses transmitting “the authentication code [first authentication information]” for verification. *Id.* at 18 (citing Pet. 34 (bracketed material and emphasis in original)).

Petitioner argues that, by referring back to its discussion of limitation 1[e], it demonstrated that Jakobsson's transmitted signals comprise "an authentication code (e.g., authentication code 292) [one or more signals] including a first authentication code (e.g., authentication code 291) [first authentication information], a strength of a biometric match (E) [indicator of biometric authentication], and a time-varying value (T) [time-varying value]." Reply 2 (quoting Pet. 33 (emphasis omitted; bracketed material in original)).

Patent Owner's argument refers to Petitioner's use of "authentication code" without acknowledging that Petitioner identified two different types of "authentication code" from Jakobsson. *Compare* PO Resp. 18, *with* Pet. 33. Because Petitioner asserts that the transmitted authentication code includes information in a first authentication code and additional information added to that first authentication code, Petitioner asserts that the transmitted information includes all three aspects of the claimed signals. Accordingly, we do not agree with Patent Owner that Petitioner fails to assert teachings that satisfy claim limitations 1[f], 1[h], or the corresponding limitations of claim 12. *See* PO Resp. 18–20.

Petitioner specifically points to Jakobsson's wide range of disclosures. Pet. 32. Furthermore, Petitioner specifically points to Jakobsson's disclosure that the combination function may operate "by prepending or appending . . . by arithmetically adding . . . or using a block cipher or other one-way function, or other algorithm, or a combination of these and other techniques that combine two or more input values together." *Id.* at 31–32 (quoting Ex. 1113 ¶ 73). Petitioner also identifies that Jakobsson's "event state (E)"

includes the “strength of a biometric match,” and “dynamic value (T)” is a “dynamic, time-varying value.” *Id.* at 30–33 (quoting Ex. 1113 ¶¶ 52, 60).

Based on Petitioner’s assertions and Jakobsson’s disclosures, we explained in the Institution Decision that we understand Petitioner’s assertions map Jakobsson’s E and T to the claimed biometric information and time-varying value, respectively, and map the other factors included in Jakobsson’s transmitted authentication code (including user data value P and device secret K) to the claimed first authentication information. Inst. 10–11 (citing Ex. 1113 ¶¶ 52, 59, 65–77). Patent Owner acknowledges our Institution Decision but argues that it impermissibly went beyond the Petition. PO Resp. 21. We do not agree because, as explained above, our understanding is consistent with Petitioner’s assertions.

Patent Owner argues that the authentication code transmitted in Jakobsson does not include the three claimed elements “because the combination function transformed those pieces of information into a unitary authentication code prior to transmission.” PO Resp. 22. The argument appears to be based on viewing Jakobsson’s combination function as a one-way hash function. *Id.* (citing Ex. 2010 ¶ 54). Jakobsson discloses that the combination function may comprise a one-way function, but also discloses that it may combine information “by prepending or appending,” or “arithmetically adding” information. Ex. 1113 ¶ 73. Petitioner relies on Jakobsson’s broad disclosure for the combination function to assert that it would have been obvious to form the claimed “one or more signals” that include “first authentication information, an indicator of biometric authentication, and a time varying value.” Pet. 31–32 (citing Ex. 1113 ¶ 73). Thus, we do not agree that Jakobsson discloses only a combination function

that produces “a unitary authentication code.” See Sur-reply 4. Similarly, Patent Owner’s argument that Jakobsson discloses transmitting on “**one of** code 291, 292, or 293” (*id.*) directly contradicts Jakobsson’s disclosure that the user device first generates authentication code 291 and “combination function 230 then combines the generated authentication code 291 with the PIN (P) to generate an authentication code 292 that is a function of (K, T, E, P).” Ex. 1113 ¶ 73. In light of Jakobsson’s disclosures of (1) combination functions that include prepending or appending information and (2) using one authentication code as a further input to the combination function to generate another authentication code for transmission, we do not agree with Patent Owner that Petitioner’s assertions amount to “double-counting.” See Sur-reply 4.

Based on the foregoing discussion, we find Jakobsson teaches claim 1’s “one or more signals including the first authentication information, an indicator of biometric authentication, and a time varying value in response to valid authentication of the first biometric information” as an authentication code generated by combining a user data value (P), a device secret (K), a dynamic value (T), and an event state that includes an indicator of biometric match (E). See Pet. 30–33. Furthermore, as discussed, Petitioner relies on transmission of that combined authentication code to assert that Jakobsson teaches the first processor is “programmed . . . to provide the one or more signals including the first authentication information for transmitting to a second device.” See Pet. 34–35. Patent Owner does not contest that Jakobsson teaches that transmission and only challenges whether the transmitted information includes the claimed “one or more signals.” See

PO Resp. 17–22. For the foregoing reasons, we find that Jakobsson teaches providing the one or more signals for transmitting to a second device.

Because claim 12 recites parallel limitations (*see id.* at 20), we reach the same conclusion for claim 12.

*b. “Enablement Signal”
(Limitations 1[h], 1[i], 12[h], and 12[i])*

Claim 1 recites “the system further including the second device that is configured to provide the enablement signal indicating that the second device approved the transaction based on use of the one or more signals” and “wherein the second device includes a second processor that is configured to provide the enablement signal based on the indication of biometric authentication of the user of the first device, at least a portion of the first authentication information, and second authentication information of the user of the first device to enable and complete processing of the transaction.”

As the claimed “second device that is configured to provide the enablement signal indicating that the second device approved the transaction based on use of the one or more signals,” Petitioner points to Jakobsson’s verifier 105 that approves a transaction based on information in the received authentication code. Pet. 36–38 (citing Ex. 1113 ¶¶ 118, 39, 50; Ex. 1102 ¶¶ 91–94).

Regarding the recitation in claim 1[i] that the enablement signal be “based on the indication of biometric authentication of the user of the first device, at least a portion of the first authentication information, and second authentication information of the user of the first device,” Petitioner points first to Jakobsson’s authentication codes, which, as described above, are made using a combination function to include a strength of biometric match and additional authentication information. Pet. 40–41 (citing Ex. 1113 ¶¶ 60,

52, 64, 50). For the second authentication information, Petitioner relies on Jakobsson's verifier comparing received authentication code (A_D) to an authentication code generated by the verifier (A_V). Pet. 39–40 (citing Ex. 1113 ¶¶ 117, 118 (“The verifier compares the value of the first authentication code (A_{1V}) with the value of the received authentication code (A_D) generated by the authentication device 120.”), 50).

Regarding the “enablement signal indicating that the second device approved the transaction,” Petitioner points to Jakobsson's disclosure that its verifier may accept the received authentication code and then “[a]uthentication can result in the performance of one or more actions including . . . providing access or privileges, taking action, or enabling some combination of the two.” Pet. 37 (quoting Ex. 1113 ¶ 118). Petitioner also relies on Jakobsson's disclosure that “the verifier can communicate positive or negative acknowledgement to the communications terminal.” *Id.* at 37–38 (quoting Ex. 1113 ¶¶ 50).

Patent Owner argues that Petitioner relies on Jakobsson's authentication code as both the “indicator of biometric authentication” and “first authentication information.” PO Resp. 23. According to Patent Owner, Petitioner fails to identify Jakobsson's disclosure of an authentication code “made up of data showing the ‘strength of a biometric match’ (as opposed to being generated from such data)” (Prelim. Resp. 24) but the distinction does not hold up.

Patent Owner's argument ignores that, as discussed above, Petitioner relies on a transmitted “authentication code” comprising multiple distinct types of information, including an indicator of biometric authentication and “first authentication information.” *See supra* at 14. Petitioner maps different

parts of Jakobsson’s transmitted “authentication code” to the claimed “first authentication information” and “indicator of biometric authentication.” That view of Jakobsson is supported by Jakobsson’s disclosure that “an authentication code is generated in a manner that communicates to the verifier information about the occurrence of one or more reportable events” including “confidence level in a biometric reading.” Ex. 1113 ¶ 11; *accord id.* ¶ 52 (“[R]eportable events can include . . . the strength of a biometric match”); see Pet. 31 (citing Ex. 1113 ¶ 52). Additionally, Jakobsson discloses that the verifier compares a received authentication code with one that it generates; the verifier enables a transaction only if the two codes match—requiring that the verifier correctly determines the event code used in the received authentication code. Ex. 1113 ¶¶ 118–119; see Pet. 37 (citing Ex. 1113 ¶ 118), 40 (same).

Patent Owner also argues that the one-way function used in Jakobsson’s combination function means it is impossible to reconstruct the inputs to the function (including the event code). PO Resp. 25 (citing Ex. 2010 ¶¶ 58–59. Patent Owner relies on testimony of its declarant, Dr. Jakobsson, to support its position. *Id.* We find that testimony directly contradicts statements in the Jakobsson reference and that the testimony is therefore not credible. *Compare* Ex. 2010 ¶ 59 (“[T]he combination function is not simply stringing together different input data to form the authentication code”), *with* Ex. 1113 ¶ 73 (disclosing that inputs to the combination function may be combined “by prepending or appending”); see Pet. Reply 9 (citing Ex. 1130 ¶¶ 39–43).

Based on the foregoing discussion, we find Jakobsson teaches using the biometric information as distinct from the other authentication information in the authentication code.

Moreover, we agree with Petitioner that, even in an embodiment with a one-way combination function, Jakobsson's verifier enables a transaction "based on" both the authentication information and an indicator of biometric authentication because both aspects of the transmitted authentication code must be correct for the code to match that generated by the verifier. *See* Pet. Reply 8; Ex. 1113 ¶¶ 118–119.

Patent Owner also argues that the "positive or negative acknowledgement" of the authentication code sent by Jakobsson's verifier indicates only successful receipt of information, not that the transaction is enabled. PO Resp. 26. But Patent Owner fails to adequately explain the reason Jakobsson's verifier would have to send a "negative acknowledgement" indicating it did not receive information. Rather, because the acknowledgement may be communicated "directly to the user" and follows the verifier's comparison of a received authentication code to a generated code (*see* Ex. 1113 ¶ 50), we are satisfied the acknowledgement indicates whether the verifier enables a transaction based on the received code. We agree with Petitioner that a skilled artisan would understand Jakobsson's "positive or negative acknowledgement," sent in response to receiving and processing an authentication code, to correspond to the claimed enablement signal. *See* Pet. Reply 9–10.

Patent Owner argues that Jakobsson teaches away from the claimed enablement signal because it "would be antithetical to a primary goal of Jakobsson: to covertly convey an event state without alerting a potential

attacker that the state has been conveyed to the verifier. PO Resp. 27. That argument is not persuasive because, as we find above, Jakobsson discloses sending an acknowledgement signal to indicate successful authentication. Ex. 1113 ¶ 50; see Pet. Reply 11. Patent Owner’s argument relies on a view of Jakobsson that is not consistent with its disclosures. See PO Resp. 27 (“By modifying Jakobsson to send an ‘enablement signal’ back to the first processor, the user of the first device would learn whether the second device approved the transaction (and the event state indicative of tampering).”). In particular, nothing in Petitioner’s asserted combination would result in Jakobsson’s system identifying to the user device when tampering is detected. Indeed, Jakobsson discloses covertly transmitting certain event states to the verifier when device tampering is detected, and in the same discussion explains that certain event-state information may be reported with “one or more bits included in the authentication code” as opposed to covert transmission “communicated implicitly.” Ex. 1113 ¶ 15. Thus, we agree with Petitioner that maintaining event states as covert is not a “primary goal” for all conditions. Pet. Reply 11 (citing Ex. 1113 ¶¶ 19, 52)

We, therefore, find Jakobsson teaches “enablement signal based on the indication of biometric authentication of the user of the first device, at least a portion of the first authentication information, and second authentication information of the user of the first device to enable and complete processing of the transaction.”

c. Uncontested limitations

As for the remaining limitations of claim 1, Petitioner provides a detailed analysis of Jakobsson’s disclosures that teach every element of the claim. Pet. 20–41. Other than as discussed above, Patent Owner offers no

argument disputing those disclosures. *See* PO Resp. 16–28. We cautioned Patent Owner “that any arguments for patentability not raised in the response may be deemed waived.” Paper 10, 5; *cf.* 37 C.F.R. § 42.23 (“Any material fact not specifically denied may be considered admitted.”).

We have reviewed the contentions in the Petition and the underlying evidence cited in support, which we determine are persuasive, and find that Jakobsson teaches the remaining limitations of claim 1 and those of claim 12 as set forth by Petitioner. *See* Pet. 20–41, 50–53.

d. Secondary Considerations of Nonobviousness

Patent Owner argues that long-felt need and failure of others, and commercial success of the patented invention, both show that the subject matter of claim 1 would not have been obvious. PO Resp. 38–44. Patent Owner argues that Petitioner’s analysis is deficient because it did not consider such evidence. *Id.* at 39.

We do not fault Petitioner for failing to address secondary considerations of nonobviousness in a Petition. While the Petitioner always has the burden to prove unpatentability (35 U.S.C. § 316(e); *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015), the Patent Owner may nonetheless be required to produce evidence supporting arguments against unpatentability (*see id.*, 800 F.3d at 1379; *Novo Nordisk A/S v. Caraco Pharm. Labs., Ltd.*, 719 F.3d 1346, 1353 (Fed. Cir. 2013) (applying a shifting burden of production to secondary considerations of nonobviousness)).

Patent Owner asserts that evidence shows it was known that electronic payment systems required additional security in 1997. PO Resp. 40–41 (citing Ex. 2012, 28, 35). Patent Owner further asserts that the need for such

security remained unmet in 2004. *Id.* at 41 (citing Ex. 2013, 239, 251). And Patent Owner asserts that such deficiencies were met by the inventions claimed in the '137 patent. *Id.* at 42 (citing Ex. 2010 ¶ 86). In particular, Patent Owner points to: “locally authenticating both secret information and biometric information”; “inclusion of the time varying value”; and “basing transaction approval on at least (1) the indication of biometric authentication of the user and (2) the authentication information.” *Id.* But Patent Owner’s declarant provides no support other than identifying claim limitations as the evidence that the '137 patent satisfied an unmet need. *See* Ex. 2010 ¶ 87. As Petitioner points out, the declarant admitted that at least some of those features were known before the '137 patent. *See* Pet. Reply 23 (citing Ex. 1127, 98:12–15, 113:6–10).

Because Patent Owner relies on the limitations of the '137 patent itself as evidence showing it met certain needs, Patent Owner’s assertion of satisfying an unmet need stands or falls with its arguments related to unpatentability. Stated otherwise, our conclusions that Jakobsson teaches the limitations of claim 1 undermines Patent Owner’s arguments that the '137 patent solved an unmet need or succeeded where others had failed.

Patent Owner also submits that commercial success weighs against a conclusion of obviousness, because “the claimed inventions are practiced by several commercially successful payment processing systems and e-wallet solutions, including at least the Apple Pay and Visa Checkout services.” PO Resp. 42 (citing Ex. 2010 ¶¶ 88–89). Although Patent Owner’s declarant makes such a statement, he provides insufficient support for the statement—indeed, nothing beyond the bald statement—that would justify a finding in Patent Owner’s favor. *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.”). Thus, we find Patent Owner has produced insufficient evidence supporting that existing systems practice the claimed invention.

As a whole, Patent Owner’s assertions regarding objective indicia of nonobviousness provide little to no persuasive evidence to support patentability. This evaluation applies not only to independent claims 1 and 12, discussed in this section, but also to the other conclusions of obviousness we reach below.

e. Conclusion regarding obviousness

Petitioner has proven by a preponderance of the evidence that Jakobsson teaches claim 1’s limitations, as discussed above. We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has proven by a preponderance of the evidence that the subject matter of claims 1 and 12 would have been obvious over Jakobsson.

2. Dependent Claim 6

Claim 6, which depends from claim 1, recites that “the first processor is further configured to encrypt the first authentication information to communicate to the second device.”

a. Jakobsson alone

Petitioner asserts that Jakobsson teaches claim 6’s additional limitation by disclosing that “the verifier 105 decrypts a value encrypted by the user authentication device 120 using symmetric key encryption or asymmetric encryption techniques, such as public key encryption.” Pet. 43 (quoting Ex. 1113 ¶ 58).

Patent Owner contests that conclusion, arguing that encrypting and decrypting “a value” falls short of encrypting the entire first authentication information. PO Resp. 30. We note that Patent Owner’s argument is not consistent with its view of Jakobsson’s authentication code above—that the combination function produces a unitary piece of information for transmission. *See supra* at 14. We do not adopt that view of Jakobsson, which includes disclosure that the transmitted authentication code contains multiple distinct values.

Petitioner asserts further that the cited paragraph of Jakobsson teaches other types of encryption such as arithmetic combination, applying to the whole authentication code. Pet. Reply 14. Although Patent Owner asserts that the argument, raised in Petitioner’s Reply, is too late, we need not decide that issue because, as discussed below, we agree with Petitioner that evidence submitted with the Petition demonstrates that the combination of Jakobsson and Maritzen renders obvious the subject matter of claim 6.

b. Jakobsson and Maritzen

Petitioner relies also on Maritzen. Pet. 43–45. Petitioner asserts that “[i]t would have been obvious to combine the encryption taught by Maritzen with the authentication system of Jakobsson” because “Jakobsson’s authentication code already involves several encryption steps” and the combination would “improv[e] overall security by adding an additional layer of encryption.” Pet. 44–45. As Petitioner points out, Maritzen discloses a “transaction key” transmitted to a clearing house and “is encrypted prior to transmission using well-known encrypting methods.” Ex. 1114 ¶ 90.

Patent Owner challenges the combination, arguing that “these references are not in the same field of endeavor, do not address the same

problem, and do not have the same structure.” PO Resp. 34–35. Patent Owner draws a distinction because Maritzen relates to “vehicle-accessed financial transactions that provide anonymity and security,” while Jakobsson relates to personal transactions. *Id.* We do not agree with Patent Owner that Maritzen and Jakobsson are nonanalogous art. As Petitioner points out, both references are “directed toward secure financial transactions that address the issue of electronic fraud.” Reply 17 (citing Pet. 22–25). Further, we agree that both references are in the same field of secure transaction systems. Pet. 22–23; *compare* Ex. 1113 ¶ 39 (describing authentication for access to financial services), *with* Ex. 1114 ¶ 31 (describing embodiments for “secure, anonymous, real time settlement of financial transactions”). We do not agree with Patent Owner that Maritzen’s goal of anonymity precludes use of its teachings with those of Jakobsson.

Rather, in our view, Petitioner adequately justifies why a skilled artisan would have applied Maritzen’s teaching of encrypting the entire transmission to Jakobsson’s authentication code. Petitioner’s declarant supports that Maritzen’s teaching of encryption for transmitted information would have improved overall security. Ex. 1102 ¶ 111. Particularly in light of Jakobsson’s teaching of encrypting a particular value sent to the verifier (Ex. 1113 ¶ 58), modifying Jakobsson’s system to encrypt the entire authentication code as with Maritzen’s transaction key would have been obvious.

We have reviewed the contentions in the Petition and the underlying evidence cited in support, which we determine are persuasive, and find that the combination of Jakobsson and Maritzen teaches the additional limitation of claim 6 as set forth by Petitioner. *See* Pet. 43–45. We have considered all

of Petitioner's assertions and all of Patent Owner's argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 6 would have been obvious over Jakobsson and Maritzen.

3. Dependent Claim 7

Claim 7 depends from claim 1 and recites further "the first device includes a first memory coupled to the first processor and configured to store the first biometric information." Petitioner asserts that Jakobsson teaches the additional limitation by disclosing that "the user authentication device 120 includes a microprocessor with on-board memory" (Ex. 1113 ¶ 41) and that "the data derived from the biometric observation is stored on the authentication device" (*id.* at claim 11). Pet. 46.

Patent Owner argues that "[d]ata 'derived from' biometric observation is not necessarily the same 'first biometric information' captured by the biometric sensor, as required by claim 7." PO Resp. 32.

Petitioner's showing is persuasive. In the challenge to claim 1, Petitioner shows that Jakobsson teaches "an indicator of biometric authentication" by disclosing strength of a biometric match used as part of the authentication code. *See supra* at 16; Pet. 30–33. Jakobsson's claim 11, upon which Petitioner relies for unpatentability of challenged claim 7, requires that the "data derived from a biometric observation" is both used to generate an authentication code (through dependence from Jakobsson's claim 10) and stored in memory. Thus, we find that Jakobsson teaches a user device that includes memory and is configured to store the first biometric information.

We have reviewed the contentions in the Petition and the underlying evidence cited in support, which we determine are persuasive, and find that Jakobsson teaches the additional limitations of claim 7 as set forth by Petitioner. See Pet. 45–46. We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 7 would have been obvious over Jakobsson.

4. Dependent Claims 2 and 9

Claim 2 depends from claim 1 and further recites “the first processor is programmed to determine the first authentication information so that the first authentication information is generated based on at least part of the first biometric information or generated based on receiving the first biometric information.” Claim 9 depends from claim 1 and further recites “the first processor is further configured to communicate information associated with the biometric information of the user of the first device.” Petitioner provides a detailed analysis of Jakobsson’s disclosures that teach the additional limitations of claims 2 and 9. Pet. 42–43 (claim 2), 46–47 (claim 9). Patent Owner offers no argument disputing those disclosures. See PO Resp. 16–37; Paper 10, 5.

We have reviewed the contentions in the Petition and the underlying evidence cited in support, which we determine are persuasive, and find that Jakobsson teaches the additional limitations of claims 2 and 9 as set forth by Petitioner. See Pet. 42–43, 46–47. We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that

the subject matter of claims 2 and 9 would have been obvious over Jakobsson.

D. UNPATENTABILITY OVER JAKOBSSON, MARITZEN, AND NIWA

Claim 5 depends from claim 1 and recites further “the first processor is further configured to compare stored authentication information with the authentication information of the user and configured to enable the first device based on a valid comparison.” For its assertions against claim 5, Petitioner additionally relies on disclosures in Niwa, as combined with those from Jakobsson and Maritzen discussed above for claim 1. Pet. 53–63.

Petitioner relies on Jakobsson’s disclosure that “a first authentication of user 110 is performed by the user authentication device 120 based on information supplied to the authentication device 120 by the user 110.” Pet. 53–54 (quoting Ex. 1113 ¶ 59; also citing Ex. 1113 ¶¶ 110–111). Because Jakobsson does not expressly state the local authentication is performed by comparing stored information with that from the user, Petitioner relies on Niwa’s disclosure of a fingerprint identification device that “produces the authentication code when a fingerprint of the customer matches a stored fingerprint within the fingerprint identification device.” Pet. 54–55 (quoting Ex. 1117, Abstract). Petitioner reasons that skilled artisans would have used Niwa’s teaching as asserted because it was a known technique to improve overall security in handheld user authentication devices, and to facilitate user access. Pet. 58 (citing Ex. 1102 ¶ 157). Petitioner also asserts that comparing a received value to a stored value is one of limited options for authenticating a user, and therefore was obvious to try. *Id.* (citing Ex. 1102 ¶ 158).

Patent Owner argues a skilled artisan had no reason to combine Niwa, Jakobsson and Maritzen. PO Resp. 37–38. According to Patent Owner, Niwa’s teaching of transmitting “personally identifiable information” to a bank for authentication is not consistent with Maritzen’s goal of anonymity. *Id.* (citing Ex. 1117, 7:37–52, 8:35–49; Ex. 1114 ¶ 6).

Patent Owner’s argument does not undermine Petitioner’s combination because Petitioner does not rely on Niwa for its teachings of sending fingerprint data, but rather for performing biometric-based authentication through comparison of received data to stored data. *See* Pet. Reply 12–13. Moreover, our conclusion of unpatentability for claim 1 did not depend on teachings from Maritzen, and thus are not affected by Maritzen’s goal of anonymity.

We agree with Petitioner’s arguments and underlying evidence cited in support, which we determine are persuasive, and find that the combination of Jakobsson and Niwa teaches claim 5’s limitations and that skilled artisans had reason to use those teachings as asserted. *See* Pet. 53–63.

We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 5 would have been obvious over Jakobsson and Niwa.

E. CONTINGENT MOTION TO AMEND

Patent Owner requests that we substitute proposed claims 13–21 for original claims 1–7, 9, and 12, “should any of claims 1, 2, 5–7, 9, and 12 . . . be found unpatentable.” MTA 1.

Petitioner asserts that Patent Owner’s proposed substitute claims: (1) improperly attempt to reintroduce previously disclaimed subject matter

(MTA Opp. 3–6); (2) fail to recite patent-eligible subject matter (*id.* at 8–17); (3) are obvious over the prior art (*id.* at 17–23); (4) and fail to satisfy § 112 (*id.* at 23–25).⁷

1. Proposed Claims

Proposed substitute claims 13 and 21 include the elements of original claims 1 and 12, respectively, and further recite added limitations. See MTA 2. Those added limitations in proposed claims 13 and 21 largely parallel each other. Compare MTA A1–2, with *id.* at A3–4. Proposed claim 13 is illustrative and recites, with added limitations underlined:

13. (Proposed Substitute for Claim 1) A system for authenticating a user for enabling a credit and/or debit card transaction, the system comprising:
- a first device including:
 - a first processor, the first processor programmed to authenticate a user of the first device based on secret information and to retrieve or receive first biometric information of the user of the first device;
 - a first wireless transceiver coupled to the first processor and programmed to transmit a first wireless signal including first authentication information of the user of the first device, the first authentication information including a multi-digit identification (ID) code allowing a networked validation-information entity to map the multi-digit ID code to a credit and/or debit card number; and

⁷ Petitioner also argues that Patent Owner proposes too many substitute claims because it includes proposed substitutes for original claim 3 and 4, which Petitioner did not challenge. MTA Opp. 6–8. Patent Owner has withdrawn proposed substitute claims 15 and 16 (see MTA Reply 8), so those arguments are moot.

a biometric sensor configured to capture the first biometric information of the user;

wherein the first processor is programmed to generate one or more signals having at least three separable fields that include ~~including~~ the first authentication information, an indicator of biometric authentication, and a time varying value in response to valid authentication of the first biometric information, and to provide the one or more signals having the at least three separable fields including the first authentication information, the indicator of biometric authentication, and the time varying value for transmitting to a second device, the second device being the networked validation information entity configured to enable the credit and/or debit card transaction based on authentication of the user; and

wherein the first processor is further configured to receive an enablement signal from the second device; and

the system further including the second device that is configured to provide the enablement signal indicating that the second device approved the credit and/or debit card transaction based on use of the one or more signals;

wherein the second device includes a second processor that is configured to provide the enablement signal based on the indication of biometric authentication of the user of the first device, at least a portion of the first authentication information, and second authentication information of the user of the first device to enable and complete processing of the credit and/or debit card transaction.

MTA A1–2.

2. Requirements of 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121

“These requirements describe a threshold showing the Board must deem satisfied before the amended claims can be considered in—i.e.,

‘entered into’—an IPR.” *Aqua Prods., Inc. v. Matal*, 872 F.3d 1290, 1304 (Fed. Cir. 2017). We consider the requirements of § 316(d) as initial thresholds, and further consider overlapping substantive issues in more detail below.

A motion to amend must propose a reasonable number of substitute claims. 35 U.S.C. § 316(d)(1)(B); 37 C.F.R. § 42.121(a)(3). Because Patent Owner proposes one substitute claim for each challenged claim, it proposes a reasonable number of substitute claims. *See* 37 C.F.R. § 42.121(a)(3); *supra* n.7.

Proposed substitute claims must respond to a ground of unpatentability involved in the trial. 37 C.F.R. § 42.121(a)(2)(i). Patent Owner contends that the limitations added by proposed substitute claims 13 and 21 are not taught by the references asserted by Petitioner. MTA 11–12. Patent Owner contends further that the limitations added by proposed substitute claim 17 further differentiate that claim from the prior art. *Id.* at 12. Petitioner disputes this aspect of Patent Owner’s showing, arguing that the proposed substitute claims reintroduce subject matter of disclaimed original claims 8 and 11. MTA Opp. 4. Petitioner also argues that the proposed substitute claims do not respond to a ground of unpatentability because they remain unpatentable over the asserted combinations. *Id.* We address both contentions below.

Proposed substitute claims may not enlarge the scope of the claims. 35 U.S.C. § 316(d)(3); 37 C.F.R. § 41.121(a)(2)(ii). Patent Owner establishes that the proposed substitute claims “include all of the original features of original independent claims 1 and 12, respectively, and further include” additional limitations. MTA 2. Patent Owner makes similar

assertions for some of the proposed substitute dependent claims. *Id.* We do not understand Petitioner to challenge this showing by Patent Owner, and we determine it to be adequate.

A motion to amend must show that the limitations of the proposed substitute claims have written-description support in the specification. 37 C.F.R. § 42.121(b)(1). Patent Owner provides a chart of proposed substitute claims that includes citations for written-description support to the as-filed applications. MTA 3–11. Petitioner challenges certain aspects of that showing, which we address below.

3. Relationship to disclaimed subject matter

Petitioner raises several arguments that relate to Patent Owner’s disclaimer of claims originally challenged in the Petition. Patent Owner’s disclaimer (Ex. 2003) removed claims 8, 10, and 11 from the review, although they were originally challenged in the Petition. Inst. 6–7.

Petitioner argues that the proposed substitute claims fail to respond to a ground of unpatentability as required by 37 C.F.R. § 42.121(a)(2)(i) because they “reintroduce subject matter that is virtually identical to original claims 8 and 11.” MTA Opp. 4. Relatedly, Petitioner argues that because Patent Owner successfully prevented review of the disclaimed claims, it should be estopped from pursuing the same subject matter in substitute claims. *Id.* at 5. Petitioner argues also that because Patent Owner did not raise arguments against unpatentability of claims 8, 10, or 11 in the Patent Owner Response, it has waived the ability to do so now. *Id.* at 5–6. Finally, Petitioner argues that Patent Owner failed to meet its duty of candor under 37 C.F.R. § 42.11 because proposing substitute claims 13 and 21 contradicts

its assertion in the Preliminary Response that the unpatentability of claims 8 and 11 was moot. Pet. 6.

Patent Owner contests all of Petitioner's related arguments by contending that proposed substitute claims 13 and 21 are distinct from the disclaimed claims. MTA Reply 2–8. Thus, according to Patent Owner, there is no concern over recapturing disclaimed subject matter. Tr. 36:17–38:14. Patent Owner also submits that it could not have waived arguments related to the MTA by failing to raise them in the Patent Owner Response because the two relate to different aspects of the proceeding. *Id.* at 7.

For the following reasons, we will proceed with an analysis of Patent Owner's proposed substitute claims. First, Petitioner was not prevented from raising arguments for unpatentability of the proposed substitute claims, and the proposed substitute claims are at least potentially distinct from the disclaimed claims. Second, because the proposed substitute claims are considered in a motion to amend, the restrictions on unpatentability arguments in IPR petitions do not apply. *Amazon.com, Inc. v. Uniloc Luxembourg S.A.*, IPR2017-00948, Paper 34, at 7–9 (PTAB Jan. 18, 2019) (precedential) (available at <https://go.usa.gov/xVvjC>). Last, as discussed in more detail below, we permit Petitioner to rely on the arguments made in the Petition as to the disclaimed claims. Accordingly, we determine that the best course is to consider Patent Owner's Motion to Amend on its merits.

4. Obviousness Over Jakobsson, Martizen, and Schutzer

Petitioner asserts that proposed claims 13 and 21 include limitations that are obvious for the same reason that Petitioner explained for original claims 8 and 11, which depended from claim 1. MTA Opp. 17. Petitioner

asserts further that Jakobsson discloses the limitation added to proposed claim 13—that the signals have “at least three separable fields.” *Id.* at 18–20.

a. Incorporation from the Petition

Patent Owner argues that Petitioner improperly attempts to incorporate arguments from the Petition into the Opposition to Patent Owner’s Contingent Motion to Amend. MTA Reply 14 n.2. We determine that, in the unique circumstances presented where Petitioner’s arguments oppose limitations added from previously disclaimed claims, Petitioner’s approach is acceptable. We waive the prohibition on incorporation by reference as to this narrow issue. 37 C.F.R. § 42.5.

b. Proposed claims 13 and 21

(1) “the first authentication information including a multi-digit identification (ID) code allowing a networked validation-information entity to map the multi-digit ID code to a credit and/or debit card number”
and
“the second device” is “the networked validation-information entity configured to enable the [credit and/or debit card]/[financial] transaction based on authentication of the user”

Petitioner addresses the above two phrases in proposed claim 13 and 21 together, as the phrases both relate to the “networked validation-information entity”—the second device of original claim 1 must be a “networked validation-information entity” that maps a multi-digit ID code included in the first authentication number to an account number and enables a transaction based on authentication of the user. *See* MTA A1–2, A3–4, B1, B4; MTA Opp. 17–20.

Original claim 8 depended from claim 1 and recited “the first authentication information includes a multidigit public ID code for a credit card account, which a credit card issuer can map to a usable credit card

number.” Original claim 11 depended from claim 1 and recited “the second device . . . is a networked credit card validation-information entity configured to approve or deny financial transactions based on authentication of the user.” Based on the limitations of those two original dependent claims, Petitioner submits that the additional limitations 13[c] and 13[e] would have been obvious for the same reasons as for original claims 8 and 11. MTA Opp. 17 (citing Pet. 63–72; Ex. 1102 ¶¶ 169–174; Ex. 1129 ¶ 36).

Patent Owner challenges that conclusion, arguing that original claim 8 recited a multidigit public ID code that a credit card issuer can map to a usable credit card number, which Patent Owner contrasts with the “networked validation-information entity” in the proposed claims. MTA Reply 15–16. Petitioner argues in return that the distinction of a networked validation-information entity (“NVIE”) from a credit-card company is meaningless because an NVIE can be a credit-card company. MTA Sur-reply 2 (citing MTA Reply 22 (“the claimed networked validation-information entity may be a financial institution, such as a credit card company”).

We agree with Petitioner. While a credit-card company does not necessarily act as the claimed networked validation-information entity, it may do so. Ex. 2021 ¶ 46. Petitioner demonstrates that Schutzer⁸ discloses authenticating a user with an “alternate card number” in place of a card user’s actual card number. Pet. 64–65 (citing Ex. 1115 ¶¶ 2, 19, 11). When Schutzer’s credit-card company (the card issuer) receives the alternate card number, it “can be associated by the card issuer with the proper cardholder

⁸ European Patent Application Publication No. EP 1028401, published August 16, 2000 (Ex. 1115).

and the cardholder’s account can be authorized.” Ex. 1115 ¶ 11. Schutzer also discloses that the alternate card number is “linked to the user’s actual card number” and that the actual card number is sent to the card issuer’s authorization processor. *Id.* ¶¶ 26, 32. Thus, Schutzer teaches mapping a multi-digit ID code received from the user to a credit card number, as claimed.

Petitioner demonstrates also that Schutzer’s card issuer acts as the claimed second device that is a networked validation-information entity that approves or denies financial transactions based on authentication of the user. Pet. 69–71 (citing Ex. 1115 ¶¶ 12, 24, 27, Fig. 1). Petitioner’s contentions, as described above, include that Schutzer’s card issuer both maps the alternate card number to the actual card number and then approves a transaction, sending an authorization to the merchant bank. Ex. 1115 ¶ 27; *see id.* ¶ 32. Furthermore, Petitioner demonstrates that skilled artisans had reason to use Schutzer’s alternate card number and card-issuer processing system with Jakobsson’s authentication system because it would have obscured exploitable account information during authentication and would have validated credit-card users. MTA Opp. 17–18; Pet. 66–68, 71–72.

Accordingly, we conclude that it would have been obvious for the claimed “second device” to be a “networked validation-information entity” that maps the multi-digit ID code to an account number, as taught by Schutzer combined with Jakobsson.

(2) “at least three separable fields”

Proposed claim 13 (but not proposed claim 21) adds a requirement that the generated signals have “at least three separable fields that include” the same three pieces of information required by original claim 1—first

authentication information, an indicator of biometric authentication, and a time varying value.

Petitioner contends that Jakobsson discloses the “three separable fields” limitation because its disclosures include authentication codes formed in iterative steps that build on prior authentication codes, including by “prepending or appending” information. MTA Opp. 18–19 (citing Ex. 1113 ¶¶ 63, 73, 15). Thus, Petitioner asserts, it would have been obvious to create an authentication code such that Jakobsson’s event state, dynamic value, and user data value would be separable. *Id.* at 19 (citing Ex. 1129 ¶¶ 37–39; Ex. 1130 ¶¶ 39–43). Petitioner reasons that using Jakobsson’s teachings in such a manner would have been an obvious application of a known technique that would securely authenticate a user. *Id.* (citing Ex. 11129 ¶ 40).

Petitioner also reasons that it would have been obvious to try Jakobsson’s prepending or appending combination function in light of Jakobsson’s teaching that “the manner of combination and the input provided to the combination function 230 could vary from these examples.” MTA Opp. 19–20 (quoting Ex. 1113 ¶ 63; citing *id.* ¶¶ 15, 73).

Patent Owner refuses to take a position on the effect that this phrase has on the scope of the claims. Tr. 38:15–40:15. Patent Owner’s arguments, discussed below, largely follow the arguments it makes against original claim 1. Patent Owner argues that Jakobsson discloses sending only a unitary authentication code, not a combination of an authentication code, event code, and time-varying value together. MTA Reply 16–17. We addressed that argument in Petitioner’s principal unpatentability arguments, concluding that Jakobsson discloses generating one authentication code and

then combining it with additional information to make a second authentication code that is transmitted to the verifier. *See supra* at 15 (citing Ex. 1113 ¶ 73).

Patent Owner argues further that Jakobsson's one-way function renders an authentication code irreversible, such that it is not possible to separate the information used to make the code. MTA Reply 17–18. We addressed that argument in Petitioner's principal unpatentability arguments, concluding that Jakobsson does not disclose using the one-way function in all embodiments of its combination function. *See supra* at 14, 18. Because Patent Owner's argument is not consistent with Jakobsson's disclosures that the combination function may operate “by prepending or appending,” or “arithmetically adding” information, Patent Owner's argument is not persuasive. Ex. 1113 ¶ 73. Indeed, we agree with Petitioner that Jakobsson discloses an embodiment in which the verifier reverses the combination operation to extract information. Ex. 1113 ¶ 58; MTA Sur-reply 3. Thus, Jakobsson is not limited to an irreversible, one-way combination function.

Because Jakobsson's transmitted authentication code comprises multiple, distinct values including those that the claim language reads on (i.e., a user data value (P), dynamic value (T), and event state indicating strength of a biometric match (E)), and because Jakobsson teaches forming that authentication code by prepending or appending information to an existing code, we find Jakobsson teaches the additional limitation requiring “at least three separable fields.”

(3) “credit and/or debit card transaction”
or “financial transaction”

Proposed claim 13 recites a “credit and/or debit card transaction” while proposed claim 21 recites a “financial transaction.” Original claim 8 recited the use of a credit card account and original claim 11 recited a “credit card validation-information entity configured to approve or deny financial transactions.” Thus, Petitioner submits that the additions in proposed claims 13 and 21 would have been obvious to skilled artisans for the same reasons as the language in original claims 8 and 11. MTA Opp. 20.

Patent Owner does not contest that assertion. *See generally* MTA Reply. We agree with Petitioner for the reasons given in the Petition. Pet. 63–72. Just as discussed above regarding the “networked validation-information entity” limitations in the proposed claims, Schutzer discloses using the system for credit card transactions. *See supra* at 35. It would have been obvious to employ the combined teachings of Jakobsson, Martizen, and Schutzer as claimed.

(4) Summary

We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of proposed substitute claims 13 and 21 would have been obvious over Jakobsson, Martizen, and Schutzer.

c. Proposed claims 14 and 19

Proposed claims 14 and 19 depend from proposed claim 13 and add the same limitations recited in original claims 2 and 7, respectively. MTA A2, A3, B2, B3. Petitioner relies on that relationship to argue that the

subject matter of proposed claims 14 and 19 would have been obvious for the same reasons as original claims 2 and 7. MTA Opp. 20–21 (citing Pet. 42–43, 45–46; Ex. 1102 ¶¶ 102–105, 113–115; Ex. 1129 ¶ 43). Patent Owner does not contest that assertion. *See generally* MTA Reply.

We agree with Petitioner for the reasons discussed above and those given in the Petition. *See supra* at 26, 27; Pet. 42–43, 45–46. We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of proposed claims 14 and 19 would have been obvious over Jakobsson, Martizen, and Schutzer.

d. Proposed claim 18

Proposed claim 18 depends from proposed claim 13, includes the same limitation recited in original claim 6, and further recites “the first authentication information further including a digital signature generated using a private key associated with the first device.” MTA A3, B3. Petitioner asserts that proposed claim 18 would have been obvious for the same reason as original claim 6, and because Schutzer discloses the added limitation. MTA Opp. 21–23 (citing Pet. 43–44; Ex. 1102 ¶ 106–109; Ex. 1129 ¶¶ 44–51; Ex. 1113 ¶¶ 21, 97, 112; Ex. 1115 ¶¶ 13, 29). Schutzer discloses that user information can include “a personal identification number, a password, a biometric sample, a digital signature or the transaction card number for the transaction card user.” Ex. 1115 ¶ 13; *accord id.* ¶ 29 (“[I]ssuing bank 8 can require more secure authentication, such as . . . digital signatures.”). Petitioner argues that it “would have been obvious to try adding the digital signature of Schutzer to the other authentication values disclosed by Jakobsson.” Pet. 22–23 (citing Ex. 1129 ¶¶ 49–51). Petitioner’s declarant

Dr. Shoup explains that in one approach within Jakobsson’s disclosures, “a user could decrypt data with their private key to create a digital signature, and then append the digital signature to the authentication code” whereby the “recipient of this digital signature could (1) reverse the appending operation and then (2) confirm that the device that created the digital signature is in possession of the user’s private key by encrypting with the user’s public key.” Ex. 1129 ¶ 50.

Patent Owner contends that “Schutzer says nothing about the ‘first authentication information’ having separable fields further including a digital signature generated using a private key associated with the first device” or “how the issuing bank receives the digital signature.”

MTA Reply 19–21. We agree with Petitioner, however, that its declarant provided an adequate explanation of why it would have been obvious to try the claimed approach in light of Jakobsson’s and Schutzer’s disclosures. MTA Sur-reply 5–6 (citing Ex. 1129 ¶¶ 44–51). We credit Dr. Shoup’s detailed explanation of why it would have been obvious to include a digital signature, created with a private key, that secretly authenticates a user. Ex. 1129 ¶¶ 50–51.

We have considered all of Petitioner’s assertions and all of Patent Owner’s argument and evidence, and we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of proposed claim 18 would have been obvious over Jakobsson, Martizen, and Schutzer.

5. Written-Description Support

Petitioner contends that two limitations in the proposed substitute claims lack written-description support in the original disclosure—one in the

independent proposed claims and one in proposed claim 17. MTA Opp. 23–25.

a. Proposed claims 13 and 21

Petitioner submits that proposed claims 13 and 21 lack written-description support because “[t]he specification does not discuss a single element performing the claimed functions of both the ‘networked validation-information entity’ and the ‘second device.’” MTA Opp. 24. Patent Owner contends, on the other hand, that the original disclosure includes embodiments including “the networked credit card validation-information entity configured to approve and deny financial transactions based on authentication of the user” and where “the USR authenticates a user to approve/deny a financial transaction by determining whether a code it received from the user is valid.” MTA Reply 22–23 (citing Ex. 2006, 10:27–29, 23:20–24:11). We agree with Petitioner.

The first passage Patent Owner identifies states that the validation-information entity can “approve and deny financial transactions based on authentication of the user.” Ex. 2006, 10:27–29. That disclosure, however, is not adequately connected to the other claim limitations regarding the “second device” and does not provide sufficient detail to support those added limitations. Stating that approval is “based on authentication of the user” does not inform a reader where or how that authentication is performed.

The passage relating to Figure 7 (Ex. 2006, 23:20–24:11) provides more detail, but still fails to show possession of the proposed claimed invention. The passage describes that a user device may generate a code that is then provided to a merchant and transmitted to a credit-card company.

Ex. 2006, 23:23–28. In the passage, once the credit-card company receives the code, it sends the code to the USR to obtain the user’s actual credit-card number. *Id.* at 23:28–32. The disclosure states that although such passing of data occurs over a secure link, the consequence of that link being compromised “may be avoided by instead transmitting, on approval, a multidigit public ID code for the credit card holder which the credit card company can map to the correct credit card number.” *Id.* at 23:32–24:2. That description does not support the claimed arrangement where the second device (the USR) also acts as the networked validation-information entity because the description maintains the credit-card company and the USR as distinct entities, with information being sent between them. When the original disclosure states that the credit-card company may map “a multidigit public ID code” to the actual account number, that description arises in an embodiment where the multidigit public ID code comes from the USR. Ex. 2006, 23:32–24:2. Overall, the passage Patent Owner relies on does not support that “the USR authenticates a user to approve/deny a financial transaction” as Patent Owner asserts. See MTA Reply 22–23.

Furthermore, Patent Owner’s showing is deficient regarding mapping the multidigit ID code to a financial account number. See MTA Reply 22–34 (citing Ex. 2006, 23:20–24:11). As Petitioner argues, disclosure that the “USR software 18 determines if the code is valid . . . and if valid accesses the user’s credit card information” does not mean that the USR maps the code to credit-card information. MTA Sur-reply 7 (quoting Ex. 2006, 23:30–31). Rather, the disclosure is consistent with using the code as a validation condition but not the key to locate the user’s credit-card information.

Patent Owner asserts that the original disclosure includes passages supporting that a “second device” performs authentication of a user (see MTA Reply 23 (citing Ex. 2006, 6:26–33, 38:11–14, 43:27–29, 44:3–12, 45:7–46:2) but those passages do not remedy the deficiency discussed—insufficient disclosure that the “second device” maps a multidigit ID code to an account number.

Accordingly, we find that the original disclosure does not show possession of the claim to a device that authenticates a user based on the claimed information, maps a “multi-digit ID code” to a financial account number, and enables a financial transaction. In light of the foregoing, we find that the original disclosure does not support proposed substitute claim 13 or 21. Because all other substitute claims depend from claim 13, they suffer from the same deficiency.

b. Proposed claim 17

Petitioner argues that proposed claim 17, which depends from proposed claim 13, lacks written-description support for the additional limitation that “the first device communicates with the second device periodically to prevent intentional deletion of information stored at the first device.” MTA Opp. 25. Although Patent Owner points to a portion of the original disclosure discussing preventing automatic deletion (MTA 9 (citing Ex. 2006, 39:21–32, 40:8–24)), we agree with Petitioner.

The identified portion of the original disclosure states that “the device 2110 can also be configured to automatically delete any portion of or all of the data stored in memory 2118 at step 206” and that “the first wireless device can be configured to periodically communicate with the secure database 2146 to remain alive” such that “[i]f the first device does not

communicate with the secure database at such periodic intervals at step 208, then the first device can be configured to delete any or a portion of the data stored in memory at step 206.” Ex. 2006, 40:8–24. Petitioner identifies persuasively that “intentional deletion” is not the same as “automatic deletion” as described in the original disclosure. MTA Sur-reply 9–10.

Thus, for that additional reason, we find that the original disclosure does not support proposed substitute claim 17.

6. Indefiniteness

Petitioner argues that “to prevent intentional deletion” in proposed claim 17 is indefinite. MTA Opp. 25; MTA Sur-reply, 9–10. Because we address that limitation and determine it lacks written-description support, we do not address Petitioner’s indefiniteness argument.

7. Ineligible Subject Matter

Petitioner contends that proposed substitute claims are directed to ineligible subject matter under § 101. MTA Opp. 8–17. Because, as discussed above, we determine that the proposed substitute claims are not supported by the original disclosure, and that many of the proposed claims would have been obvious over the prior art, we do not address Petitioner’s § 101 arguments.

F. PETITIONER’S MOTION TO STRIKE

Petitioner seeks to preclude reliance by Patent Owner in its Conditional Motion to Amend on an embodiment in which a user’s electronic ID device sends a code to the USR. Paper 35, 2. That argument applies to Petitioner’s assertion that proposed substitute claims 13 and 21 lack written-description support. *See supra* at 42; MTA Sur-reply 6–8.

We are sympathetic to Petitioner’s position, in that a Motion to Amend must itself set forth the written-description support for proposed amended claims. *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, -01130, Paper 15, at 7–8 (PTAB Feb. 25, 2019) (precedential) (available at <https://go.usa.gov/xV7rk>). That said, however, Petitioner was able to respond to Patent Owner’s position through Petitioner’s MTA Sur-reply. See *Innovative Memory Sys., Inc. v. Micron Tech., Inc.*, No. 2018-1348, 2019 WL 4458399, at *5 (Fed. Cir. Sept. 18, 2019) (“[T]he surreply afforded IMS sufficient additional opportunity to be heard.”). Additionally, Patent Owner did cite the portion of the original disclosure in question, albeit in connection with a different claim limitation than is now in dispute. Paper 41, 5–7. We do not conclude such citation adequately informed Petitioner of the asserted support, but especially in light of Petitioner’s ability to respond, we deny Petitioner’s motion to strike.

G. PATENT OWNER’S MOTION TO STRIKE

Patent Owner seeks to strike one of Petitioner’s reply declarations, submitted by Dr. Juels. (Ex. 1130), and portions of the Reply that rely on the declaration. Paper 36 (“PO Mtn. Strike”), 1. Petitioner asserts the declaration properly responds to assertions in Dr. Jakobsson’s declaration submitted by Patent Owner (Ex. 2010). Paper 44 (“Pet. Opp. to PO Mtn. Strike”), 2–5. Petitioner includes a chart showing how each of Dr. Juels’s substantive declaration paragraphs maps to Dr. Jakobsson’s statements. *Id.* at 4–5. Petitioner also submits that it had no reason to anticipate that Patent Owner’s declarant, Dr. Jakobsson, would make the statements in his Declaration. *Id.* at 6–7.

Despite Petitioner identifying how Dr. Juels's Declaration responds to Dr. Jakobsson's Declaration or deposition testimony (Pet. Opp. to PO Mtn. Strike 4–5), Patent Owner does not challenge Petitioner's assertions. *See* Paper 46. We agree with Petitioner that Dr. Juels's Declaration is responsive to Patent Owner's arguments and evidence in the Response. Additionally, Patent Owner had an opportunity to respond in a Sur-reply. *See Innovative Memory Sys.*, 2019 WL 4458399, at *5. We, therefore, deny Patent Owner's Motion to Strike.

III. CONCLUSION⁹

In summary:

Claims	Basis	References	Claims Shown Unpatentable	Claims Not shown Unpatentable
1, 2, 6, 7, 9, 10, and 12	§ 103	Jakobsson and Maritzen	1, 2, 6, 7, 9, and 12	
5	§ 103	Jakobson, Maritzen, and Niwa	5	
Overall Outcome			1, 2, 5–7, 9, and 12	

⁹ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

Additionally, we reach the following conclusions regarding Patent Owner's Conditional Motion to Amend:

Motion to Amend Outcome	Claim(s)
Original Claims Canceled by the Amendment	1–7, 9, 12
Substitute Claims Proposed in the Amendment	13–21
Substitute Claims: Motion to Amend Granted	
Substitute Claims: Motion to Amend Denied	13, 14, 17–21
Substitute Claims: Not Reached	15, 16

IV. ORDER

Accordingly, it is:

ORDERED that claims 1, 2, 5–7, 9, and 12 of the '137 patent are unpatentable;

FURTHER ORDERED that Patent Owner's Contingent Motion to Amend is denied; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Monica Grewal

Benjamin Fernandez

Kelvin Chan

Mark Selwyn

WILMER CUTLER PICKERING HALE AND DORR LLP

Monica.grewal@wilmerhale.com

Ben.fernandez@wilmerhale.com

Kelvin.chan@wilmerhale.com

Mark.selwyn@wilmerhale.com

PATENT OWNER:

Jim Glass

Tigran Guledjian

Christopher Mathews

Nima Hefazi

Richard Lowry

QUINN EMANUEL URQUHART & SULLIVAN LLP

jimglass@quinnemanuel.com

tigranguledjian@quinnemanuel.com

chirsmathews@quinnemanuel.com

nimahefazi@quinnemanuel.com

richardlowry@quinnemanuel.com