

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

UNIVERSAL SECURE REGISTRY, LLC,
Patent Owner.

IPR2018-00812
Patent 8,856,539 B2

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

MELVIN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. BACKGROUND AND SUMMARY

Petitioner, Apple Inc., filed a Petition (Paper 3, “Pet.”) requesting *inter partes* review of claims 1–3, 5–8, 16–24, 26–30, 37, and 38 of U.S. Patent No. 8,856,539 B2 (Ex. 1101, “the ’539 patent”). 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 5–8, 17–20, and 26–30 (Ex. 2110; *see* Paper 25, 1 n.1), and because we treat such claims as if they never existed (*Guinn v. Kopf*, 96 F.3d 1419, 1422 (Fed. Cir. 1996)), the instituted review does not include those claims. *Cf. SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1357 (2018) (“[T]he claims challenged ‘in the petition’ will not always survive to the end of the case; some may drop out thanks to the patent owner’s actions.”). Thus, we review claims 1–3, 16, 21–24, 37, and 38 (“the challenged claims”) of the ’539 patent.

Patent Owner filed a Response (Paper 25 (“PO Resp.”)) and a Conditional Motion to Amend (Paper 21); Petitioner filed a Reply (Paper 30 (“Pet. Reply”)) and an Opposition to Patent Owner’s Conditional Motion to Amend (Paper 29); Patent Owner filed a Sur-reply (Paper 33 (“PO Sur-reply”)) and a Reply to Petitioner’s Opposition (Paper 34); and Petitioner filed a Sur-reply to the Conditional Motion to Amend (Paper 36). We held a hearing on August 27, 2019, and a transcript is included in the record. Paper 44 (“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

not shown by a preponderance of the evidence that any of the challenged claims is unpatentable.

B. 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. 3–4; Paper 7, 2 (Patent Owner’s Updated Mandatory Notices).

C. THE ’539 PATENT

The ’539 patent is titled “Universal Secure Registry” and describes “a universal identification system . . . used to selectively provide personal, financial or other information about a person to authorized users.” Ex. 1101, code (54), 3:5–9. The ’539 patent discloses that the secure registry system may include “[a] multicharacter public code . . . which the system can map to provide permit delivery of items, complete telephone calls and perform other functions for entities. The system may also be utilized to locate an individual based on limited biological data.” *Id.* at code (57).

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 3:5–9. The ’539 patent states that the USR database is designed to “take the place of multiple conventional forms of identification.” *Id.* at 3:22–24. According to the ’539 patent, “the USR system may enable the user’s identity to be confirmed or verified without providing any identifying information about the person to the entity requiring identification.” *Id.* at 3:25–27. In one regard, the USR may restrict

access to information based on the identity of the party requesting the information. *Id.* at 10:40–57.

The '539 patent describes an embodiment in which a user may use an electronic ID device to generate a code that a merchant passes on to the USR along with purchase information. *Id.* at 12:19–54. If the USR correctly validates the code, it may in turn pass transaction information to a credit-card company to facilitate the transaction. *Id.* at 12:27–46.

D. ILLUSTRATIVE CLAIMS

Challenged claims 1, 22, 37, and 38 are independent. Claim 1 is illustrative of the claimed subject matter and is reproduced below:

1. A secure registry system for providing information to a provider to enable transactions between the provider and entities with secure data stored in the secure registry system, the secure registry system comprising:
 - [a] a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and
 - a processor configured
 - [b] to receive a transaction request including at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the provider requesting the transaction,
 - [c] to map the time-varying multicharacter code to the identity of the entity using the time-varying multicharacter code,
 - [d] to execute a restriction mechanism to determine compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication

of the provider and the time-varying multicharacter code of the transaction request, and to allow or not allow access to the secure data associated with the entity including information required to enable the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information,

[e] wherein the account identifying information is not provided to the provider and the account identifying information is provided to a third party to enable or deny the transaction with the provider without providing the account identifying information to the provider.

Ex. 1101, 18:29–60.¹

E. PRIOR ART AND ASSERTED GROUNDS

Petitioner asserts claims 1–3, 16, 21–24, 37, and 38 are unpatentable as obvious under 35 U.S.C. § 103(a) in view of Reber² and Franklin³.

Pet. 19–71. Petitioner also relies on the Declaration of Dr. Victor Shoup (Ex. 1102). *Id.* at 6.

¹ We add formatting and square-bracketed annotations to separate claim limitations as identified by the parties. Our formatting and annotations imply no functional or structural aspect of the claim beyond identifying limitations for discussion.

² U.S. Patent No. 5,930,767 (filed May 28, 1997; issued July 27, 1999) (Ex. 1131).

³ U.S. Patent No. 6,000,832 (filed Sept. 24, 1997; issued Dec. 14, 1999) (Ex. 1132).

II. ANALYSIS

A. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner submits that a person of skill in the art at the time of invention for the '539 patent “would have a Bachelor’s Degree in electrical engineering, computer science, or a related scientific field, and approximately two years of work experience in the computer science field including, for example, operating systems, database management, encryption, security algorithms, and secure transaction systems, though additional education can substitute for less work experience and vice versa.” Pet. 10 (citing Ex. 1102 ¶¶ 61–62). Patent Owner submits that the level of skill would involve “a Bachelor of Science degree in electrical engineering and/or computer science, and three years of work or research experience in the fields of secure transactions and encryption, or a Master’s degree in electrical engineering and/or computer science and two years of work or research experience in related fields.” PO Resp. 17 (citing Ex. 2018 ¶¶ 16–20). Patent Owner agrees that its “description of the level of ordinary skill in the art is essentially the same as that of the Petitioner, except that Petitioner’s description requires two years of work or research experience (as compared to three years).” *Id.* at 17–18. We do not understand any of the parties’ disputes to turn on a precise definition of the level of skill in the art and apply the level of skill as defined by the parties.

B. CLAIM CONSTRUCTION

In a Board proceeding based on a petition filed before November 13, 2018, 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 Speed Techs., LLC*

v. Lee, 136 S. Ct. 2131, 2144–46 (2016).⁴ Under that standard, 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. 1994).

Petitioner proposes constructions for several terms in the ’539 patent: “provider,” “entity,” “time-varying multicharacter code,” “indication of the provider,” “account identifying information,” and “secure registry.” Pet. 12–17. Patent Owner proposes constructions for three terms: “the provider requesting the transaction,” “access restrictions for the provider,” and “third party.” PO Resp. 19–25.

To support our analysis of the disputed issues below, we construe “account identifying information” and “third party.” We conclude that there is no need to construe any other term to resolve the issues in this decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

⁴ 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).

1. “Account identifying information”

Petitioner submits that “account identifying information” means “personal information about an entity such as name, address, or account number.” Pet. 16. Petitioner cites the Specification’s statement that “providing anonymous identification of a person enables the person to purchase goods and/or services . . . without ever transmitting to the merchant information, such as the person’s credit card number, or even the person’s name.” *Id.* (quoting Ex. 1101, 3:44–50).

Patent Owner does not substantively contest Petitioner’s proposed construction and relies on it to argue that the claim language does not read on the prior art. PO Resp. 28. Because Petitioner’s proposed construction is supported by the Specification as identified by Petitioner, we adopt this construction. Below, we further discuss aspects of the parties’ constructions as applied to the prior art. *See infra* at 16.

2. “Third party”

Patent Owner submits that the claimed “third party” must be exclusive of the secure registry, specifically “a party other than the entity, the provider, and the secure registry.” PO Resp. 24. As Patent Owner recognizes, we agreed with that construction in the Institution Decision. *Id.* (quoting Inst. 6–7). Petitioner does not appear to contest Patent Owner’s construction. Pet. Reply 14–19.

The term “third party” appears only in the claims, not elsewhere in the Specification. Patent Owner relies on the fact that the claims recite “third party” separately from “a secure registry,” “a provider,” and “an entity.” PO Resp. 24. Patent Owner also points out that the Specification describes “how the secure registry accesses and then transmits the user’s credit card or

bank account number to the credit card company (CCC) or bank, respectively.” *Id.* at 25 (citing Ex. 1101, 11:61–65, 12:29–31, 13:3–7, Fig. 7 (708), Fig. 8 (808), Fig. 9 (908)).

We agree the claim language supports that the separately recited “third party” must be different from the claimed “provider” and “entity.” As to the secure registry itself, we agree further with Patent Owner that the claim language mandates that the “third party” cannot be the secure registry system. The claims recite that the secure-registry processor is configured such that “account identifying information is provided to a third party.” By using “provided,” the claim instructs that the secure registry must send account-identifying information somewhere, not simply perform an additional operation on the information.⁵

Patent Owner further focuses on the party at issue. According to Patent Owner, the “third party” should be “a party other than one of these other parties already recited in the claims.” PO Resp. 24. Although the claims recite the “secure registry” as a system, as opposed to the “provider” and “entity,” which it recites as “parties,” we agree with Patent Owner that for a third party to be distinct from the secure registry, it should be distinct from whomever operates the secure registry. *See id.* at 24–25, 47–48 n.8; *infra* at 21.

Accordingly, we construe “third party” as “a party that is not the secure registry, the entity, or the provider.”

⁵ This restriction appears either as a capability of the processor (claims 1, 37, and 38) or as a separate step of the claimed method (claim 22)

C. OBVIOUSNESS OVER REBER AND FRANKLIN

As the primary reference, Petitioner relies on Reber, which discloses “a system for conducting secure financial transactions anonymously by utilizing proxy information representing a user.” Pet. 17. In particular, a user device in Reber transmits a transaction request that includes data representing the user and the merchant. Ex. 1131, 5:45–60. The data identifying the user includes both a personal identification code and a time-varying value. *Id.* at 4:14–20. Once a transaction request is transmitted to a remote computer, that computer may approve the transaction based on authenticating the user. *Id.* at 5:4–9, 5:16–32.

Petitioner further relies on Franklin, which “discloses a system for anonymous authentication of a party to a financial transaction using a randomly generated ‘transaction number’ in place of a user’s personal account information.” Pet. 18 (citing Ex. 1132, code (57)). The transaction number is used in place of a regular card number, and a merchant passes the transaction number to its bank, which in turn passes it to the user’s bank, the issuing institution. Ex. 1132, 2:35–38. The issuing institution uses information in the transaction number to identify the customer and generate matching information so it can authenticate the user and approve the transaction. *Id.* at 2:51–3:6. Franklin discloses that the acquiring bank (the merchant’s bank) “validates the authorization request by verifying that the merchant is a valid merchant.” *Id.* at 11:43–45. It also discloses that once the issuing bank’s system verifies the transaction number and substitutes the customer account number for the transaction number, the system performing authentication “then submits the authorization request to the bank’s

traditional processing system 84 for normal authorization processing.” *Id.* at 12:27–33.

Petitioner submits that Reber teaches most limitations of the challenged claims and that a skilled artisan would have incorporated certain teachings from Franklin to arrive at the claimed subject matter. Pet. 19–42. In particular, Petitioner submits that Franklin teaches merchant validation and that a skilled artisan had reason to incorporate merchant validation “as part of the validation process performed by the processor and database . . . to improve the security of the Reber system,” thereby “reducing fraud by merchants.” *Id.* at 37 (citing Ex. 1102 ¶ 114).

Additionally, Petitioner submits that a skilled artisan had reason to incorporate Franklin’s teaching to submit an authorization request to its traditional processing system “to complete the transaction.” *Id.* at 40–41.

Patent Owner argues that the combination of Reber and Franklin fails to render the challenged claims obvious for several reasons. PO Resp. 26–64. We address two limitations below, each of which is dispositive to certain unpatentability issues before us.

*1. Whether the prior art determines compliance
with any access restrictions for the provider*

Independent claim 1 requires the secure-registry processor be configured “to execute a restriction mechanism to determine compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request” and, based on that compliance, “to allow or not allow access to the secure data associated with the entity including information required to

enable the transaction.” Independent challenged claims 22 and 37 recite similar limitations. *See* Ex. 1101, claims 22, 37.

Petitioner submits that, although Reber does not discuss a restriction mechanism for the provider, skilled artisans would have understood that “both the merchant (provider) and the transacting user need to be valid in order to prevent fraud.” Pet. 36. Thus, reasons Petitioner, such artisans would have looked to Franklin, which “expressly discloses checking to ensure that the merchant has complied with access restrictions—and is therefore a valid merchant.” *Id.* at 37. Petitioner acknowledges that “merchant validation in Franklin takes place at the acquiring bank”—the merchant’s bank—and thus, not at the claimed secure registry as claimed. *Id.*; *accord* Ex. 1132, 11:43–46. According to Petitioner, however, skilled artisans “would have found it obvious to . . . implement merchant validation as part of the validation process performed by the processor and database.” *Id.*

Patent Owner argues also that Petitioner fails to justify combining Reber and Franklin such that the claim language would read on the combination. PO Resp. 42–45. In particular, Patent Owner argues the Petition gives no reason why skilled artisans “would add the alleged merchant validation found within Franklin’s acquiring bank into Reber’s secure registry, as opposed to, for example, following Franklin’s teaching of performing merchant validation at the acquiring bank.” PO Resp. 44.⁶ We agree.

⁶ Patent Owner argues that, properly construed, “access restrictions for the provider to secure data for the entity” requires multiple restrictions specific to the provider. PO Resp. 21–23, 38. We do not reach that issue because

The Petition states that it would have been obvious to perform merchant validation at the processor and database, but gives no reason for making that change. See Pet. 37. Instead, the Petition states a skilled artisan “would have applied the known techniques of Franklin to improve the security of the Reber system” and that doing so would have reduced fraud by merchants. *Id.* (citing Ex. 1102 ¶ 114). As explained, “the known techniques of Franklin” were to perform merchant validation at the merchant’s bank, not at the secure registry. Ex. 1132, 11:43–46 (“The acquiring bank validates the authorization request by verifying that the merchant is a valid merchant and that the credit card number represents a valid number.”). Thus, a reason to use Franklin’s techniques does not further justify modifying Franklin’s teaching to perform validation at the secure registry as claimed.

Petitioner attempts to justify the combination in the Reply, arguing that, in Franklin, “it would have been obvious simply to perform the merchant validation procedure at the issuing bank, depending on the needs of a particular implementation (for example, where the issuing bank and the acquiring bank are the same).” Pet. Reply 12–13. Petitioner reasons that “organizing the system in this way would . . . increase efficiency by reducing the overall number of computations (e.g., conducting only one validation/compliance operation and not two separate operations at two separate places).” *Id.* at 13. Those statements serve to highlight the deficiency of the Petition. Petitioner’s arguments in the Reply do not respond to Patent Owner, other than attempting to fill in a gap in the

we conclude Petitioner’s showing regarding access restrictions at the secure registry is inadequate regardless of the construction of “access restrictions for the provider to secure data for the entity.”

Petition. We agree with Patent Owner that Petitioner’s Reply arguments go too far beyond those of the Petition. *See* PO Sur-reply 15–16; 37 C.F.R. § 42.23(b) (2017); Trial Practice Guide Update 14–15 (Aug. 2018), <https://go.usa.gov/xU7GP> (“[A] reply . . . that raises a new issue or belatedly presents evidence may not be considered. . . . Examples of new issues are new theories or arguments necessary to make out petitioner’s case-in-chief . . . , such as a newly raised rationale to combine . . . that was not expressed in the petition.”); *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369–70 (Fed. Cir. 2016) (holding that the Board did not err in excluding a reply as improper under 37 C.F.R. § 42.23(b) because Petitioner relied on a new rationale to combine). Petitioner failed to make an adequate showing in the Petition regarding a plain requirement of the claims. The Petition identifies no prior-art disclosure that taught or suggested to skilled artisans to implement access restrictions at the secure registry, and provides insufficient reasons why a skilled artisan would have had reason to do so.

Thus, Petitioner fails to show that challenged claims 1, 22, or 37 would have been obvious. Because of dependency from those claims, we reach the same conclusion for challenged claims 2, 3, 16, 21, 23, and 24 (i.e., this conclusion applies to all challenged claims other than claim 38).

2. Whether the prior art teaches account-identifying information is not provided to the provider and is provided to a third party

Claim 1 requires restricted access to “secure data associated with the entity including information required to enable the transaction” and further that “the information includ[es] account identifying information, wherein the account identifying information is not provided to the provider and the

account identifying information is provided to a third party to enable or deny the transaction with the provider without providing the account identifying information to the provider.” The other independent challenged claims recite parallel limitations. *See* Ex. 1101, claims 22, 37, 38. These limitations have two aspects relevant here: (1) that account-identifying information required to enable the transaction not be provided to the provider (e.g., the merchant) and (2) that the information is provided instead to a third party.

Petitioner points to Reber’s system for verifying purchasers’ information, arguing that “the database could be controlled by anyone in possession of information sufficient to verify the user’s identity, including an independent third party and/or a financial service provider such as a bank that has access to the user’s account number, such as a credit or debit card number.” Pet. 40. Petitioner reasons further that, for a “database controlled by an independent third party, it would have been obvious to have the database interface with a separate financial institution (*i.e.*, an issuing institution) to complete the transaction.” *Id.* That conclusion, according to Petitioner, would have motivated skilled artisans to use Franklin’s teaching of passing a user’s account-identifying information to a traditional backend processing network. *Id.* at 40–41.

Patent Owner disputes Petitioner’s assertions, arguing that (1) “Reber and Franklin both teach that account identifying information is provided to a merchant provider” (PO Resp. 27–32); (2) neither Reber nor Franklin discloses providing information to a third party (*id.* at 45–48); and (3) Petitioner did not provide an adequate reason to modify Reber’s or Franklin’s teachings (*id.* at 33–35, 48–55).

a. Withholding “account identifying information” from the provider

As discussed above, we adopt Petitioner’s proposed construction for “account identifying information” as “personal information about an entity such as name, address, or account number.” *See supra* at 8. As Patent Owner submits, Reber discloses that, when a transaction is authorized, the authentication system transmits “a message indicating the transaction” to the provider that includes the purchaser’s name and address. PO Resp. 28–29 (quoting Ex. 1131, 6:18–25). Thus, under Petitioner’s construction, Reber discloses sending account-identifying information to the provider. *Id.*

Petitioner argues in response that the Specification includes embodiments in which personal information is sent to the provider or made public. Pet. Reply 2–3 (citing Ex. 1101, 12:57–62, 13:66–14:1, 17:34–38). But as Petitioner agrees, “[i]n other embodiments, personal information is withheld.” *Id.* at 3. Although Petitioner argues that the Specification is consistent with protecting only sensitive information, claim 1 requires simply that “the account identifying information is not provided to the provider and the account identifying information is provided to a third party to enable or deny the transaction with the provider without providing the account identifying information to the provider.” Thus, it is inapposite that the Specification discloses embodiments where personal information is shared. *See* PO Sur-reply 2.

Petitioner argues that claim 4, which depends from claim 1, “explicitly *requires* the secure registry to transmit address information to the provider.” Pet. Reply 2. Thus, according to Petitioner, claim 1 must encompass sharing address information but protecting other information such as an account number. *Id.* But as Patent Owner points out, claim 4

requires that the system “obtain the appropriate address for delivery of the item by the third party.” PO Sur-reply 2 (quoting Ex. 1101, claim 4) (emphasis omitted). Because the third party delivers the item, only it need receive address information. We agree with Patent Owner that claim 4 supports that address information is not shared with the provider.

Petitioner argues that Reber and Franklin both disclose protecting a user’s credit card number from the provider and therefore teach withholding account-identifying information from the provider. *See* Pet. Reply 4. In light of claim 1 treating “account identifying information” collectively (i.e., not distinguishing one type from another), that argument is not persuasive. Moreover, interpreting the claim to require withholding only some possible account-identifying information would render the limitation all but meaningless.

Petitioner argues further that because Reber discloses that a message allowing a transaction “can include” account-identifying information, Reber therefore discloses that such messages may not include account-identifying information. *Id.* at 4–5. We do not agree. Petitioner has not identified a disclosure in Reber that would enable a transaction without sending account-identifying information. Petitioner asserts that Reber’s “second data element,” although received by the provider, may be encoded with a time-varying value and thus remains protected from the provider. Pet. 41. But Petitioner does not address Reber’s disclosure of the message sent from the authenticating computer to the provider (Ex. 1131, 6:18–25 (“If the second data element is authentic, the computer 64 sends a message indicating the transaction to the first party.”)). It is that message that Reber discloses as

including account-identifying information sent to the provider. *See* PO Resp. 28–29.

Petitioner argues that understanding the possible fraud resulting from sending sensitive information would have motivated skilled artisans “to withhold such information in certain contexts (*e.g.*, where the merchant is known not to have taken adequate data security measures).” Pet. Reply 5. But that assertion lacks adequate support. Petitioner asks us to view the prior art as accommodating a wide-ranging interpretation sufficient to support Petitioner’s case, but we decline to do so without a sound basis in the references’ disclosures. Our conclusion is not that Petitioner asserts a reason to combine itself absent from the prior art, but that the prior art does not adequately support the predicate conditions Petitioner requires to support the asserted reason to combine.

Petitioner draws parallels between Franklin’s disclosures and those of the ’539 patent, arguing that Franklin’s “disclosure is consistent with the ’539 patent’s teaching that in some contexts, transmission of personal information is appropriate.” Pet. Reply 6. That position, however, does not address the express claim language, which prohibits transmission of account-identifying information.

We conclude Petitioner has not proven that Reber and Franklin teach that “the account identifying information is not provided to the provider.” As described above, this limitation appears in each independent challenged claim. Accordingly, Petitioner has failed to prove the unpatentability of any challenged claim.

b. Providing “account identifying information” to a third party

Regarding the requirement to send account-identifying information to a third party, Petitioner asserts that Reber’s database “could be controlled by anyone in possession of information sufficient to verify the user’s identity, including an independent third party.” Pet. 40. That assertion does not address the claim language, which requires that the secure registry system verify the user’s identity and then pass information to a third party. *See* Ex. 1101, claim 1 (“A secure registry system . . . comprising: . . . a processor configured to . . . map the time-varying multicharacter code to the identity of the entity .”). As we note above, the claimed “third party” must be distinct from the secure registry itself. *See supra* at 8; PO Resp. 46 n.7.

Petitioner argues further that if the database were controlled by an independent third party, “it would have been obvious to have the database interface with a separate financial institution (*i.e.*, an issuing institution) to complete the transaction.” Pet. 40. But Petitioner does not provide persuasive evidence why a person of skill would configure Reber’s system to require a third-party processor. The Petition asserts no benefit that would have come from using such a configuration instead of Reber’s integrated bank. *Id.*

Petitioner argues in the Reply that Reber discloses a third party because it discloses that “computer 64 directs that an account for the first party be credited by the transaction amount, and an account for the second party be debited by the transaction amount.” Pet. Reply 14–15 (quoting Ex. 1131, 6:25–28) (emphasis omitted). Patent Owner objects to that argument as newly made and inconsistent with those in the Petition. PO Sur-reply 17. Patent Owner argues also that Reber’s disclosure does not address

a third party enabling or denying the transaction, because Reber only discusses actions that the computer itself takes. *Id.* at 17–18.

We agree with Patent Owner. As an initial matter, the Petition did not identify Reber’s disclosure that its computer optionally “directs that” the relevant accounts be credited and debited (Ex. 1131, 6:25–28). Allowing Petitioner to rely on that disclosure only after Patent Owner contested the initial showing would improperly skew the process. *See* 37 C.F.R. § 42.104(b)(4) (requiring that the “petition must specify where each element of the claim is found in the prior art patents or printed publications relied upon”). Moreover, even considering Reber’s statement, we would find that it does not indicate what system controls the relevant accounts and therefore falls short of disclosing the “third party” limitation as claimed.

Petitioner asserts also that, in light of Reber’s disclosures, a person of skill would have been motivated to apply Franklin’s disclosure that “the user’s account identifying information is passed on to a traditional backend processing network.” Pet. 40–41 (citing Ex. 1132, 12:27–33). In the Institution Decision, we viewed Franklin’s “processing system 84” as functionally distinct from the claimed secure registry and therefore potentially serving as the claimed third party. Inst. 18. Patent Owner disputes that Franklin discloses a third party. PO Resp. 46–48. In Patent Owner’s view, Franklin discloses all components for user validation and transaction processing as within “bank computing center 32.” *Id.* at 46–47 (citing Ex. 1132, Fig. 7, 11:25–12:44). Patent Owner points out that Franklin does not disclose any entity that handles account identifying information, other than the customer, merchant, and bank computing center. *Id.* at 47–48. Patent Owner submits that the processing system is “coextensive with all

other components . . . of the bank computing center 32” and therefore coextensive with the claimed secure registry. PO Resp. 48 n.8. Petitioner, in response, submits that Franklin’s bank “could be physically distributed and controlled by different parties.” Pet. Reply 16.

Considering the record as a whole, we are not persuaded that Franklin discloses a third party that enables or denies the transaction. While Franklin’s “traditional processing system” provides functionality outside that of the components that make up Franklin’s secure registry, if that were sufficient to disclose the claimed third party, it would trivialize that claim element. Rather, as we explained above in our claim construction analysis of “third party,” we agree with Patent Owner that the claimed third party must operate independently from the secure registry. *See* PO Resp. 23–25; *supra* at 8. Because Franklin’s processing system is part of the bank computing center 32 (Ex. 1132, Fig. 7), it does not serve as a third party as claimed.

We further find that Petitioner has not adequately shown why a skilled artisan would have configured the system to separate user authentication and transaction enablement as claimed (the first performed by the secure registry and the latter performed by a third party). As discussed above, the Petition asserts that a skilled artisan would have understood that Reber’s database “could be” controlled by a third party. Pet. 40. It asserts that, “[i]n light of these suggestions in the prior art,” skilled artisans would have looked to Franklin. *Id.* We do not agree that a possible configuration alone gives reason to look to another reference.

In the Institution Decision, we cited to Petitioner’s statement that persons of skill had reason “to ensure that the transaction data provided to the merchant in Reber did not contain any account identifying information,

such as the user's account number,' and that doing so would 'protect[] the user's account information from misappropriation.'" Inst. 17 (quoting Pet. 41–42). Patent Owner argues that the Petition presents that reasoning only for withholding account-identifying information from the provider, not for submitting transaction enablement to a third party. PO Resp. 54. Upon consideration of the whole record, we agree with Patent Owner. The Petition discusses protecting information from the merchant "[s]eparately" from sending transaction enablement to a third party. Pet. 41. We conclude that the Petition lacks sufficient support for configuring the system to use a third party as claimed.

As to Petitioner's arguments in the Reply that skilled artisans would have configured the system as claimed, we agree with Patent Owner that Petitioner made those arguments too late. Petitioner submits for the first time in the Reply that the claimed arrangement would "minimize changes to the software running existing processing systems." Pet. Reply 18–19; *see* PO Sur-reply 20. Such reasoning, though, is not merely an expansion of what was in the Petition. We consider it too far afield and thus do not consider Petitioner's late arguments. *See* Trial Practice Guide Update 14–15

For the reasons discussed, we conclude that Petitioner has not proven that it would have been obvious to provide account-identifying information to a third party to enable or deny the transaction with the provider. Thus, Petitioner fails to show that challenged claims 1, 22, 37, or 38 would have been obvious. Because of dependency from those claims, we reach the same conclusion for challenged claims 2, 3, 16, 21, 23, and 24. Accordingly, our conclusion applies to all challenged claims.

D. PATENT OWNER’S CONDITIONAL MOTION TO AMEND

Patent Owner filed a Conditional Motion to Amend. Paper 21.
Because we conclude that Petitioner has not proven any claim unpatentable, we do not reach Patent Owner’s Motion and therefore dismiss it as moot.

E. PATENT OWNER’S MOTION TO STRIKE

Patent Owner filed a Motion to Strike certain evidence and argument associated with Petitioner’s Sur-reply to Patent Owner’s Conditional Motion to Amend. Paper 39. Because we do not reach Patent Owner’s Conditional Motion to Amend, Patent Owner’s Motion to Strike is moot and we dismiss it as such.

III. CONCLUSION

For the reasons discussed above, we conclude Petitioner has not proven any of the challenged claims unpatentable over the prior art of record.

In summary:

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–3, 16, 21–24, 37, 38	103	Reber, Franklin		1–3, 16, 21–24, 37, 38

Motion to Amend Outcome	Claims
Original Claims Cancelled by Amendment	
Substitute Claims Proposed in the Amendment	1–3, 16, 21–24, 38
Substitute Claims: Not Reached	1–3, 16, 21–24, 38

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–3, 16, 21–24, 37, and 38 of U.S. Patent No. 8,856,539 B2 are not determined to be unpatentable;

FURTHER ORDERED that Patent Owner’s Conditional Motion to Amend is *dismissed*;

FURTHER ORDERED that Patent Owner’s Motion to Strike is *dismissed*; 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.

IPR2018-00812
Patent 8,856,539 B2

For PETITIONER:

Monica Grewal
Benjamin Fernandez
Mark Selwyn
WILMER CUTLER PICKERING HALE AND DORR LLP
monica.grewal@wilmerhale.com
ben.fernandez@wilmerhale.com
mark.selwyn@wilmerhale.com

For PATENT OWNER:

James M. Glass
Tigran Guledjian
Christopher Mathews
Nima Hefazi
Richard Lowry
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
tigranguledjian@quinnemanuel.com
chrismathews@quinnemanuel.com
nimahefazi@quinnemanuel.com
richardlowry@quinnemanuel.com