Paper No. 31

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

UNIVERSAL SECURE REGISTRY LLC,

Patent Owner

Case IPR2018-00809

U.S. Patent No. 9,530,137

PATENT OWNER'S REPLY IN SUPPORT OF ITS MOTION TO AMEND PURSUANT TO 37 C.F.R. § 42.121

TABLE OF CONTENTS

Page

PATENT OWNER'S LIST OF EXHIBITS III
I. INTRODUCTION 1
II. PETITIONER'S ARGUMENTS FOR DENIAL OF SUBSTITUTE CLAIMS HAVING FEATURES THAT OVERLAP WITH DISCLAIMED CLAIMS 8 AND 11 ARE MERITLESS 1
A. Substitute Claims Respond to a Ground of Unpatentability 2
B. Estoppel and Waiver Do Not Apply 6
C. Patent Owner Satisfies Its Duty of Candor 7
III. SUBSTITUTE CLAIMS DIRECTED AT UNCHALLENGED CLAIMS 8
IV. SUBSTITUTE CLAIMS ARE PATENT ELIGIBLE UNDER § 101 8
V. SUBSTITUTE CLAIMS ARE NOVEL AND NONOBVIOUS 13
A. It Would Not Have Been Obvious to Have the Claimed "Second Device" Map the ID Code to a Card or Account Number 14
B. Using "Three Separable Fields" Is Not Obvious 16
C. Substitute Dependent Claim 18 Is Not Obvious 19
D. Petitioner Fails to Address Substitute Claims 17 and 20 21
VI. SUBSTITUTE CLAIMS SATISFY 35 U.S.C. § 112 21
VII. CONCLUSION 25

TABLE OF AUTHORITIES

Page

Cases

Alice Corp. Pty. Ltd. v. CLS Bank Int'l,
134 S. Ct. 2347 ____ 12

Apple Inc. et al. v. Valencell, Inc.,
IPR2017-00321, Paper 44 _____ 6

Aqua Products, Inc. v. Matal,
872 F.3d 1290 (Fed. Cir. 2017) 20, 21

Ariosa Diagnostics v. Verinata Health, Inc.,
805 F.3d 1359 (Fed. Cir. 2015) 21

Ex parte Levy,
17 USPQ2d 1461 (Bd. Pat. App. & Inter. 1990) 20

Universal Secure Registry, LLC v. Apple, Inc.,
1:17-cv-00585-JFB-SRF, Dkt. 137 (D. Del. Sep. 18, 2018) 9

Statutory Authorities

35 U.S.C. § 112 21

Rules and Regulations

37 C.F.R. § 42.121 i

Other Authorities

Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,767 (Aug. 14, 2012) 7

PATENT OWNER'S LIST OF EXHIBITS

Ex. 2001	Declaration of Dr. Markus Jakobsson in Support of Patent Owner's Preliminary Response.
Ex. 2002	Curriculum Vitae of Dr. Markus Jakobsson.
Ex. 2003	USR Disclaimer Filed July 6, 2018.
Ex. 2004	Declaration ISO Motion Pro Hac Vice Harold Barza.
Ex. 2005	Declaration ISO Motion Pro Hac Vice Jordan Kaericher.
Ex. 2006	U.S. Application No. 15/019,660.
Ex. 2007	U.S. Application No. 11/677,490.
Ex. 2008	U.S. Provisional Application No. 60/775,046.
Ex. 2009	U.S. Provisional Application No. 60/812,279.
Ex. 2010	Declaration of Dr. Markus Jakobsson in Support of Patent Owner's Response.
Ex. 2011	Deposition Transcript of Dr. Victor John Shoup.
Ex. 2012	N. Asokan, et. al, The State of the Art in Electronic Payment Systems, IEEE Computer, Vol. 30, No. 9, pp. 28-35 (IEEE Computer Society Press, Sept. 1997).
Ex. 2013	M. Baddeley, Using E-Cash in the New Economy: An Economic Analysis of Micropayment Systems, J. Electronic Commerce Research, Vol. 5, No. 4, pp. 239-253 (Nov. 2004).
Ex. 2014	Declaration of Dr. Markus Jakobsson ISO PO's Conditional Motion to Amend.

Ex. 2015	U.S. Provisional Application No. 60/859,235.
Ex. 2016	U.S. District Court for Delaware Report and Recommendation.
Ex. 2017	Deposition Transcript of Dr. Markus Jakobsson.
Ex. 2018	A. Juels and M. Sudan, "A Fuzzy Vault Scheme."
Ex. 2019	Deposition Transcript (Rough) of Dr. Ari Juels.
Ex. 2020	U.S. Patent No. 8,495,372.
Ex. 2021	Declaration by Dr. Markus Jakobsson ISO Reply to Motion to Amend.

Universal Secure Registry LLC ("Patent Owner") submits this Reply in support of its Conditional Motion to Amend, Paper 19 ("Mot."), and in response to Petitioner's Opposition to Patent Owner's Conditional Motion to Amend, Paper 24 ("Op").

I. INTRODUCTION

Petitioner advances a myriad of baseless arguments against the patentability of some of Patent Owner's substitute claims, while completely failing to address other substitute claims at all (and hence conceding their patentability). Petitioner also improperly attempts to incorporate substantive arguments from its Petition (and its expert's declaration in support thereof) in a flagrant attempt to circumvent this Board's order on page limits. *See* Paper No. 17. Petitioner's opposition lacks any merit whatsoever as the majority of its arguments either have been already rejected by this Board (or the district court), or are specious attacks on the propriety of Patent Owner's presentation of the substitute claims.

II. PETITIONER'S ARGUMENTS FOR DENIAL OF SUBSTITUTE CLAIMS HAVING FEATURES THAT OVERLAP WITH DISCLAIMED CLAIMS 8 AND 11 ARE MERITLESS

The Petitioner first argues that Patent Owner's substitute claims 13 and 21 "recite subject matter that is virtually identical to the now-disclaimed subject matter by dependent claims 8 and 11." Op. at 2. Petitioner then argues that the substitute

claims should be denied because: the substitute claims fail to respond to a ground of unpatentability under 37 C.F.R. § 42.121(a)(2)(i); Patent Owner is estopped from reintroducing subject matter of disclaimed claims 8 and 11; and Patent Owner has "violated" its duty of candor with the Board for taking a position in its Motion that is inconsistent with its Patent Owner's Preliminary Response (POPR). *See* Op. at 3-6. The Petitioner also argues that USR should be deemed to have waived any arguments relating to Ground 3 and, as such, USR "has conceded limitations 13[c], 13[e], 21[d], and 21[f] [as] obvious under Ground 3." *Id.* Petitioner's arguments for denial of the substitute claims or waiver of potential arguments are meritless.

A. Substitute Claims Respond to a Ground of Unpatentability

First, substitute claims 13 and 21 are not "virtually identical" to the disclaimed subject matter of claims 8 and 11. For instance, substitute claims 13 and 21 both recite "a multi-digit identification (ID) code allowing **a networked validation-information entity** to map the multi-digit ID code," while disclaimed claim 8 recites, "a multidigit **public** ID code for a credit card account, which a **credit card issuer** can map…" *Compare* Motion at A1 (claim 13) and A4 (claim 21) *with* Ex. 1101 at 46:34-37 (claim 8) (emphasis added). Thus, in substitute claims 13 and 21, a "networked validation information entity" maps the multi-digit ID code, while in claim 8, a *credit card issuer* performs the mapping of a multidigit public ID code.

This distinction is important because substitute claims 13 and 21 further specify that **the networked validation-information entity is the claimed "second device"** that is configured to enable the credit and/or debit card [or financial] transaction based on authentication of the user. Motion at A1 (claim 13) and A4 (claim 21). Thus, in these substitute claims, the *same* entity—the networked validation-information entity—responsible for mapping the multi-digit ID code is also responsible for enabling the financial transaction.

By contrast, claims 8 and 11 taken together[1] do not specify that the *credit card issuer*, which performs the mapping (claim 8) operation, is the second device (the networked validation-information) that "approve[s] or den[ies] [the] financial transaction[]" (claim 11). Rather, claims 8 and 11 taken together merely require that a credit card issuer perform the mapping while separately the second device, which is the networked validation-information entity, approves/denies the financial transaction. *See* Ex. 1101 at 46:34-37, 46:50-54.

[1] Claims 8 and 11 do not have interdependency and instead separately depend from claim 1. Thus, Petitioner also neglects the impact that subject matter from these claims (that may exist in substitute claims 13 and 21) have on the substitute claims *taken as a whole*.

Indeed, **Petitioner contradicts itself** by vehemently arguing that claim limitations 13[e] and 21[f] lack written description support "because the original disclosure does not show a financial institution [*e.g.*, credit card issuer] being a networked validation-information entity." Op. at 23-24. If Petitioner believes that a financial institution, such as a "credit card issuer," is different from a "networked validation-information entity" for written description purposes, then it cannot in the same breath argue that the two terms are "virtually identical" in attempting to establish that Patent Owner purportedly fails to respond to Ground 3.

Second, substitute claim 13 additionally recites "the first processor is programmed to generate one or more signals having at least three separable fields that include…" This limitation responds to Ground 1 of unpatentability because, among other things, Jakobsson, which purportedly discloses "first authentication information," "indicator of biometric authentication," and "time varying value" (*see* Petition at 30-33; Inst. Dec. (Paper 9) at 11), fails to disclose that the inputs (*e.g.*, P, K, T, E, etc.) to its combination function generate an authentication code with at least three separable fields. *See discussion infra* Section V; *see also* Motion at 11-12. The Board has indicated that 37 C.F.R. § 42.121(a)(2)(i) "does not require, however, that every word added to or removed from a claim in a motion to amend be solely for the purpose of overcoming an instituted ground," and that "once a

proposed claim includes amendments to address a prior art ground in the trial, a patent owner also may include additional limitations." *Western Digital Corp. v. SPEX Tech.*, IPR2018-00082, -00084, Paper 13 at 6. Consequently, even if the limitations identified by Petitioner related to "financial transaction" and "credit and/or debit card transaction" did not address a ground of unpatentability, these amendments are valid and includable by virtue of the "separable fields" amendment, which Petitioner does not dispute responds to a ground of unpatentability.

Third, as to substitute claim 21, disclaimed claims 8 and 11 did not depend from independent claim 12, which substitute claim 21 proposes to replace. As such, no ground in the Petition was directed at a dependent claim that depended from claim 12 and also included the subject matter of claims 8 and 11. Thus, in addition to the aforementioned differences between the subject matter of claims 8 and 11 and the amended features of limitations 13[c], 13[e], 21[d], and 21[f], differences between independent claims 1 and 12 also merit denial of Petitioner's argument that substitute claim 21 should be denied for failing to respond to Ground 3 of unpatentability.

Lastly, the amended features of limitations 13[c], 13[e], 21[d], and 21[f] do respond to Ground 3 of unpatentability because the combination of Jakobsson, Maritzen, and Schutzer fail to disclose several claimed features. *See discussion infra* Section V. Thus, even if Patent Owner had failed to respond to Ground 3 of

unpatentability in its Motion (because it disclaimed the claims subject to Ground 3), it does so now expressly here in its Reply. *See Apple Inc. et al. v. Valencell, Inc.*, IPR2017-00321, Paper 44 at 53-54 (Patent Owner did not address a ground of unpatentability in its MTA, but Patent Owner satisfied its burden with arguments made in its Reply brief).

B. Estoppel and Waiver Do Not Apply

Patent Owner is not estopped from submitting the pending substitute claims. As a preliminary matter and contrary to Petitioner's assertions (*see* Op. at 5), the substitute claims include claim limitations that are substantively different than disclaimed claims 8 and 11 and for at least this reason Petitioner's arguments concerning estoppel (or waiver) do not apply. *See discussion supra* Section II.A.

Petitioner alleges that "USR's current position is clearly inconsistent with USR's earlier position in the instant proceeding." However, Patent Owner has not taken any "position" in the past that now contradicts its stance that the substitute claims are patentable in view of the prior art. For instance, Patent Owner has never stated that the subject matter of claims 8 and 11 is obvious in view of prior art or were unpatentable for any other reason. Instead, on July 6, 2018, Patent Owner submitted a disclaimer under 37 C.F.R. § 1.321(a) disclaiming claims 8, 10, and 11 of the '137 Patent (Ex. 2003). Patent Owner then stated in its POPR that it

"maintains [that claims 8 and 11] are valid" but that Ground 3 was moot in view of the disclaimer. Paper 8 at 32. Patent Owner has taken no conflicting positions.

Moreover, Patent Owner does not "derive an unfair advantage and impose an unfair detriment on Petitioner" because it allegedly "avoided full, fair, and timely consideration of Ground 3" or the Board somehow "was persuaded to refrain from addressing the merits of Ground 3." Op. at 5. If Petitioner believes the arguments it made with respect to the combination of Jakobsson, Maritzen, and Schutzer in Ground 3 apply to the substitute claims, it may raise those arguments—and any other *new* argument—in its Opposition. *Office Patent Trial Practice Guide*, 77 Fed. Reg. 48,756, 48,767 (Aug. 14, 2012). Indeed, Petitioner did just that. *See* Op. at 17-23.

Petitioner further argues that Patent Owner has "waived any arguments relating to Ground 3…and amended limitations 13[c], 13[e], 21[d], and 21[f]" because "[t]he Board's Trial Practice Guide states that 'any arguments for patentability not raised in the [Patent Owner's Response] may be deemed waived.'" Op. at 5-6 (citing Trial Practice Guide Update, 83 Fed. Reg. 38,989). Petitioner's argument is meritless: Patent Owner's CMTA is not a POR, and any arguments Patent Owner did not include in its POR do not affect Patent Owner's ability to respond to invalidity arguments presented in Petitioner's Opposition.

C. Patent Owner Satisfies Its Duty of Candor

Petitioner fails to establish that Patent Owner has violated its duty of candor with the Board. As previously discussed, Patent Owner does not "contradict its arguments in its POPR that the validity of such subject matter was moot" as Petitioner alleges. Op. at 6; *see discussion supra* Section II.B. Also, the substitute claims recite limitations that are substantively different than the subject matter of disclaimed claims 8 and 11. *See discussion supra* Section II.A. Petitioner's contention that Patent Owner violated 37 C.F.R. § 42.51(b)(1)(iii) is also baseless. This rule relates to discovery between parties and a duty of one party to serve relevant information concerning inconsistencies, not to any duty of candor.

III. SUBSTITUTE CLAIMS DIRECTED AT UNCHALLENGED CLAIMS

Per the conference call the parties had with the Board on April 22, 2019, all substitute claims directed at unchallenged claims are void.

IV. SUBSTITUTE CLAIMS ARE PATENT ELIGIBLE UNDER § 101

Petitioner argues that substitute claims 13-21 are unpatentable under § 101 because they purportedly claim patent-ineligible abstract ideas. Op. at 8-14. However, on September 19, 2018, United States Magistrate Judge Sherry R. Fallon for the District Court of Delaware issued a Report and Recommendation (R&R) rejected virtually identical arguments made by Petitioner, and recommending that the District Court deny Petitioner's motion to dismiss under § 101 since claims 1-12

of the '137 Patent are "**not** directed to an abstract idea because 'the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity.'" Ex. 2016, *Universal Secure Registry, LLC v. Apple, Inc.*, 1:17-cv-00585-JFB-SRF, Dkt. 137 at 21 (D. Del. Sep. 18, 2018) (emphasis added). Specifically, Judge Fallon stated that:

> [t]he '137 patent is directed to an improvement in the security of mobile devices by using biometric information to generate a time varying or other type of code that can be used for a single transaction, preventing the merchant from retaining identifying information that could be fraudulently used in subsequent transactions. ('137 patent, col. 18:14-34) **While certain elements of claim 12 recite generic computer components, the claim as a whole describes an improved authentication system with increased security**.

Id. at 22 (emphasis added). As such, substitute claims 13 and 21, which are narrower than claims 1 and 12, are patent eligible for the same reasons. Ex. 2021 at ¶ 29.

This Board also reached the same conclusion of patent eligibility when it rejected substantially similar arguments made by Petitioner for related U.S. Patent 8,577,813 ("the '813 Patent") in CBM2018-00026. CBM2018-00026, Paper 10 at 23-24. Indeed, in its Petition for CBM2018-00026, Petitioner advanced the same abstract idea of "verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction" as it does

here now, and also cited to the same cases making substantially similar arguments for patent ineligibility. The Board's reasoning for dismissing these arguments in CBM2018-00026, and finding the claims of the '813 Patent are not abstract, applies equally to the present substitute claims.

For instance, Petitioner has oversimplified the claimed inventions and ignores many recited key claim limitations. Ex. 2021 at ¶¶ 30-34. The specification shows that the substitute claims are directed to specific, concrete, technological improvements **to secure distributed transaction approval systems that incorporate both local and remote authentication without compromising the user's sensitive information**, and these inventions are demonstrably valid under the analysis of *Alice* and its progeny. *Id.* **Moreover, the problems addressed by the '137 Patent are firmly rooted in technological challenges associated with distributed electronic transactions, and so are the claimed solutions**. *Id.*

By arguing that the substitute claims are directed to the abstract idea of "verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction" (Op. at 10), Petitioner fails to account for multiple claim requirements. Substitute claims 13 and 21 recite a unique and highly secure distributed transaction approval system including a local "first device" that authenticates a user of the device based on "secret information" (e.g., a

PIN code) and retrieves or receives "biometric information" (e.g., a fingerprint captured by the "biometric sensor" of the first device) before the first device generates and wirelessly transmits a transaction approval request "signal" to a remote "second device." *Id.* at ¶ 32. This signal includes at least three specific types of data: "first authentication information," an "indicator of biometric authentication" of the user by the first device, and a "time varying value." The remote second device receives the signal and, based on the specific data contained therein, as well as the user's "second authentication information" available at the second device, the second device may provide the first device with an "enablement signal" indicating the second device's approval of the transaction. Petitioner's proffered overbroad abstract idea does not capture these recited features. *Id.*

Petitioner also fails to explain how the ordered combination of elements in the claims manifestly claim no more than Petitioner's purported abstract idea. Although it is true that the "mere recitation of a generic computer" cannot transform a method claim directed to a patent-ineligible abstract idea into a system claim directed to a patent-eligible invention, *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2358, the substitute claims do more than merely state "an abstract idea while adding the words 'apply it.'" Instead, they recite a specific, concrete, technological solution providing an improved secure distributed transaction approval system that

incorporates both local and remote authentication without compromising the user's sensitive information. *Id.* at ¶ 33. Thus, Petitioner fails to adequately address that the claimed "biometric information" and "indicator of biometric authentication" are specifically employed in two ways: the former used to *locally* authenticate the user of the first device, and the latter used to *remotely* authenticate the first device by the second device when the indicator of biometric authentication is used to generate one or more signals that are sent to the second device. Further, the claims do not preempt the field of secure electronic transactions, but instead cover very specific technologies used on specialized devices (*e.g.*, with biometric sensors), while leaving open other known or unknown technology for conducting such transactions. *Id.*

Even assuming the substitute claims are directed to the Petitioner's abstract idea, the ordered combination of elements in these claims "transform the nature of the claim into a patent-eligible application." *Id.* at ¶ 34. Petitioner does not substantively address the claims as an ordered combination. *See* Op. at 14-17. By contrast, the '137 Patent's specification teaches that the ordered combination of elements do much more than merely recite an abstract idea or a rudimentary prior art verification system. *See, e.g.,* Ex. 1101 at 2:50-52, 3:63-5:31, 13:62-14:53, 15:43-50, 16:49-17:54, 18:13-34, 19:45-20:37, 22:16-20, 29:21-44, 32:31-34:6.

Instead, the ordered combination of claim elements recite a highly secure distributed transaction approval system including a local "first device" that authenticates a user of the device based on "secret information" (e.g., a PIN code) and retrieves or receives "biometric information" (*e.g.*, a fingerprint captured by the "biometric sensor" of the first device) before the first device generates and wirelessly transmits a transaction approval request "signal" to a remote "second device" that includes at least three specific types of data. Ex. 2021 at ¶ 34. The remote second device may then provide the first device with an "enablement signal" indicating the second device's approval of the transaction based on the data contained in the "signal." *Id.* For these reasons, the substitute claims are patent eligible.

V. SUBSTITUTE CLAIMS ARE NOVEL AND NONOBVIOUS

Not only do the substitute claims respond to a ground of unpatentability, they are clearly distinguishable over the prior art of record. As discussed above, the substitute claims further specify that the networked validation-information entity is the claimed "second device" that is configured to enable the credit/debit/financial transaction based on authentication of the user. The substitute claims further recite that the first authentication information included a multi-digit identification (ID) code allowing the networked validation-information entity to map the multi-digit ID code to a credit/debit card (or financial account) number. Substitute claim 13

additionally recites that the first processor is programmed to generate one or more signals "having at least three separable fields" that include the first authentication information, an indicator of biometric authentication, and a time varying value. Contrary to Petitioner's assertions (Op. at 17-23), and as described in more detail below, these amendments patentably distinguish the substitute claims over the Jakobsson, Maritzen, and Schutzer references. Ex. 2021 at ¶¶ 35-43.

A. It Would Not Have Been Obvious to Have the Claimed "Second Device" Map the ID Code to a Card or Account Number

Petitioner fails to present **any arguments** in its Opposition with respect to the newly added limitation in substitute claims 13 and 21 that "the first authentication information include[ed] 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/financial account] number," but instead refers **solely** to the arguments made its Petition with respect to disclaimed claims 8 and 11. Op. at 17-18. Even if this cross-reference (and apparent incorporation by reference) were proper,[2] Petitioner has

[2] Patent Owner objects to Petitioner's naked incorporation of arguments made in its Petition for this limitation (as well as limitations 13[pre], 13[g], 13[h], 21[pre], 21[h], and 21[i] (*see* Op. at 20) and substitute claim 18 (*see* Op. at 21)) as a blatant

failed to establish this limitation is obvious in view of Jakobsson, Maritzen, and Schutzer.

Disclaimed dependent claim 8 recited a multidigit public ID code for which "**a credit card issuer** can map to a usable credit card number." Ex. 1001 at Cl. 8. Substitute claims 13 and 21, on the other hand, require "a networked validation-information entity" to perform the mapping. This is a critical distinction because Petitioner acknowledges (1) that Jakobsson fails to show or reasonably suggest this claimed feature (*see* Pet. at 64), and (2) Schutzer merely discloses that the "card issuer" can associate an "anonymous card number" with the "proper cardholder." *See* Pet. at 65. At no point in the Petition (or in its Opposition to Patent Owner's MTA) does Petitioner point to any disclosure of the "**networked validation-information entity**"[3] performing the mapping between multi-digit ID code to a

---

circumvention of this Board's order on page limits. *See* Paper No. 17. Petitioner's incorporated arguments with respect this these limitations should therefore be disregarded.

[3] Importantly, the claimed "networked validation-information entity" in the substitute claims is the same claimed "second device" that is "configured to enable

[credit and/or debit card/financial account] number. Ex. 2021 at ¶ 37. Petitioner had therefore failed to meet its burden to establish any of the substitute claims are obvious.

B. Using "Three Separable Fields" Is Not Obvious

Substitute claim 13 recites that the claimed "one or more signals" has "at least three separable fields" that include "the first authentication information, an indicator of biometric authentication, and a time varying value in response to valid authentication of the first biometric information." Petitioner alleges that Jakobsson discloses this claimed feature (Op. at 18), but Jakobsson merely discloses transmitting a unitary authentication code (either **one of** code 291, 292, or 293) to verifier 105. Ex. 1113 at ¶¶[0060], [0071]. In other words, there is no disclosure in Jakobsson of transmitting authentication code 291, **in addition to** the values (E) and

---

the financial transaction based on authentication of the user." Petitioner fails to even allege that the prior art of record includes such an entity, nor could it since neither Jakobsson, Maritzen, nor Schutzer, alone or in combination, suggest using the same entity to both map the multi-digit ID to a card/account number and enable the financial transaction.

(T), all in the same transmission. Ex. 2021 at ¶ 38.

Moreover, as explained in more detail in Patent Owner's sur-reply, Petitioner's mapping of the three recited types of information would require transmitting authentication code 291 (Petitioner's alleged "first authentication information"), **in addition to** the values (E) (Petitioner's alleged "indicator of biometric authentication") and (T) (Petitioner's alleged "time varying value"), all in the **same transmission**—which of course is not disclosed in Jakobsson.[4] *Id.* at ¶ 39.

Moreover, as explained by the author of the reference, Dr. Jakobsson, "[t]he one-way function is a ***critical aspect*** of [the invention described in the Jakobsson reference]." Ex. 2017 at 127:6-20; Ex. 2021 at ¶ 40. While certain embodiments of Jakobsson discuss prepending and appending certain inputs, a one-way function is always used (optionally in conjunction with other functions). Dr. Jakobsson explained that a person of ordinary skill in the art would understand that all the

[4] In its Opposition, Petitioner now appears to cite to (E), (T), and (P) as the three claimed types of information, but does not explain why "user data value (P)" can qualify as the claimed "first authentication information." Op. at 18. Regardless, there is no disclosure in Jakobsson that the unitary authentication code includes "three separable fields" after the code is generated and transmitted.

examples given involve a one-way function because otherwise the system would not be secure. Ex. 2017 at 134:1-13; *see also id.* at 134:19-135:7 (explaining that it would be "clear to a person of skill in the art reading this that there has to be a one-way function"). Even Petitioner's new expert, Dr. Juels, acknowledged at his deposition that merely concatenating or XOR'ing inputs together, without more, was an inadequate way to generate or protect the authentication code from eavesdroppers. Ex. 2019 at 30:3-21 (eavesdropper can recover inputs if mere concatenation were used); 34:12-36:12 (same); 40:14-41:6 (adversary can recover input if mere XOR is used as the combination function).

Since a one-way function must be used at some point during the authentication code generation process in Jakobsson, the resultant **unitary authentication code** does not have three separable fields that include all three pieces of claimed information. Ex. 2021 at ¶ 41. In other words, a POSITA would not recognize Jakobsson's system to transmit a code as having three separable fields including the first authentication information, an indicator of biometric authentication, and a time varying value because the combination function transformed those pieces of

information into a unitary authentication code prior to transmission.[5] *Id.*

C. Substitute Dependent Claim 18 Is Not Obvious

Substitute claim 18 recites "the first authentication information further including a digital signature generated using a private key associated with the first device." Petitioner alleges this limitation is obvious in view of Schutzer, which discloses that "the issuing bank 8 can require more secure authentication, such as … digital signatures." Op. at 21-23. Regardless of whether the "issuing bank" might require more secure authentication, 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. Schutzer is **completely silent** as to how the issuing bank receives the digital signature (and no

[5] Moreover, Petitioner's own expert, Dr. Juels, testified that it would be computationally difficult to derive the inputs from the output of a one-way function, like the one-way functions described in Jakobsson. Ex-2019 at 70:6-71:10, 79:4-24. Since one cannot easily derive the inputs of a one-way function from its output, the authentication code described in Jakobsson does not have "three separable fields" or include the claimed three distinct types of information. Ex. 2021 at fn. 3.

disclosure that it is through the claimed "networked validation-information entity"), how the digital signature is generated, and whose private key (if any) is used. Ex. 2021 at ¶¶ 41-43.

In particular, no express or inherent[6] disclosure is made that the digital signature of Schutzer was generated using a private key associated with the first device. "[Section] 316(e) unambiguously requires the petitioner to prove all propositions of unpatentability, **including for amended claims**." *Aqua Products, Inc. v. Matal*, 872 F.3d 1290, 1296 (Fed. Cir. 2017) (emphasis added). Here, Petitioner's failure to address the claim limitation "a digital signature **generated using a private key associated with the first device**" represents an incurable defect to its *prima facie* case of unpatentability of substitute claim 18. Moreover, Petitioner

[6] No inherent disclosure is made in Schutzer that the digital signature is *necessarily* generated by a private key associated with the first device. *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (requiring that the inherent characteristic necessarily flow from the teachings of the prior art). Indeed, Schutzer's digital signature may be generated ***using the private key of a certificate authority*** and be used as part of a digital certificate to authenticate the user, as was common practice at the time of the Schutzer invention. Ex. 2021 at fn. 4.

cannot introduce new arguments in its sur-reply in an attempt to fill holes in its *prima facie* showing. *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1367 (Fed. Cir. 2015) (Affirming Board's rejection of Petitioner's reliance on "previously unidentified portions of a prior-art reference to make a meaningfully distinct contention" in its Reply). Accordingly, the record fails to demonstrate that the prior art discloses or renders obvious this limitation, and Petitioner has failed to meet its burden to show dependent claim 18 is obvious.

D. Petitioner Fails to Address Substitute Claims 17 and 20

Substitute claims 17 and 20 have both been substantively amended from their original forms, yet Petitioner fails to address the patentability of these substitute claims in view of the prior art. Since these claims recite new features not found in any of the prior art of record (Ex. 2021 at ¶ 44), Petitioner's failure proves fatal to its opposition; substitute claims 17 and 20 should therefore be granted. *Aqua Products,* 872 F.3d at 1296; *Ariosa Diagnostics*, 805 F.3d at 1367.

VI. SUBSTITUTE CLAIMS SATISFY 35 U.S.C. § 112

Petitioner contends that the claim limitation "the second device being the networked validation-information entity configured to enable the credit and/or debit card [or financial] transaction based on authentication of the user" does not have written description support because "the original disclosure does not show a

financial institution being a networked validation-information entity." Op. at 23-24. Petitioner's entire § 112 argument as to claims 13 and 21 hinges on the mistaken assumption that the claimed networked validation-information entity **must be** a financial institution. *See id.* Petitioner's error proves fatal to its opposition.

While the claimed networked validation-information entity may be a financial institution, such as a credit card company (CCC),[7] the specification supports an embodiment where the networked validation-information entity is not a credit card company and instead acts as a secure registry that serves to enable or deny credit/debit transactions by authenticating a user. Ex. 2021 at ¶ 46. For instance, the specification explicitly teaches that the system may comprise "**a networked credit card validation-information entity configured to approve and deny financial transactions based on authentication of the user**." Ex. 2006 at 10:27-29 (emphasis added). Similarly, the specification also describes how a universal secure registry (USR) performs substantially the same function as the networked

[7] Patent Owner's expert, Dr. Jakobsson, explains that a credit card company (CCC) may be a "*non-limiting, non-exclusive example* of a 'networked validation-information entity.'" Ex. 2021 at fn. 5. As such, the latter is not limited to a CCC.

credit card validation-information entity because the USR authenticates a user to approve/deny a financial transaction by determining whether a code it received from the user is valid. *Id.* at FIG. 7 (708), 23:20-24:11.[8] The specification also describes a "second device" that—like the USR and networked credit card validation-information entity—performs authentication of a user (*e.g.*, first device). *See, e.g.*, *id.* at 6:26-33, 38:11-14, 43:27-29, 44:3-12, 45:7-46:2. Thus, the specification provides ample support for a POSITA to understand that the inventor was in possession of the idea that a networked validation-information entity could be a "second device" (or a secure registry) that enables a credit/debit/financial transaction based on authentication of the user. Ex. 2021 at ¶ 46.

Claim limitations 13[pre], 13[c], and 13[e] together also require that first authentication information includes a multi-digit ID code and the networked validation-information entity map the multi-digit ID code to a credit and/or debit card number to enable the credit/debit card transaction. *See* Motion at B1. The specification discloses that a code, which has multiple digits and serves to identify the user, is first transmitted from the user's electronic ID device to the merchant, and is ultimately sent to the USR (*e.g.*, networked validation-information entity). *Id.* at

[8] *See* Motion at 7-8 (multiple citations to Ex. 2006 for 13[pre], 13[c], 13[e]).

FIG. 7, 23:23-30 ("[The user] presents the electronic ID device **with the code** to the merchant…The merchant transmits to the credit card company (1) **the code from the electronic ID device**…The credit card company takes this information and passes **the code from the electronic ID device** to the USR."). The USR (*e.g.*, networked validation-information entity) then maps/accesses the user's real credit card number using the code. *See id.* at FIG. 7, 23:30-32 ("**The USR software 18 determines if the code is valid, or was valid at the time offered, and if valid accesses the user's credit card information** and transmits the appropriate credit card number to the credit card company (708)."). Thus, the specification supports the amendments made to 13[pre], 13[c], and 13[e]. *See also id.* at FIG. 23, 42:24-44:12, 45:7-9 (describing public ID field 304 being sent from first device to second device as part of authentication signal).[9] Ex. 2021 at ¶ 47.

Petitioner also contends that the claim limitation "wherein the first device communicates with the second device periodically to prevent intentional deletion of information stored at the first device" (limitation 17[a]) does not have written

[9] Support for the claimed "networked validation-information entity" being a credit card issuer that maps a multi-digit ID code to a credit and/or debit card number also exists. *See* Ex. 2006 at 23:34-24:2.

description support because the disclosure provided in the specification allegedly only "relates to automatically deleting data upon failed communication between the first and second device. This is different from *intentional deletion*." Op. at 25. Petitioner, however, takes an impermissibly narrow and restrictive view of the word "intentional" to mean that data deletion at the first device must be "at the direction of a user of the first device." This is simply not true and ignores the context provided by the specification with regard to data deletion at the first device. The specification provides that if periodic communication by the first device fails, automatic deletion of data is triggered. Ex. 2006 at 39:21-32, 40:8-24. Such data deletion is on purpose (*i.e.*, intentional) and occurs in response to the specific event of failed periodic communication by the first device. There is no requirement that a user command direct the deletion of data. Indeed, given the context described in the specification of why data may be deleted (*e.g.*, failing to enter the correct PIN or biometric data or failing to communicate after successful authentication), it makes no sense to put a potential unauthorized user of the device in charge of a deletion command. *See id.* at 40:14-24. Thus, a POSITA would understand the inventor was in possession of the invention claimed. Ex. 2021 at ¶ 48.

VII. CONCLUSION

Petitioner has failed to show that the substitute claims should not be granted.

DATED: May 9, 2019

Respectfully submitted,

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ James M. Glass*

James M. Glass (Reg. No. 46,729)
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
jimglass@quinnemanuel.com

Lead Attorney for Patent Owner – Universal Secure Registry LLC

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certify that PATENT OWNER'S REPLY IN SUPPORT OF ITS MOTION TO AMEND PURSUANT TO 37 C.F.R. § 42.121, and all exhibits and other documents filed together with the reply, were served on May 9, 2019 by e-mailing copies to:

Counsel
Monica Grewal (Reg. No. 40,056) monica.grewal@wilmerhale.com Ben Fernandez (Reg. No. 55,172) ben.fernandez@wilmerhale.com Kelvin Chan (Reg. No. 71,433) kelvin.chan@wilmerhale.com WILMER CUTLER PICKERING HALE AND DORR LLP 60 STATE STREET BOSTON, MA 02109 Mark Selwyn mark.selwyn@wilmerhale.com WILMER CUTLER PICKERING HALE AND DORR LLP 950 PAGE MILL ROAD PALO ALTO, CA 94304

DATED: May 9, 2019

Respectfully submitted,

By */s/ James M. Glass*

James M. Glass (Reg. No. 46,729)
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
jimglass@quinnemanuel.com

Lead Attorney for Patent Owner – Universal Secure Registry LLC