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 EXHIBIT 2021
DECLARATION OF MARKUS JAKOBSSON
IN SUPPORT OF PATENT OWNER'S REPLY TO CONDITIONAL MOTION TO AMEND

Apple 1137
Apple v. USR
IPR2018-00809

USR Exhibit 2021

1. I have been retained on behalf of Universal Secure Registry LLC ("Patent Owner") in connection with the above-captioned *inter partes* review (IPR). I have been retained to provide my opinions in support of USR's Reply to its Conditional Motion to Amend. I am being compensated for my time at the rate of $625 per hour. I have no interest in the outcome of this proceeding.

2. In preparing this declaration, I have reviewed and am familiar with the Petition for IPR2018-00809, U.S. Patent No. 9,530,137 (hereinafter "the '137 Patent"), and its file history, and all other materials cited and discussed in the Petition (including all prior art references cited therein) and all other materials cited and discussed in this Declaration.

3. The statements made herein are based on my own knowledge and opinion. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

I. QUALIFICATIONS

4. My qualifications can be found in my Curriculum Vitae, which includes my detailed employment background, professional experience, and list of technical publications and patents. Ex. 2002.

5. I am currently the Chief of Security and Data Analytics at Amber Solutions, Inc., a cybersecurity company that develops home and office automation technology. At Amber, my research studies and addresses abuse, including social engineering, malware and privacy intrusions. My work primarily involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches.

6. I received a Master of Science degree in Computer Engineering from the Lund Instituted of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a Researcher at the San Diego Supercomputer Center, where I did research on authentication and privacy.

7. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract exchange, digital commerce including crypto payments, and fraud detection and prevention. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems. During that time I predicted the rise of what later became known as phishing. I was also an Adjunct

Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols.

8. From 2004 to 2016, I held a faculty position at the Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for Applied Cybersecurity Research (CACR) from 2004 to 2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, resulting in over 50 publications and two books.

9. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, and Chief Scientist at Agari from 2016 to 2018. Agari is a cybersecurity company that develops and commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on

social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing countermeasures, including technological countermeasures, user interaction and education.

10. I have founded or co-founded several successful computer security companies. In 2005 I founded RavenWhite Security, a provider of authentication solutions, and I am currently its Chief Technical Officer. In 2007 I founded Extricatus, one of the first companies to address consumer security education. In 2009 I founded FatSkunk, a provider of mobile malware detection software; I served as Chief Technical Officer of FatSkunk from 2009 to 2013, when FatSkunk was acquired by Qualcomm and I became a Qualcomm employee. In 2013 I founded ZapFraud, a provider of anti-scam technology addressing Business Email Compromise, and I am currently its Chief Technical Officer. In 2014 I founded RightQuestion, a security consulting company.

11. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of the technical advisory board at Stealth Security (an anti-fraud

company). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

12. I have authored five books and over 100 peer-reviewed publications, and have been a named inventor on over 100 patents and patent applications.

13. My work has included research in the area of applied security, privacy, cryptographic protocols, authentication, malware, social engineering, usability and fraud.

II. LEGAL UNDERSTANDING

A. The Person of Ordinary Skill in the Art

14. I understand that a person of ordinary skill in the relevant art (also referred to herein as "POSITA") is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

15. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

16. A person of ordinary skill in the art relevant to the ’137 patent at the time of the invention would have 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.

17. I am well-qualified to determine the level of ordinary skill in the art and am personally familiar with the technology of the ’137 Patent. I was a person of at least ordinary skill in the art at the time of the priority date of the ’137 Patent in 2006. Regardless if I do not explicitly state that my statements below are based on this timeframe, all of my statements are to be understood as a POSITA would have understood something as of the priority date of the ’137 Patent.

B. Legal Principles

18. I am not a lawyer and will not provide any legal opinions.

19. Though I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

20. I have been informed and understand that if the Board should accept Petitioner’s arguments and cancel any of the original issued claims of the ’137 Patent, Patent Owner has made a conditional motion to amend to substitute the

canceled claim(s) with corresponding proposed amended claims 13-21, as set forth in Section III of Ex. 2014 (my declaration in support of Patent Owner's motion to amend).

21. I have been informed and understand that to permit the proposed substitute claims to be entered, Patent Owner must show, among other things, that the substitute claims are supported by the written description of the original disclosure of the patent, as well as any patent application to which the claim seeks the benefit of priority in this proceeding.

22. I have been informed by counsel and understand that to satisfy the written description requirement, the substitute claims must be disclosed in sufficient detail such that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention as of the filing date sought. I understand that the Patent Owner can show possession of the claimed invention by pointing to such descriptive means as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention.

23. I have been informed by counsel and understand that incorporation by reference is a method by which material from one or more documents may be integrated into a host document. I understand that material incorporated by reference is considered part of the written description of the patent that can be used to show possession of the claimed invention.

24. I have been informed by counsel and understand that to permit the proposed substitute claims to be entered, Patent Owner must show, among other things, that the substitute claims do not introduce new subject matter.

25. I understand that new matter is any addition to the claims without support in the original disclosure.

26. I have been informed by counsel and understand that to permit the proposed substitute claims to be entered, Patent Owner must show, among other things, the substitute claims do not broaden the scope of the original claims.

27. I understand that claims in dependent form are construed to include all the limitations of the claim incorporated by reference into the dependent claim and further limit the claim incorporated by reference.

28. It has been explained to me by counsel for the Patent Owner that in proceedings before the USPTO, the claims of an unexpired patent are to be given their broadest reasonable interpretation in view of the specification from the perspective of one having ordinary skill in the relevant art at the time of the invention. I have considered each of the claim terms using the broadest reasonable interpretation standard.

III. SUBSTITUTE CLAIMS ARE PATENT ELIGIBLE UNDER § 101

29. I understand that Petitioner argues that substitute claims 13-21 are unpatentable under § 101 because they purportedly claim patent-ineligible abstract

ideas. However, I have been informed that on September 19, 2018, United States Magistrate Judge Sherry R. Fallon for the District Court of Delaware rejected virtually identical arguments made by Petitioner when Judge Fallon issued a Report and Recommendation (R&R) 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, I understand that Judge Fallon stated:

> [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 noted by Judge Fallon.

30. I understand that the same conclusion was also reached by this Board

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 cites to the same cases making substantially similar arguments for patent ineligibility. The Board dismissed these arguments then, and in my opinion it should dismiss these arguments here now because many of the reasons why the Board found the claims of the '813 Patent are not abstract equally apply to the present substitute claims.

31. For instance, Petitioner has oversimplified the claimed inventions and ignores many key claim limitations. 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. 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.

32. I understand Petitioner argues 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), but Petitioner fails to account for the specific 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." The 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 "second authentication information" of the user 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. None of these features are captured by Petitioner's proffered overbroad abstract idea.

33. 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 I understand 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, 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. 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 for *remote* authentication of 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.

34. Even assuming the substitute claims are directed to the Petitioner's abstract idea, it is my opinion that the ordered combination of elements in these claims transform the nature of the claim into a patent-eligible application. 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. 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." For these reasons, it is my opinion the substitute claims are patent eligible.

IV. SUBSTITUTE CLAIMS ARE NOVEL AND NONOBVIOUS

35. Not only do the substitute claims respond to a ground of unpatentability, they are clearly distinguishable over the prior art of record. 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. As described in more detail below, these amendments patentably distinguish the substitute claims over the Jakobsson, Maritzen, and Schutzer references.

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

36. I understand that Petitioner failed 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 referred solely to the arguments made its Petition with respect to disclaimed claims 8 and 11. Opp. at 17-18. Petitioner has failed to establish this limitation is obvious in view of Jakobsson, Maritzen, and Schutzer.

37. 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**"[1] performing the mapping between multi-digit ID code to a [credit and/or debit card/financial account] number. Petitioner had therefore failed to meet its burden to establish any of the substitute claims are obvious.

B. It Would Not Have Been Obvious to Use "Three Separable Fields"

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

38. 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 (Opp. 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 (T) all in the same transmission. This is a fatal flaw in Petitioner's argument.

39. 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.[2]

[2] 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." Opp. at 18.

40. Moreover, as I have explained in my deposition, the one-way function is a ***critical aspect*** of the invention described in the Jakobsson reference. Ex. 2017 at 127:6-20. While certain embodiments of Jakobsson discuss prepending and appending certain inputs, a one-way function is always used (optionally in conjunction with other functions). A person of ordinary skill in the art would understand that all the examples given involve a one-way function because otherwise the system would not be secure. *Id.* 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 own 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).

41. In my opinion, a POSITA would have understood the disclosure of Jakobsson to require the use of a one-way function at some point during the authentication code generation process. As such, the resultant unitary

---

Regardless, there is no disclosure in Jakobsson that the unitary authentication code includes "three separable fields" after the code is generated and transmitted.

authentication code does not have three separable fields that includes all three pieces of claimed information. In other words, a POSITA would not recognize Jakobsson's system to transmit a code with 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.[3]

C. Substitute Dependent Claim 18 Is Not Obvious

42. Substitute claim 18 recites "the first authentication information further including a digital signature generated using a private key associated with the first device." I understand 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." Opp. at 21-23. Regardless of

[3] 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 and used to generate the authentication codes. 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, this is yet another reason why the authentication code described in Jakobsson does not have "three separable fields" or include the claimed three distinct types of information.

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 (for example, through the claimed "networked validation-information entity"), how the digital signature is generated, and whose private key (if any) is used.

43. In particular, no express or inherent[4] disclosure is made that the digital signature of Schutzer was generated using a private key associated with the first device. Accordingly, it is my opinion that Petitioner has failed to meet its burden to show dependent claim 18 is obvious.

D. Petitioner Fails to Address Substitute Claims 17 and 20

[4] 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.

44. Substitute claims 17 and 20 has both been substantively amended from their original forms, yet I understand Petitioner has failed to address the patentability of these substitute claims in view of the prior art. In my opinion, both of these substitute claims recite new features not found in any of the prior art of record (particularly not in combination with the limitations found in substitute independent claim 13). These substitute claims are therefore non-obvious.

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

45. I understand 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*. In my opinion, Petitioner's error proves fatal.

46. While the claimed networked validation-information entity may be a

financial institution, such as a credit card company (CCC),[5] 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. 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 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.[6] The specification also describes a "second device" that—like USR and networked credit card validation-information entity—performs authentication of a user (*e.g.*, first device). *See, e.g.*,

---

[5] While a credit card company (CCC) may be a non-limiting, non-exclusive example of a "networked validation-information entity," there are many others examples. For example, a portion of the secure registry might constitute the claimed networked validation-information entity.

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

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.

47. 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. First, the specification discloses that a code, which has multiple digits and serves to identify the user, is transmitted from user's electronic ID device to the merchant, which in turn is ultimately sent to the USR (*e.g.*, networked validation-information entity). *Id.* at 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).[7]

48. I understand 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 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. In my opinion, Petitioner, takes an impermissibly narrow and twisted 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.

[7] 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.

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 or otherwise direct for the deletion of the data. Indeed, given the context described in the specification of why data may be deleted (*e.g.*, "If the user of the device does not enter the correct PIN number or does not match the biometric data," or device fails to communicate after successful authentication), it does not make sense to have a potential unauthorized user of the device be in charge of safe-guarding the device's data by deleting it. *See id.* at 40:14-24. Thus, a POSITA would understand that the inventor was in possession of the invention claimed.

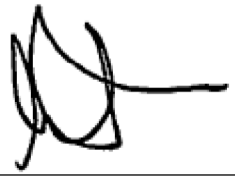
VI. CONCLUSION

49. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

50. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are

believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed: May 9, 2019



Markus Jakobsson, Ph.D.