

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Francisco Martinez de Velasco Cortina, et al.
U.S. Patent No.: 8,933,807 Attorney Docket No.: 50095-0308IP1
Issue Date: January 13, 2015
Appl. Serial No.: 14/028,469
Filing Date: September 16, 2013
Title: SYSTEM AND METHOD FOR PROVIDING SECURE
TRANSACTIONAL SOLUTIONS

DECLARATION OF DR. SETH JAMES NIELSON

I declare that all statements made herein on my own knowledge are true and that all statements made on 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 under Section 1001 of Title 18 of the United States Code.

Date: 2026-09-18

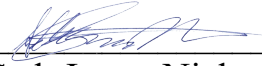
By: 
Seth James Nielson, Ph.D.

Table of Contents

I.	INTRODUCTION	4
II.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	4
III.	OVERVIEW OF CONCLUSIONS FORMED	15
IV.	LEVEL OF ORDINARY SKILL IN THE ART	16
V.	LEGAL STANDARDS	17
	A. Terminology.....	17
	B. Legal Standards.....	18
	C. Anticipation.....	18
	D. Obviousness	19
VI.	THE '807 PATENT	23
	A. Overview of the '807 Patent	23
	B. Prosecution History of the '807 Patent.....	26
	C. Claim Construction	28
VII.	OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES ..	28
	A. Overview of Maes.....	28
	B. The Prior Art References Are Analogous Art	35
	C. Overview of Dorf.....	35
	D. The Maes-Dorf Combination (MDC).....	36
	E. Overview of Shults	38
	F. The Maes-Shults Combination (MSC).....	39
	G. Overview of Walker.....	42
	H. The Walker-Maes Combination (WMC).....	44
	I. The Walker-Maes-Dorf Combination (WMDC).....	50
	J. The Walker-Maes-Shults Combination (WMSC)	51
VIII.	MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '807 CLAIMS UNPATENTABLE	51
	A. Ground 1A: Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23	51
	B. Ground 1B: Maes-Dorf Renders Obvious Claims 4, 12, and 21.....	82
	C. Ground 1C: Maes-Shults Renders Obvious Claims 7, 14, and 22	83
	D. Ground 2A: Walker-Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23[1.pre] A mobile device, comprising:.....	84
	E. Ground 2B: Walker-Maes-Dorf Renders Obvious Claims 4, 12, and 21...	105
	F. Ground 2C: Walker-Maes-Shults Renders Obvious Claims 7, 14, and 22	105

IX. CONCLUSION.....	106
---------------------	-----

I. INTRODUCTION

1. I have been retained by Fish and Richardson P.C. to offer technical opinions related to U.S. Patent No. 8,933,807 (“the ’807 patent”) (EX1001) with respect to an inter partes review (“IPR”) petition of the ’807 patent. I understand that the Petitioners in this IPR, Apple Inc. and Samsung Electronics Co., Ltd., are requesting that the Patent Trial and Appeal Board (“PTAB” or “Board”) institute an IPR proceeding on the ’807 patent.

2. I have been asked to provide my independent analysis of the ’807 patent based on the prior art publications cited in this declaration.

3. I am not and never have been an employee of Petitioners. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the ’807 patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’807 patent.

II. QUALIFICATIONS AND BACKGROUND INFORMATION

4. I am qualified by education and experience to testify as an expert in the fields of cybersecurity, computer networks, and software engineering. Attached as Appendix A to this declaration is a copy of my *curriculum vitae* detailing my education and over 25 years of experience.

5. I am the Founder and CEO of Crimson Vista, a computer research and engineering company. Furthermore, I hold appointments at the University of Texas at Austin as an Adjunct Associate Professor in the department of Computer Science. I hold a Ph.D. in Computer Science from Rice University, awarded in 2009. I also received B.S. and M.S. degrees in Computer Science from Brigham Young University in 2000 and 2004 respectively.

6. In addition to my academic degrees, I hold Certified Information Systems Security Professional (CISSP) and GIAC Certified Forensic Examiner (GCFE) certifications.

7. I have authored three books in my field on topics of cryptography, cybersecurity, and compliance. I expect to publish another book in 2027 related to the psychology of fraud in digital scams. I have also published peer-reviewed research on hacking devices including cyber-physical devices such as chemical production systems. I am a named inventor on four patents, a named researcher on two different government grants. My master's thesis, entitled "OO++ Design Patterns, GOF Revisited," focused on software engineering philosophy, theory, and practice. My Ph.D. thesis, entitled "Designing Incentives for Peer-to-Peer Systems," presented my research results related to economic mechanism design, incentives, and cybersecurity in decentralized systems.

8. In my work in industry, I have led and executed over 100 forensic and incident response engagements, evaluated the cybersecurity capabilities of dozens of academic and commercial systems, and reviewed millions of lines of source code in a dozen different software languages. I have personally led incident response teams to assist organizations currently experiencing an intrusion, analyzed what security failures allowed the breach, and recommended remediations. I have also developed AI guidance with respect to technical defensive measures, regulatory guidance, and other best practices related to security, transparency, and reliability.

9. I have engineered a wide range of software systems for many employers and clients including Microsoft, Google, Metrowerks, and various other software companies. In these endeavors, I was a key engineer on multiple commercial software projects and software infrastructure for commercial services. I worked on all parts of the engineering lifecycle for testing systems, software development kits, engineering applications, networking components, security systems, distributed file systems, cryptography components, web components, package management, and virtual-machine-based infrastructure. I also developed expertise with software development infrastructure such as testing systems, source code repositories, code reviews, network security components, remote access systems, virtual private networks, routing, firewalls, webmail components, web

servers, embedded devices, embedded deployment, and cross-architecture toolchains. Throughout my engineering years I wrote hundreds of thousands of lines of computer code in C++, C, Python, Perl, Java, Go, Ruby, and other languages.

10. My professional work also includes a large body of design, implementation, and evaluation of networked communications systems. I was a key engineer in the design, development, and evaluation of networking components between client and server applications, Internet-delivered software update packages, and a secure communications system for improved Internet security even if certificate authorities are compromised. I have also created a series of network simulation tools for academic and pedagogical environments.

11. From 2005-2011, I worked as a cybersecurity analyst for Independent Security Evaluators (ISE). During this time, I built secure software for clients, investigated security incidents, evaluated security designs, and supported forensic investigations. In one such project, I was tasked with evaluating the security of a software project for a Fortune-50 client using a massively distributed code coverage tool, which was partially designed and built by me, to ensure that code tests were not leaving any hidden vulnerabilities. I also evaluated cryptographic protocols for vulnerabilities and used formal methods to find and identify deficiencies.

12. From 2011-2015, I was a Research Scientist, and eventually a Principal, at Harbor Labs. My work at Harbor Labs delved deep into forensic source code analysis and I reviewed many dozens of software systems to determine behavior and provenance. My work also included other security evaluations such as an evaluation of an anti-privacy vendor to assess the security of their data collection and storage. I also led a team of investigators to find and identify security flaws in medical infusion pumps that had been enhanced with networking capabilities.

13. In 2016, I founded Crimson Vista, Inc. to provide cybersecurity research and engineering services under my design and direction. As the CEO of Crimson Vista, I have defined all of the cybersecurity strategy, partnerships, services, and operations. I have designed all of the employee training as well as personally led almost all the major engagements. These engagements generally fall into categories such as direct cybersecurity services, cybersecurity enhancement for partners, AI engineering, compliance support, and forensic services.

14. The direct cybersecurity services include evaluation of security and privacy, risk assessment, threat analysis, and audit and compliance. They also include offering fractional Chief Information Security Officer (CISO) services, penetration testing, evaluation, and remediation. We have built cybersecurity

programs from scratch, prepared companies for cybersecurity audits, and helped design technical controls to enforce cybersecurity policy. We also have supported companies in the event of cyber breaches. I am the primary architect and the lead engineer for providing these services. We also teach, train, and provide general cybersecurity strategy services including one project for United States Department of Justice in an antitrust investigation.

15. As part of cybersecurity audit and compliance, I have led the complete evaluation of a company's cybersecurity from top to bottom. This includes analyses related to HIPAA, SOC-2, and CMMC Level 2. These audits require my teams, under my direction, to collect all documentation and other artifacts related to security controls such as access controls, physical controls, network security, data security, and so forth, evaluate these artifacts, and require remediation where necessary.

16. We also provide partner service enhancements. In these engagements, we enable companies that provide IT and technical services to include expert-level cybersecurity offerings under our direction. We provide the necessary training, guidance, and support these partners to better serve their clients with cybersecurity capabilities. I am the primary architect for these partnerships including the design of the training and the ultimate technical expert for any partner questions relating to cybersecurity.

17. Finally, I have personally led teams on over 100 forensic projects of one form or another over the ten years of our operations. My clients have included companies of all sizes including Fortune 50 entities, Tier-1 banks, security companies, medical companies, heavy industry, insurance companies, software companies, and start-ups. The technologies related to these engagements include secure email, cloud-based multimedia delivery, document signing, anti-virus and anti-intrusion, high-performance routing, networking protocol stacks in mobile devices, PBX telecommunications software, VoIP, high-frequency trading, e-commerce, antivirus, cloud systems, digital radios, mobile devices, video games, industrial controls, deep learning systems, medical software, cryptocurrency, and peer-to-peer communications. Many forensic projects have been directed toward issues of trade secret misappropriation and stolen source code.

18. I have also been asked to lead forensic investigations into causes of cybersecurity incidents. This included a forensic reconstruction of the intrusion, analysis of the impact, remediation, and attribution. I have identified intrusion vectors that include email, software vulnerability, poorly controlled credentials, insider attacks, and so forth. These investigations made use of various professional tools and data sources from logging systems, SIEMs, and IDS/IPS components. The forensic techniques used herein vary from cryptographic analyses to custom

artifact identification. In one instance, I identified a novel technique related to electronic document (email) modification.

19. I have also led my teams in forensic data collection from digital sources using a wide range of industry-standard tools including Magnet Axiom, Cellebrite Collector, Autopsy, and others. My teams have extracted data from laptops, desktops, mobile devices, and cloud accounts and then processed that data for specific artifacts and items of interest. When necessary, I have also directed the development of custom tooling in order to provide the complete forensic analysis. Our analysis has also been used to reconstruct website content timelines for a criminal case and invalidate assertions of provenance.

20. In addition to my work with clients, I provide training and education to professionals. These trainings, which I presented at various venues, include topics related to data security, data privacy, protecting intellectual property, Blockchain basics, and improving a company's security posture. I am also a member of the program committee for the International Cryptographic Module Conference (ICMC).

21. I also contribute to industry research. I was the primary investigator on a DOD-funded research project for protecting systems from Ransomware. I also am a named contributor on another research grant to Curuvar, LLC. In this partnership, I assisted in developing insider-proof systems and secure enclaves for

government networks. I recently led a team in an investigation into prompt engineering and LLM exploitation.

22. As part of contributing to the technical community, I co-founded and co-led the Crypto Done Right project. This project was originally hosted by Johns Hopkins University and funded by a grant from Cisco. However, I transitioned the project into a completely independent non-profit entity as one of the founding directors. Crypto Done Right was designed to bridge the gap between cryptography SME's and the IT professionals that use it. This project completed its operations in 2025.

23. I also maintain ties to Academia. During the 2014-2019 time period I taught the Network Security and Advanced Network Security courses at the Johns Hopkins University. I developed my own curriculum focused on mobile code, cryptography, autonomous agents, intrusion analysis, and education psychology. I published a paper related to my curriculum in the Journal of Computer Science Education entitled, "PLAYGROUND: Preparing Students for the Cyber Battleground."

24. From 2016-2019, I was the Director of Advanced Research Projects at the Johns Hopkins University Information Security Institute (JHUI SI). During this time, I published "Potential Forensic Analysis of IoT Data: An Overview of the State-of-the-Art and Future Possibilities" in the 2017 IEEE International

Conference on Internet of Things (iThings). I also published “Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices” in 2018 IEEE International Symposium on Technologies for Homeland Security (HST).

25. In addition to published research, I mentored capstone projects related to IDS/IPS, intrusion detection, cryptography, drone security, iOS security, BitCoin, SSL vulnerabilities, and Twitter “botnets.” Many of these projects involved industry collaboration. For example, we coordinated with the company OnBoard Security to develop better security for anti-collision protocols for air traffic. I also gave a talk on “Detecting Malicious Sandboxes” at the Workshop on Defensive Deception and Trust in Autonomy, in association with the 2018 Naval Applications of Machine Learning Workshop.

26. From 2020 to the present, I have held the position of adjunct professor at the University of Texas at Austin. I have taught the undergraduate Network Security and Privacy class in the Computer Science department. I have also taught the Introduction to Cybersecurity Technology class in the Law School. In addition to regularly scheduled classes, I have also mentored independent study courses for Computer Science students on topics of computer security and artificial intelligence.

27. Finally, I have testified in numerous expert engagements and have been qualified as an expert in court. Many of these engagements are related to my forensic analysis, but I have also testified on matters related to patent infringement and validity, copyright, DMCA, and cybersecurity norms and industry standards.

28. In writing this Declaration, I have considered the following: my own knowledge and experience, including my work experience in the fields of cryptography and related security techniques; my experience in teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed the following publications and materials, in addition to other materials I cite in my declaration:

29. I have reviewed the '807 patent (EX1001), and relevant excerpts of the prosecution history (EX1002) of the '807 patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references and documents:

- EX1001 U.S. Patent No. 8,933,807 to de Velasco Cortina, et al. (the “'807 Patent”)
- EX1002 The Prosecution History of the '807 Patent (the “Prosecution History”)
- EX1004 U.S. Patent No. 6,016,476 to Maes et al. (“Maes”)
- EX1007 U.S. Patent No. 6,163,771 to Walker et al. (“Walker”)
- EX1008 U.S. Patent App. Pub. No. 2002/0011519 to Shults (“Shults”)
- EX1009 U.S. Patent No. 6,000,608 to Dorf (“Dorf”)

- EX1024 U.S. Patent No. 6,850,147 to Prokoski (“Prokoski”)
- EX1025 U.S. Patent No. 6,175,922 to Wang (“Wang”)

30. Counsel (Fish & Richardson) has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '807 patent at the time of the earliest possible priority date of the '807 patent, and I have done so during my review of these materials. I have been informed by Counsel to use 7/9/2002, the filing date of earliest provisional application to which priority is claimed.

31. I have no financial interest in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

32. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '807 Patent. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of the earliest possible priority date. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '807 Patent and the prior art discussed below.

III. OVERVIEW OF CONCLUSIONS FORMED

33. This declaration explains the conclusions that I have formed based on my analysis of all of the considered materials and my personal experience. To summarize those conclusions, based upon my knowledge and experience and my review of the prior art references listed above, I believe that:

Ground 1A: Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23

Ground 1B: Maes-Dorf Renders Obvious Claims 4, 12, and 21

Ground 1C: Maes-Shults Renders Obvious Claims 7, 14, and 22

Ground 2A: Walker-Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23

Ground 2B: Walker-Maes-Dorf Renders Obvious Claims 4, 12, and 21

Ground 2C: Walker-Maes-Shults Renders Obvious Claims 7, 14, and 22

34. In support of these conclusions, I provide an overview of the references in Section VII and more detailed comments regarding the obviousness of claims 1-23 (“the Challenged Claims”) of the ’807 patent in Section VIII.

IV. LEVEL OF ORDINARY SKILL IN THE ART

35. A person of ordinary skill in the art (“POSITA”) relating to the ’807 Patent’s subject matter as of July 9, 2002 would have had (1) at least a bachelor’s degree in computer science, computer engineering, or a related field, and (2) at least two years of industry experience including researching or developing software related to secure communication systems/networks. Additional education could substitute for professional experience, and professional experience for education.

36. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, participated in organizations, and worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of a POSITA. For example, from my industry experience, I am familiar with what a POSITA would have known and found predictable in the art. From teaching and supervising my post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

V. LEGAL STANDARDS

A. Terminology

37. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless explicitly noted otherwise and unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). The '807 patent was filed September 16, 2013, and claims

priority to an earlier-filed application, the earliest of which was filed July 9, 2002, which I refer to as the “Critical Date” in this proceeding. It is my understanding that the ’807 patent may not be entitled to priority to this Critical Date. Because I am not a lawyer, I am nonetheless using the Critical Date of the ’807 patent as the point in time for claim interpretation purposes.

B. Legal Standards

38. I have been informed by Counsel and understand that documents and materials that qualify as prior art can render a patent claim unpatentable as being anticipated or obvious.

39. I am informed by Counsel and understand that all prior art references are to be looked at from the viewpoint of a person of ordinary skill in the art at the time of the invention, and that this viewpoint prevents one from using his or her own insight or hindsight in deciding whether a claim is anticipated or rendered obvious.

C. Anticipation

40. I understand that patents or printed publications that qualify as prior art can be used to invalidate a patent claim as anticipated or as obvious.

41. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a

comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

42. I understand that a prior art reference “anticipates” an asserted claim, and thus renders the claim invalid, if all limitations of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present).

D. Obviousness

43. I understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA. I have been informed by Counsel and understand that a claim is unpatentable for obviousness and that obviousness may be based upon a combination of references. I am informed by Counsel and understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. However, I am informed by Counsel and understand that a patent claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. I am informed by Counsel and understand that when a patented invention is a combination of known elements, a court determines whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue by considering the teachings

of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art.

44. I am informed by Counsel and understand that a patent claim composed of several limitations is not proved obvious merely by demonstrating that each of its limitations was independently known in the prior art. I am informed by Counsel and understand that identifying a reason those elements would be combined can be important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. I am informed by Counsel and understand that it is improper to use hindsight in an obviousness analysis, and that a patent's claims should not be used as a "roadmap."

45. I am informed by Counsel and understand that an obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others. I have been informed by Counsel and understand that an obviousness evaluation can

be based on a single reference or a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the nexus linking two or more prior art references is sometimes simple common sense. I have been informed by Counsel and understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

46. I have been informed by Counsel and understand that if a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. I have been informed by Counsel and understand that practical and common sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I have been informed by Counsel and understand that a person of ordinary skill looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. I have been informed by Counsel and understand that obviousness analysis therefore takes into account the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

47. I have been informed by Counsel and understand that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill at the time of invention, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

48. I have been informed by Counsel and understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art. I have been informed by Counsel and understand that there must be a relationship between any such secondary considerations and the invention, and that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

49. In sum, my understanding is that prior art teachings are properly combined where one of ordinary skill having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem

known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

50. I have been informed by Counsel and understand that, according to 35 U.S.C. §316(e), in an *inter partes* review, “the petitioner shall have the burden of proving a proposition of unpatentability,” including a proposition of obviousness, “by a preponderance of the evidence.”

VI. THE '807 PATENT

A. Overview of the '807 Patent

51. The '807 Patent “generally relates to a system and method for providing secure identification solutions, and specifically to a system and method for verifying and tracking identification information.” EX1001, 1:8-10 (describing the “Field of the Invention”).

52. As shown in the '807 Patent's Fig. 1 (reproduced below), a “General RF Identification System and Method of Use” may include, for example, “an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120.” EX1001, 2:1-4.

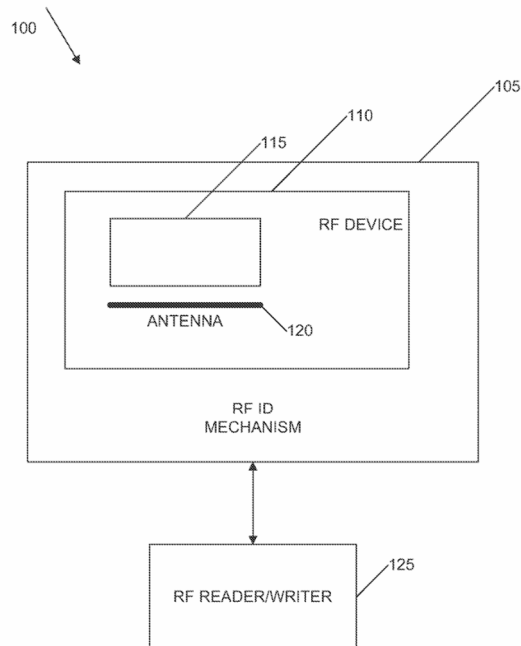


FIG. 1

EX1001, Fig. 1.

53. In some embodiments the “RF identification mechanism is a card”; however, as the ‘807 Patent acknowledges, “those experienced in the art will recognize that multiple other embodiments of the identification mechanism are possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA).” EX1001, 2:44-50.

54. An “RF device ... has a unique identifier ... and the information contained on it is protected by sundry cryptographic methods.” EX1001, 8:23-26. “The capacity of the device will allow a great deal of information about the holder to be stored on the device (*e.g.*, fingerprint minutiae or other biometric template,

the holder's biographical information, statistical information),” and the ‘807 Patent acknowledges that “[t]hose experienced in the art will see that an RF device allows data to be written to and read from the device via an antenna without the holder having to present the document for verification through traditional methods such as visual inspection, or other method of machine reading.” EX1001, 8:27-35.

55. In an embodiment that is “discussed in the context of an RF cellular telephone,” the “RF communication device creates a communication through a network to a point of sale (“POS”),” for example, “by a wireless RF device that stores a person’s identification information, and can thus become a person’s identification ‘document.’” EX1001, 12:62-67.

56. “As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone.” EX1001, 13:4-7. “The user is then asked to enter authentication information (*e.g.*, a fingerprint),” and [a]n exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information.” EX1001, 13:7-13.

57. As the ‘807 Patent acknowledges, “using a fingerprint for identification, ... is a widely recognized identification tool,” and “those skilled in the art will recognize that any type of identification information (*e.g.*, Personal

Identification Number (PIN)) or any other biometric identifier (*e.g.*, a voice print, iris recognition, facial recognition) could be used.” EX1001, 12:56-62.

58. The “RF cellular telephone can [thus] be used as a substitute for credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities” EX1001, 13:31-35.

B. Prosecution History of the ’807 Patent

59. During prosecution of the application for the ’807 Patent, the examiner issued a series of office actions rejecting the presented claims as obvious over multiple references. In one of these office actions (mailed August 8, 2014), the examiner rejected the claims under §103 over U.S. Patent No. 6,850,147 to Prokoski (“Prokoski”, EX1024) in view of U.S. Patent No. 6,175,922 to Wang (“Wang”, EX1025). *See* EX1002, 50-65. The applicant responded by amending limitations into the independent claims requiring that:

60. (i) “the biometric authentication information has been previously associated with the transaction information” such that the authentication module is configured to “authenticate that the biometric information read by the biometric reading device is associated with the transaction information,” and

61. (ii) the transaction module is configured to provide the transaction information “via [] short range RF circuitry.” EX1002, 35-39.

62. The applicant explained the amendments as follows:

The device can compare the biometric information input by the user with the stored biometric authentication information, which has already been associated with the transaction information. As such, verification of the user's identity allows the device to also authenticate the user's authorization with respect to the stored transaction information.

63. EX1002, 41.

64. In its response, the applicant represented to the examiner that the applied prior art failed to teach the features of the amended claims because the prior art's authentication operations were either not performed on the mobile device or the prior art "biometric information only authenticates the user with respect to the PEAD ... in order to verify that the user is authorized to use the device" rather than "used to indicate approval of the transaction." *Id.*, 42-43.

65. The examiner subsequently allowed the application. EX1002, 8-14. The examiner's reasons for allowance asserted that the prior art of record failed to teach multiple limitations of the allowed claims including "authenticating that the biometric information input by a user corresponds to the biometric authentication information associated with the transaction information." *Id.*, 13.

66. The examiner's decision to allow the application at this juncture, however, was in error. Indeed, the examiner failed to identify other highly relevant

prior art later cited during prosecution of applications in the '807 Patent family, including Maes (EX1004) and Walker (EX1007). Grounds 1A-2C of this Declaration show that the '807 Patent never should have been issued.

C. Claim Construction

67. In furnishing my opinions in this declaration, I have used the plain and ordinary meaning of the claim terms.

68. I have been informed by Counsel that Petitioner Apple has proposed in parallel district court litigation a construction for the claim term “transaction information” as “information used to process a transaction that includes at least credit card information or rewards card information.” I have applied this construction of “transaction information” throughout my analysis in this declaration.

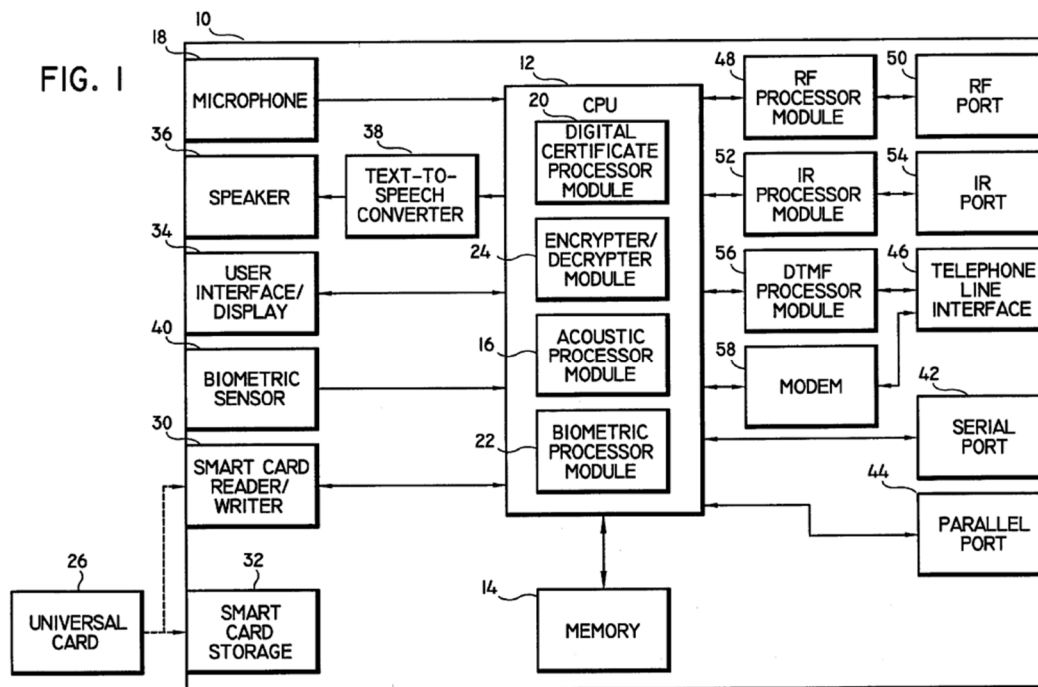
69. Should the Patent Owner or the Board provide further remarks on construction, I may supplement my analysis in response to their remarks.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Maes

70. Maes describes a “portable information and transaction processing device,” such as a “portable client PDA” that “provide[s] direct communication capability with peripheral devices (such as POS [point-of-sale] ... terminals) ... through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract, 4:16-28, 4:65-6:27, Fig. 1.

71. As shown in Maes's exemplary Fig. 1 (reproduced below), Maes's PDA includes "a memory for storing financial and personal information" that may be used when performing "biometric verification" of the user as part of secure transaction processing involving the user's associated "card information." EX1004, Abstract; *see also id.*, 4:65-6:27.



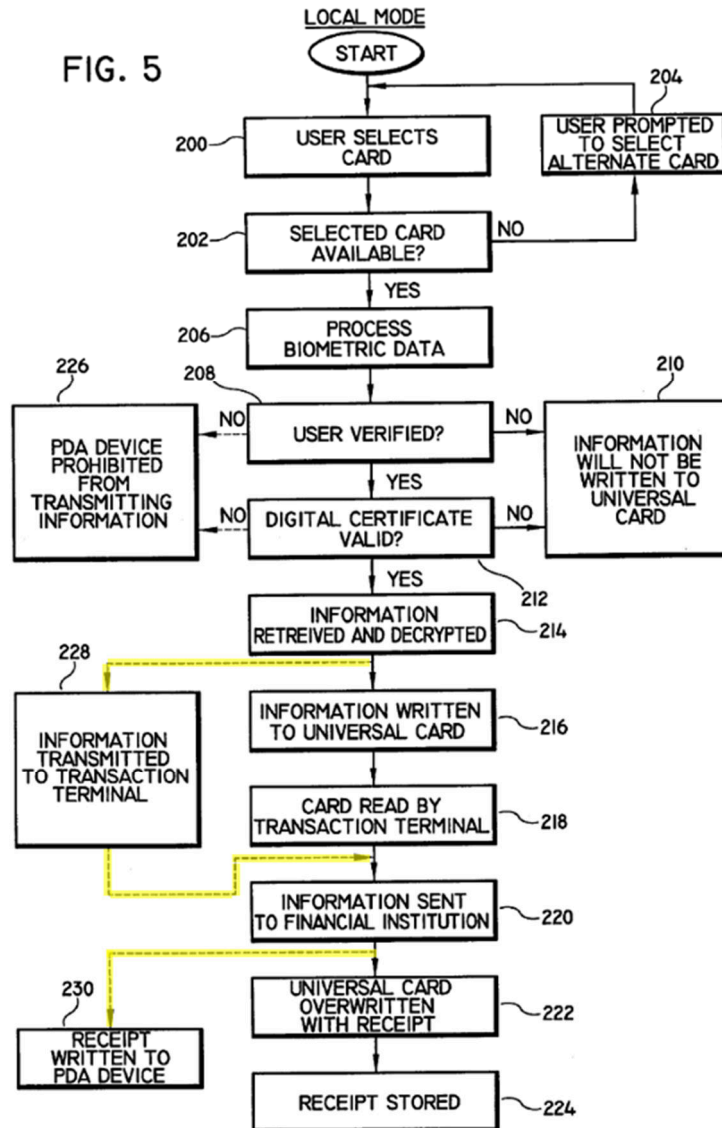
EX1004, Fig. 1.

72. In some embodiments, "[t]he PDA includes a Universal Card, which is [a] common generic smartcard with a unique imprint provided by a service provider, on which selected financial or personal information stored in the PDA can be downloaded to perform certain consumer transactions." EX1004, Abstract; *see also id.*, 4:29-30, 5:24-35 (describing a "smartcard reader/writer 26 ... for

reading and writing information to and from various cards, *e.g.*, magnetic cards, IC cards, and/or EAROM cards”¹). The Universal Card “contains a unique ... number 27 ... which is analogous to the account number provided on a credit card,” and which can therefore be used in connection with credit card transactions. *See* EX1004, 6:28-55, Figs. 2, 3.

73. Maes emphasizes, however, “that the invention may interact with electronic fund transfer systems or transaction terminals having wireless or direct communication capabilities without even having to use the Universal Card 26.” EX1004, 12:5-8. “Specifically, as demonstrated by the dotted lines in Fig. 5” (reproduced below), “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link” EX1004, 12:8-13.

¹As shown in Fig. 1, the smartcard reader/writer should have reference number 30; however the text lists reference number 26, which is quoted.



EX1004, Fig. 5 (highlighting added).

74. In more detail, Maes operates in two modes: (1) “a client/server mode” that “is periodically performed to download a temporary digital certificate ... from a central server of [a] service provider”; and (2) a “local mode” for transaction processing that “is performed by providing the PDA with biometric data and selecting one of the pre-enrolled credit cards that are stored in the PDA.”

EX1004, Abstract; *see also id.*, 7:36-10:29 (describing client/server mode operations including obtaining a digital certificate), 10:29-13:5 (describing local mode operations including transaction processing involving user biometric verification). “Upon biometric verification ... selected card information” is “used to initiate a consumer transaction.” EX1004, Abstract. Fig. 5 depicts operations in the local mode of operation. EX1004, Fig. 5 (“LOCAL MODE”).

75. However, in the absence of an “unexpired digital certificate” no transaction will take place. EX1004, Abstract. For example, “[t]he merchant can verify that local verification of the user has been properly obtained by ... transmitting the selected card information to the financial institution” in addition to an “authorization number” that “is generated upon user verification”; “[s]ince the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 in the client/server mode, the central server 60 [may then] inform the merchant that the user was properly verified” EX1004, 12:55-13:5; *see also* 6:56-7:35, Fig. 3.

76. Maes’s Fig. 3 (reproduced below) illustrates an exemplary “interaction of the PDA device 10 in connection with processing a transaction” EX1004, 6:56-59.

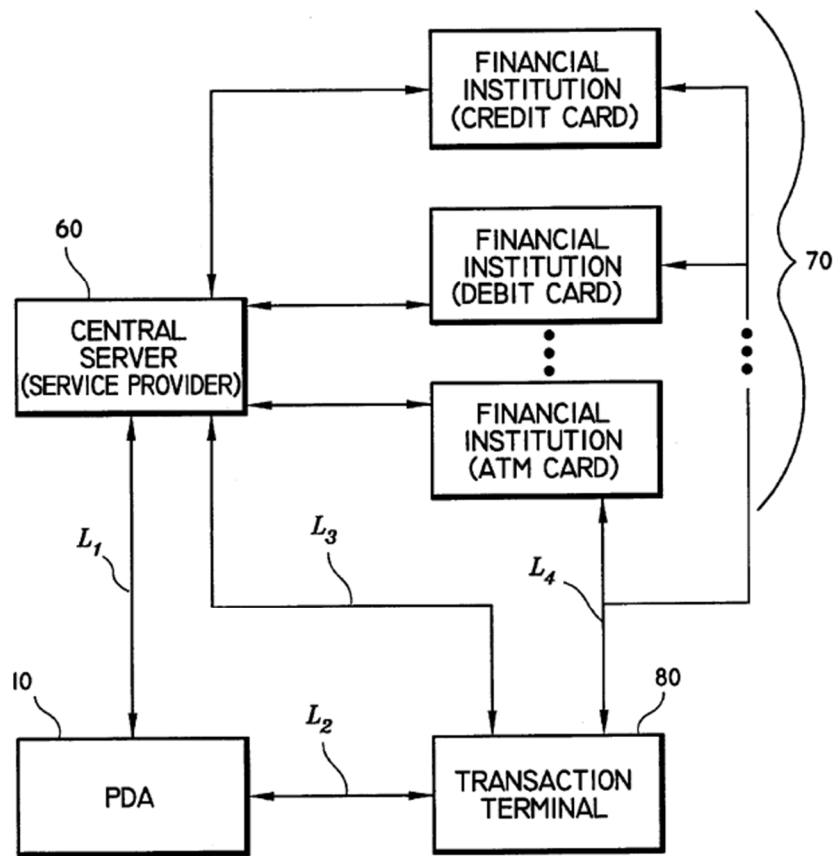


FIG. 3

EX1004, Fig. 3.

77. To “obtain the digital certificate” in the client-server mode “the user must establish a communication link (Link L1, Fig. 3) with the central server 60 of the service provider,” for example, “through a digital communication channel such as internet, intranet or local area network.” EX1004, 7:57-66, Fig. 4. The user is then prompted “to enter certain verification data” including for example voice data for comparison with “voice prints that were stored in the central server 60 during the enrollment process,” and/or a PIN for comparison with “the PIN that was

issued during the enrollment process.” *See* EX1004, 8:15-63. If the user is verified, the “central server 60 will then prompt the user to provide certain transaction limitations such as the specific financial card information to be used, ... and/or the period of time in which the temporary digital certificate will remain valid”

EX1004, 9:66-10:4. “This information is received and processed by the central server 60 and a digital certificate is then created and encoded with the user requested limitations”; an encrypted version of the digital certificate is then “downloaded into the digital certificate processing module 20 of the [PDA’s] CPU 12 via the established communication link L1” EX1004, 10:5-11, Figs. 1, 4.

78. “The local mode of operation is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14 (step 200).” EX1004, 10:31-34. “If the requested card information is found in memory, biometric verification must be performed” EX1004, 10:50-52. “If the user is verified, the digital certificate (previously obtained in the client/server mode) is retrieved from memory 14 and loaded into the digital certificate processor module 20,” which “determine[s] whether the digital certificate is still valid” (*i.e.*, unexpired); if so, “the requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24,” which decrypts the selected card information “using an encryption key unique to the PDA device 10 (step 214).” EX1004, 11:15-32. “The decrypted card information is then sent to the smartcard

reader/writer 30 where it is then written to the Universal Card 26,” which can then be “removed from the smartcard reader/writer 30 and swept through the magnetic reading device of the transaction terminal 80 (Fig. 3) (step 218).” EX1004, 11:32-37.

79. Alternatively, “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, Fig. 3)” EX1004, 12:9-14, Figs. 1, 3, 5.

B. The Prior Art References Are Analogous Art

80. Grounds 1A-2C below demonstrate that the Challenged Claims of the ’807 Patent would have been obvious to a POSITA before the Critical Date based on Maes, and on prior-art combinations involving Maes, Walker, Shults, and Dorf. Each of these references is analogous art in the same field as the ’807 Patent (*e.g.*, secure transactions and communications) and/or reasonably pertinent to problem(s) purportedly addressed by the ’807 Patent (*e.g.*, verifying or authenticating users in secure transactions). *See* EX1001, Abst., Figs. 12-17; EX1004, 1:10-17; EX1008, [0003], [0009], [0030], Abst.; EX1007, 1:6-10, 3:59-4:4, Abst.; EX1009, Abst., 1:24-35 (“secure environment”), 7:5-9.

C. Overview of Dorf

81. Dorf discloses a “multifunction card system” that adds a loyalty-card function to a payment card alongside its debit, phone-card, and gift-certificate functions. EX1009, Abstract. Dorf explains that “the system 108 ... may provide a separate loyalty card much like a frequent flier card that can have points added at virtually any POS device 105.” EX1009, 9:27-31. Dorf discloses that this loyalty function can be product- or manufacturer-specific, stating that “[t]he card could be issued by a certain manufacturer to reward a customer with loyalty points for purchasing the manufacturer’s product, regardless of the retail location of the purchase.” EX1009, 9:33-36; *generally id.*, 9:25-10:6. Likewise, “the card could be issued by a particular retailer to reward customers for purchases made in the retailer’s location(s),” crediting points “for any purchase within the store” or for “special promotional items.” EX1009, 9:53-58. Dorf further discloses that loyalty points accumulated in this manner may be redeemed for value, disclosing redemption “for an item selected from the group consisting of goods, services, discounts on goods and services, long distance telephone calling time value, and money value.” EX1009, 20:60-64.

D. The Maes-Dorf Combination (MDC)

82. Maes discloses a mobile device that stores information for multiple pre-enrolled “financial cards.” EX1004, 10:32-52, 12:9-23; *supra*, [1.3.1], [1.6.1]-[1.6.2]. Maes notes that the term “financial card” encompasses a wide range of

payment cards, including “credit cards, ATM cards and direct debit cards.”

EX1004, 1:50-54; *see also id.*, 2:25-27, 11:51-57. Maes does not provide an exhaustive list of different types of financial cards, as a POSITA would have been familiar with additional types not explicitly discussed in Maes. For example, as addressed above (*supra*, §VII.C), Dorf describes a financial card having a “loyalty function.” EX1009, 9:25-10:6, 12:22-27, 20:60-64. A POSITA would have found it obvious to implement Maes’s system in accordance with Dorf’s suggestion for attaching a loyalty function to a financial card. Multiple reasons would have motivated a POSITA to pursue this Maes-Dorf combination (“MDC”).

83. First, Maes already stores multiple types of financial card data, but discloses no mechanism for rewarding continued use of a given card. Given that the benefits of loyalty programs were well-established before the Critical Date of the ’807 Patent, a POSITA would have found it obvious to use a card with a loyalty-function in Maes’s system to encourage use of particular financial cards through Maes’s mobile-device based payment instrument. EX1004, 4:1-3, 5:24-27.

84. Second, attaching a loyalty-rewards balance to an existing payment card was, by the Critical Date, a widely recognized consumer convenience, as reflected in Dorf’s own description of frequent-flier-style loyalty programs already in common use. EX1009, 9:27-29.

85. Third, Maes's own card data already extends to non-payment types, such as "access control cards ... cash cards ... calling cards ... and employee cards." EX1004, 5:24-27. Thus, attaching a loyalty-point field to a financial card's data was simply one further, obvious selection from the range of data types Maes's architecture was already designed to accommodate.

86. Fourth, attaching Dorf's known loyalty-point functionality to Maes's existing financial cards amounts to a simple substitution or addition of a known element for a predictable result (*e.g.*, a loyalty function with point balance).

87. A POSITA would have had a reasonable expectation of success pursuing MDC. Indeed, loyalty-point crediting functions, such as the one Dorf discloses, were well known and conventional in the payment-card art long before the Critical Date. Accordingly, implementing a loyalty function on an existing financial card would have been a straightforward task.

E. Overview of Shults

88. Shults describes "a hand-held apparatus incorporating both electronic identity and optical identity," in which "[t]he electronic identity is provided by a radio-frequency electronic transponder 104." EX1008, [0024]. In Shults, "when a customer presents apparatus 100 at scanner 312 or 314, the point-of-sale system 304, 306, 308 determines the identity (electronic or optical) and sends that identity information to server complex 302 ... to identify the particular customer and

customer account associated with that apparatus.” EX1008, [0043]. Shults discloses that the electronic identity “is provided by a radio-frequency identification (RFID) circuit 104.” EX1008, [0030].

89. Per Shults, the apparatus can be “a portable cellular telephone or a personal digital assistant.” EX1008, [0009]. Shults further notes that “[t]he hand-held or portable aspect of apparatus 100 is particularly advantageous when it is used for purchasing or other types of financial transactions.” EX1008, [0024].

F. The Maes-Shults Combination (MSC)

90. Maes discloses that its PDA “may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:9-15; *supra*, §VII.A.

91. Maes further explains that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link ... via ... the RF port 50.” EX1004, 12:10-15.

92. Although Maes broadly describes the PDA having short-range RF circuitry, Maes does not disclose the specific type of RF circuitry applied in the PDA (or cellular phone). Shults does. Specifically, Shults describes a hand-held

apparatus in the form of “a portable cellular telephone or a personal digital assistant” whose “electronic identity is provided by a radio-frequency identification (RFID) circuit 104.” EX1008, [0009], [0030]. Shults’s RFID circuit 104 is implemented with a conventional, commercially available system such as “a Texas Instruments TIRIS system,” “a ROADCHECK system from Mark IV Inc.,” or “an ASSET ID system from HID Corp.” EX1008, [0031]. Shults’s “hand-held or portable aspect of apparatus 100 is particularly advantageous when it is used for purchasing or other types of financial transactions.” EX1008, [0024].

93. A POSITA would have found it obvious to implement the RF circuitry in Maes’s mobile device using RFID in accordance with Shults’s teachings. EX1004, 6:9-15, 12:10-15; EX1008, [0024], [0030], [0031]. Multiple reasons would have motivated the combination.

94. First, a POSITA would have been motivated to use RFID in Maes’s device because Shults confirms that an RFID-based electronic identity is “particularly advantageous when it is used for purchasing or other types of financial transactions” and Maes’s PDA is used for exactly this purpose. EX1004, 6:9-15, 12:10-15; EX1008, [0024].

95. Second, a POSITA would have been motivated to implement RFID in Maes’s device to enable transactions with existing point-of-sale systems without requiring modification to those systems. Shults explains that apparatus 100 “is

intended to be used with existing point-of-sale systems to the maximum extent possible, without requiring significant modifications to the point-of-sale system.” EX1008, [0037]. Adding Shults’s circuit 104 allows the mobile device to transact with existing point-of-sale systems having “electronic scanner equipment 314,” without substantial (or even any) modification to those systems. EX1008, [0037].

96. Third, a POSITA would have been motivated to use RFID in Maes’s device to achieve a cost-effective implementation using off-the-shelf, commercially available components. Indeed, Shults expressly teaches that RFID circuit 104 can be implemented with a conventional, commercially available system such as “a Texas Instruments TIRIS system,” “a ROADCHECK system from Mark IV Inc.,” or “an ASSET ID system from HID Corp.” EX1008, [0031].

97. Fourth, a POSITA would have been motivated to implement RFID in Maes’s device because doing so merely involved the application of a known RF technique (*e.g.*, RFID) that was both consistent with Maes’s RF-based embodiments and well within the POSITA’s technical grasp. A POSITA seeking to implement RF-based identification in Maes’s mobile device would have looked to Shults’s RFID circuit 104 as a familiar, readily available element performing its established function, requiring nothing more than ordinary skill to apply it as Maes’s RF circuitry. EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031].

98. The resulting Maes-Shults Combination (MSC) includes a mobile device (such as a PDA or cellular phone per Maes), whose RF circuitry (which uses “conventional constructions and techniques”) further includes Shults’s RFID circuit 104 (per Shults). *Supra*, Ground 1A at [1.2]; EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031]. MSC’s PDA operates as in Maes, including transmitting the selected card information to the POS transaction terminal via the RF port 50. *Supra*, Ground 1A at [1.2]; EX1004, 12:10-15.

99. A POSITA would have reasonably expected success applying RFID to Maes’s device, especially as Maes already contemplates the use of RF circuitry “using conventional constructions and techniques,” and Shults’s RFID circuit 104 represents such a conventional construction. EX1004, 6:9-15; EX1008, [0031].

G. Overview of Walker

100. Walker proposes to address security vulnerabilities associated with conventional credit card numbers, which are typically re-used across many transactions, by providing a “single-use, transaction-specific financial account number” that stands in for the cardholder’s real account number for one transaction only. EX1007, 1:17-19, Abst.. Walker discloses two embodiments for producing single-use numbers. In the first, the cardholder’s device cryptographically derives a new number for each transaction on the fly. EX1007, 6:60-7:9.

101. In the second embodiment, rather than cryptographically generating a fresh number for each transaction, Walker's device is provisioned with and draws from a pre-populated inventory of numbers. EX1007, 11:19-12:24, FIGS. 10-14. The device's memory stores "a database with a list of Single-use credit card numbers and a flag for each number indicating whether the number has already been used." EX1007, 11:21-24. These numbers are "assigned to the cardholder by the credit card issuer." EX1007, 11:24-25. To obtain a number for use in a transaction, the cardholder authenticates with the device (e.g., via PIN or biometric input), and the device then searches its stored list. If an unused number remains, it is displayed to the cardholder, and if none remain, the cardholder is instructed to obtain a new device from the credit card issuer. EX1007, 11:58-59. The device then updates that entry's status from "not used" to "used." EX1007, 11:60-62.

102. On the issuer side, a corresponding central processor maintains a mirror-image database associating each cardholder's account with its own list of numbers and their used/not-used status, so that when a merchant transmits a number for authorization, the issuer's processor checks whether the number matches one in its database and, if so, whether its status shows it has already been used, aborting the transaction if there is no match or if the number was already spent. EX1007, 12:17-42, FIG. 13. If the number checks out and the cardholder's

account satisfies the issuer's approval criteria, the issuer generates an authorization code and marks the number as used. *Id.*; *generally id.*, 11:19-12:24, FIGS. 10-14.

H. The Walker-Maes Combination (WMC)

103. The Walker-Maes Combination ("WMC") includes (per Walker) a device 100, including its keypad 103, display screen 102, memory 104, central processor 101, and biometric interface 105. EX1007, 5:52-54, 5:58-61. In WMC, device 100 is (per Maes) implemented as a mobile device such as a PDA or cellular phone that includes RF cellular circuitry, the RF processor module 48 and RF port 50, and the encrypter/decrypter module 24, as well as other functionalities of CPU 12. EX1004, 2:23-30, 5:14-17, 6:8-15, 14:12-16. *Supra*, Ground 1A at [1.1], [1.2], [5], [6].

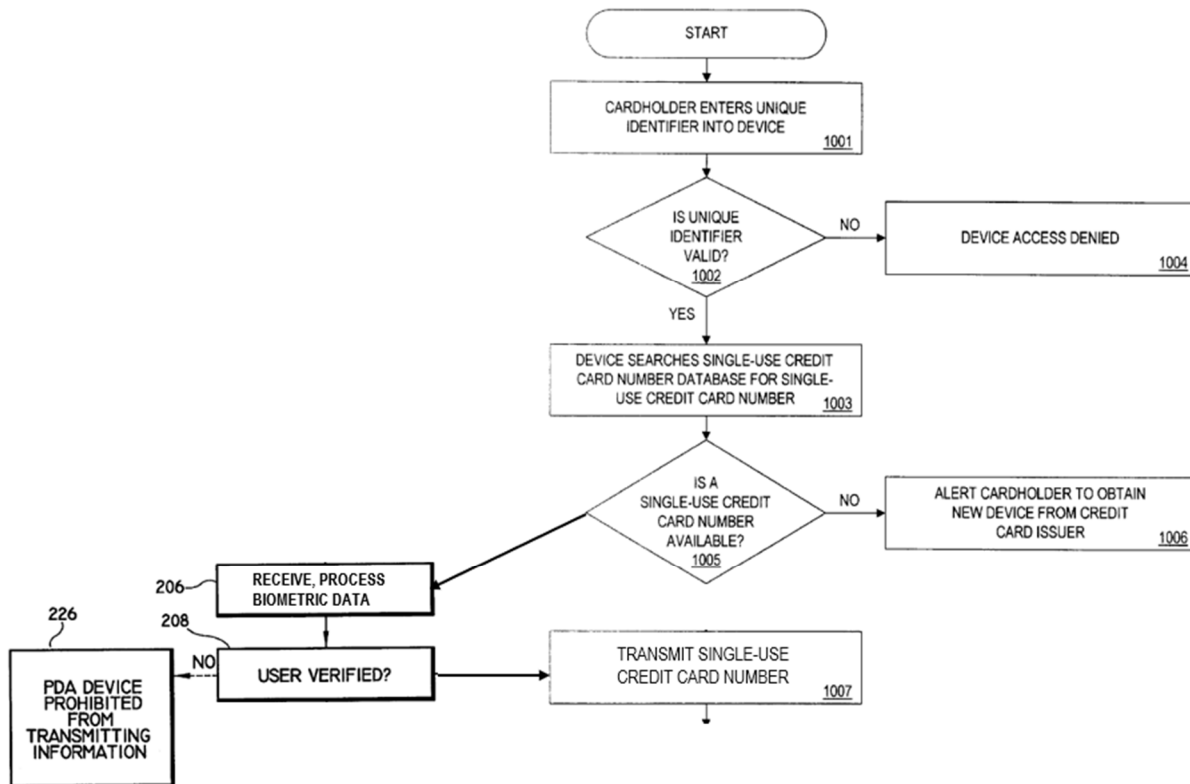
104. A POSITA would have been motivated to implement Walker's device 100 as a PDA or cellular phone, e.g., as described in Maes. A POSITA would have recognized that implementing device 100 as a PDA or cellular phone places the single-use credit card numbers on a device the cardholder carries and uses for other purposes, rather than requiring a separate dedicated device. EX1007, 11:21-25; EX1004, 14:2-7. Implementing device 100 as a PDA or cellular phone further supplies device 100 with the capability to provide the single-use credit card number over an RF link and to verify the cardholder biometrically at the time of

the transaction, providing the advantages described below. EX1004, 6:8-15, 12:9-16, 12:18-23.

105. A POSITA would have reasonably expected success in implementing device 100 as a PDA as described in Maes. Indeed, Walker's device 100 and Maes's PDA device 10 are portable, cardholder-carried devices having a central processor and a memory storing financial information. Implementing device 100 as a PDA combines known elements according to known methods to yield the predictable result of a portable device used to complete a purchase. EX1007, 5:52-54, 11:21-25; EX1004, 3:22-27.

106. In WMC, device 100 obtains a single-use credit card number pre-stored in memory 104 by performing the method of Walker's FIG. 10 according to Walker's second embodiment. EX1007, 11:21-25, 11:46-56; *generally id.*, 11:19-12:51. The cardholder enters a biometric identifier (step 1001); device 100 determines whether that identifier is valid for the device (step 1002) and denies access if it is not (step 1004); and if the identifier is valid, device 100 searches memory 104 for a single-use credit card number (step 1003) and determines whether one is available (step 1005). EX1007, 11:47-55. In Walker's FIG. 10 method, device 100 then displays that number on display screen 102 (step 1007). EX1007, 11:55-56.

107. Further in WMC, (per Maes) device 100 provides the single-use credit card number only if the cardholder is biometrically verified at the time of the transaction. EX1004, 12:9-16, 12:18-23, FIG. 5. Per Maes, before providing that number, device 100 receives the cardholder's biometric information through biometric interface 105, compares that information against the biometric authentication information stored in memory 104 (step 206), determines whether the cardholder is an authorized user (step 208), and withholds the number if the cardholder is not biometrically verified (step 226). EX1004, 10:54-61, 11:9-13, 12:18-23, FIG. 5; EX1007, 5:58-61. Additionally, per Maes, at step 1007, device 100 provides the single-use credit card number over RF port 50 rather than displaying it on display screen 102. EX1007, 11:55-56; EX1004, 12:9-16. The WMC process is illustrated in part below.



EX1004, FIG. 5 (excerpt, modified); EX1007, FIG. 10 (excerpt, modified).

108. A POSITA would have been motivated to provide the single-use credit card number over RF port 50 in place of displaying it on display screen 102 at step 1007. In Walker, the cardholder reads the single-use credit card number from display screen 102 and conveys it to the merchant, with Walker explaining that “[i]n step 1101, the cardholder provides the merchant with a single-use credit card number displayed on the device (see step 1007 of FIG. 10).” EX1007, 12:21-23. A POSITA would have recognized that manually reading and re-entering a credit card number is slow and prone to transcription errors.

109. Maes avoids such manual handling, explaining that a consumer transaction “may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal,” and that (in that embodiment) “the PDA device 10 itself actually takes the place of the Universal Card 26.” EX1004, 12:9-16, 12:23-29. Therefore, a POSITA would have been motivated to provide the single-use credit card number over the PDA’s RF port 50 instead of merely displaying it.

110. A POSITA would have reasonably expected success, because in WMC, device 100 includes RF processor module 48 and RF port 50 to enable such transmissions. EX1004, 6:8-15, 12:9-16.

111. Additionally, to improve security, in WMC, a POSITA would have been motivated to perform transaction-time biometric verification (per Maes) in addition to device-access authorization (per Walker). Maes explains that “[a]nother disadvantage in using financial cards is that consumers are not fully protected from the unauthorized use of lost or stolen cards.” EX1004, 2:1-3. In WMC, device 100 is implemented as a PDA, and a POSITA would have recognized that after the cardholder activates the PDA and before a transaction is attempted, the PDA may be lost or stolen or otherwise come into the possession of another person without the cardholder’s permission. EX1007, 5:56-61, 11:49-52; EX1004, 2:1-3, 2:23-30.

112. In response, Maes explains that the stored card information is not transmitted unless the user is biometrically verified at the time of the transaction, stating that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23, FIG. 5. A POSITA would therefore have been motivated to require the cardholder to present biometric information again immediately before device 100 provides the single-use credit card number (per Maes), so that provision confirms the identity of the person actually transacting.

113. Further, WMC retains both Walker’s and Maes’s determinations, and each serves a distinct role. Walker’s determination at step 1002 governs access to device 100, with Walker explaining that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:49-52. The transaction-time verification drawn from Maes governs release of the single-use credit card number used in a transaction, with Maes explaining that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. In WMC, device 100 performs both, and

provides the single-use credit card number only if the cardholder is biometrically verified at the time of the transaction. EX1007, 11:49-52; EX1004, 12:18-23.

114. A POSITA would have reasonably expected success. Device 100 (per Walker) already includes biometric interface 105 for receiving the cardholder's biometric information, and memory 104 already holds the biometric authentication information against which device 100 evaluates it. EX1007, 5:58-61, 11:47-52.

WMC adds a conventional comparison of biometric information, using components and stored information already present in device 100. The combination applies a known technique, conditioning release of stored payment information on contemporaneous biometric verification, to a similar device, with the predictable result that the stored number is provided only to the cardholder. EX1004, 12:18-23.

I. The Walker-Maes-Dorf Combination (WMDC)

115. Walker discloses single-use credit card numbers that can be used for credit card transactions. *Supra*, Ground 2A, [1.3.1]. Walker does not disclose an exhaustive list of payment cards types that its single use numbers could be used for, but Dorf explains that payment cards can be attached to a loyalty program. *Supra*, §VII.C. A POSITA would have found it obvious to attach a loyalty program like that described in Dorf to the credit card accounts disclosed in Walker, and a POSITA would have been motivated and reasonably expected success in pursuing

this Walker-Maes-Dorf combination (WMDC) for substantially similar reasons to those discussed above in Ground 1B. *Supra*, §VII.D.

J. The Walker-Maes-Shults Combination (WMSC)

116. The Walker-Maes-Shults Combination (WMSC) is WMC (Ground 2A), further modified in view of Shults’s teachings such that the RF circuitry in WMC’s mobile device is implemented using an RFID device. *Supra*, §§VII.E-F; EX1008, [0030]. For the reasons described in §VII.F, a POSITA would have been motivated to add Shults’s RFID circuit to WMC’s mobile device and would have reasonably expected success. *Supra*, §VII.F.

117. WMSC mobile device otherwise operates as in WMC, including transmitting the single-use credit card number to a POS terminal via short range RF circuitry. *Supra*, §VII.H; EX1008, [0030].

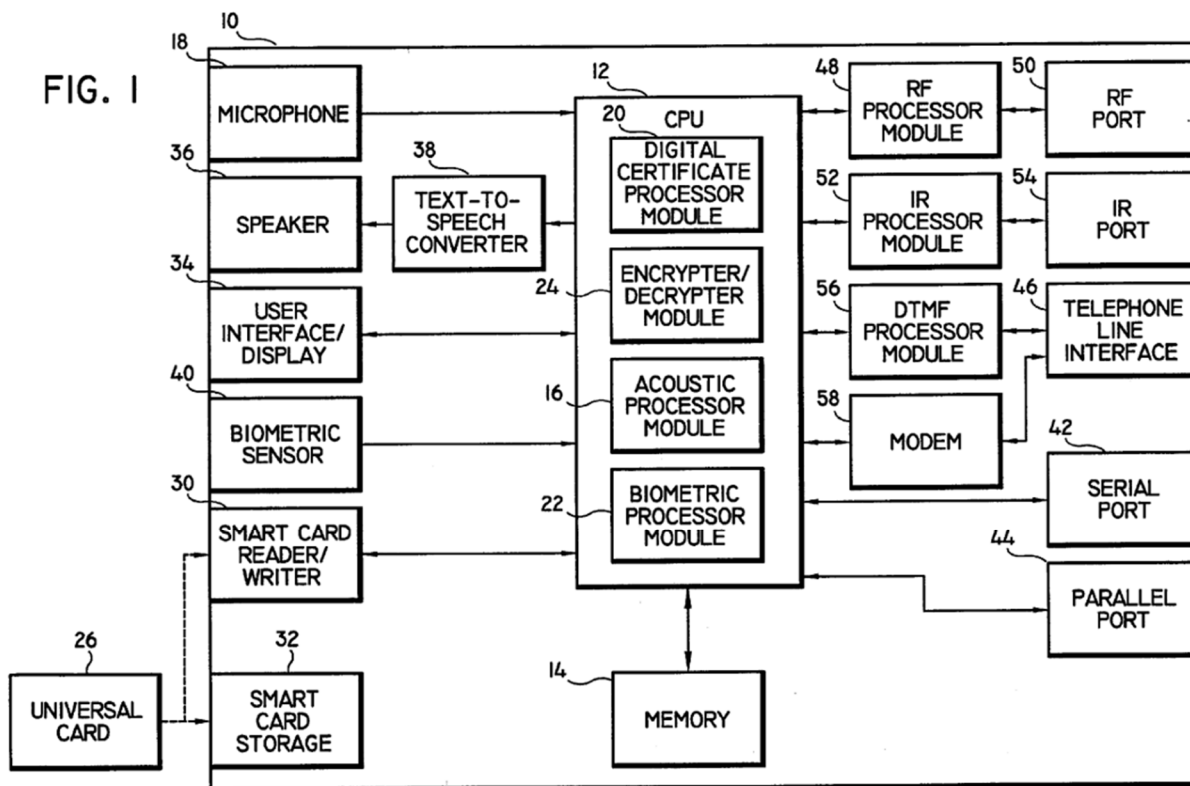
VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE ’807 CLAIMS UNPATENTABLE

A. Ground 1A: Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23

[1.pre] A mobile device, comprising:

118. Maes renders [1.pre] obvious.

119. Maes discloses a “portable client PDA” (*mobile device*), *e.g.*, PDA device 10 depicted in Fig. 1 below and embodied in a “cellular phone.” EX1004, Abstract, 4:65-6:27, 14:12-16 (“the functions and components of the PDA device 10 may be built into a cellular phone”).



EX1004, Fig. 1.

120. Maes's PDA "provide[s] direct communication capability with peripheral devices (such as POS ... terminals) and is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication." EX1004, Abstract; *see also id.*, 6:8-19, 12:5-29, Fig. 3.

[1.1] Radio Frequency (RF) cellular circuitry;

121. Maes renders [1.1] obvious.

122. Maes explains that its *mobile device* may be implemented as a cellular phone using cellular communication protocols, expressly disclosing that "the functions and components of the PDA device 10 may be built into a cellular phone,

whereby communication with the central server 60 may be achieved through a cellular communication channel, which may be analog or digital (e.g., CDMA, GSM, etc.).” EX1004, 14:12-17.

123. From these and related descriptions, a POSITA would have understood that Maes’s mobile device includes “***RF cellular circuitry***” that allows it to establish “communication ... through a cellular communication channel.”

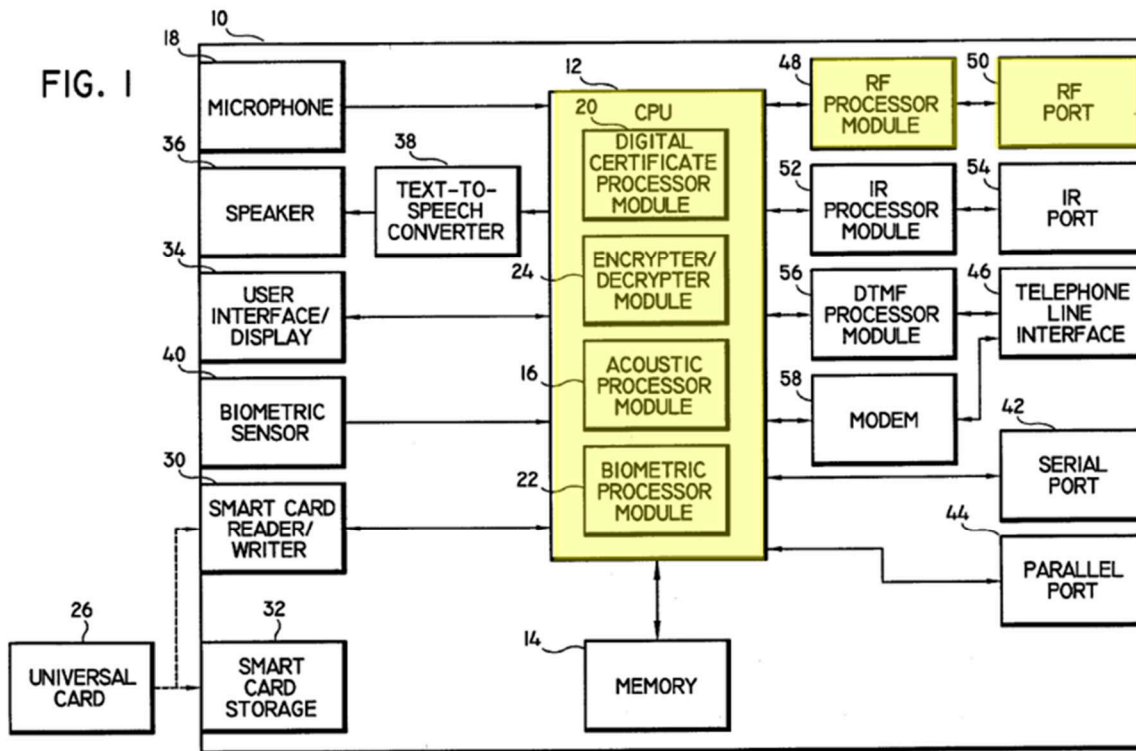
[1.2] short range RF circuitry;

124. Maes renders [1.2] obvious.

125. Maes’s mobile device “is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication.” EX1004, Abstract.

126. With reference to Fig. 1 (reproduced below), Maes explains that “the portable information and transaction processing (PDA) device 10” is “equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:1-27, 4:65-5:26.

From these and related descriptions, a POSITA would have understood that Maes’s mobile device includes ***short range radio frequency (RF) circuitry*** such as RF port 50, RF processor module 48, and/or CPU 12.



EX1004, Fig. 1 (highlighted).

127. A POSITA would have understood Maes's RF circuitry depicted in Fig. 1 to be "*short range*" circuitry. Maes describes an RF link L2 as a direct wireless channel between the PDA held by the user and the POS ... terminal 80. EX1004, 12:5-29 ("the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal"), Figs. 3, 5. Maes identifies its RF port 50 and IR port 54 as interchangeable options for the direct link, and IR communication is a short range line-of-sight technology. EX1004, 3:34-36, 12:13-15, 13:35-36. Maes also distinguishes its direct device-to-terminal RF link from the long-range wireless

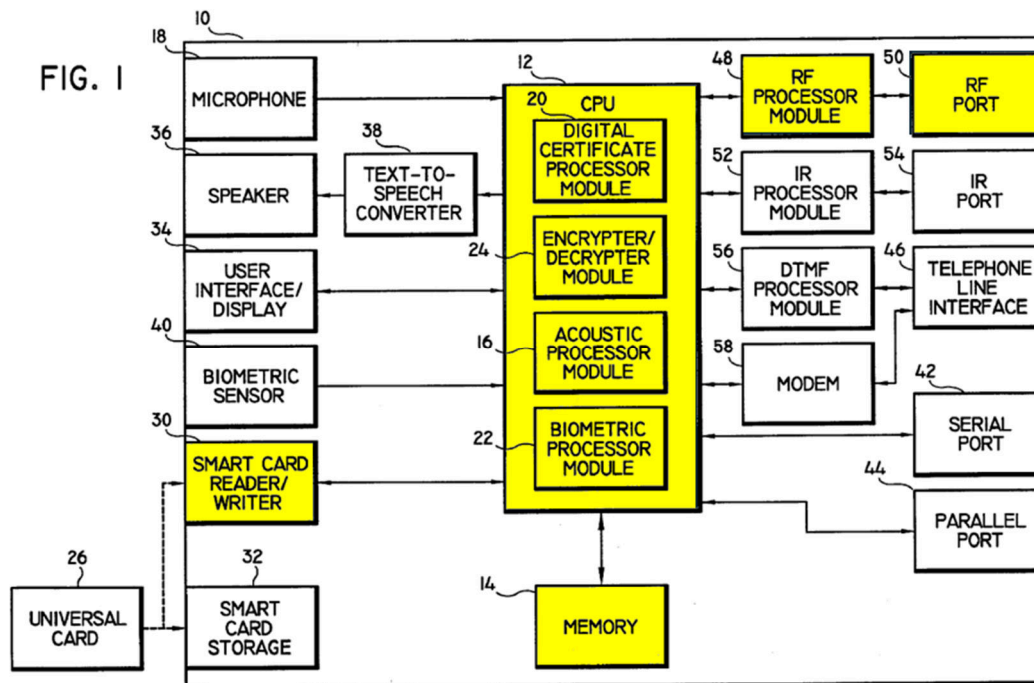
communications used to connect the PDA to remote central server 60 in client/server mode. EX1004, 7:65-8:14. Accordingly, a POSITA would have understood Maes's RF circuitry that is used for a direct link between the PDA and a nearby transaction terminal to be "*short range RF circuitry*."

[1.3.1] memory configured to store biometric authentication information and transaction information,

128. Maes renders [1.3.1] obvious.

129. Maes discloses that the mobile device "includes a memory for storing financial and personal information of the user." EX1004, Abstract; *see also id.*, ("selecting one of the pre-enrolled credit cards that are stored in the PDA").

130. With reference to Fig. 1 (reproduced below), Maes explains that "[t]he heart of the device is a central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12." EX1004, 5:1-4. "The CPU 12 also includes a digital certificate processor module 20, for processing a digital certificate obtained in the client/server mode of operation ... a biometric processor module 22 for processing biometric data ... to provide user verification," and "an encrypter/ decrypter module 24 for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user." EX1004, 5:8-17; *see also id.*, 5:18-24 (describing special-purpose processors and associated memory).



EX1004, Fig. 1 (highlighted).

131. The “financial information” that Maes’s memory 14 stores includes information for at least one credit card (*transaction information*). For example, Maes explains that “the user may ... download [credit card] information into the PDA device 10 by establishing a communication link (L1) with [a] central server 60.” EX1004, 7:1-4. “Alternatively, the credit ... may be loaded into the PDA device 10 by directly reading information contained on such cards through a smartcard reader/writer 30 of the PDA device 10.” *Id.*, 7:4-7. In “[t]he local mode of operation,” “the user select[s] a pre-enrolled credit card that is stored in memory 14” of the PDA device 10. *Id.*, 10:29-33, Figs. 1, 5. Then, a “consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established

communication link” *Id.*, 12:10-13; *see also id.*, 13:33-38. Accordingly, Maes’s “card information” constitutes **transaction information** stored in **memory** (*e.g.*, memory 14) of PDA-integrated cellular phone (**mobile device**) as claimed. *Supra*, §VI.

132. The “personal information” stored in memory 14 further includes **biometric authentication information**, such as voice or fingerprint data belonging to an authorized user of the PDA. For example, Maes explains that “biometric voice data is [] sent to [an] acoustic processor module 16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:57-61. Maes further discloses that “[a] biometric sensor 40 of any conventional type may also be provided for collecting biometric data ... such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification ...” EX1004, 5:54-60; *see also id.*, 5:13-17 (“encrypting the personal and financial information before being stored in memory 14”), 10:66-11:8, Figs. 1, 5. From these and related descriptions, a POSITA would have understood that the **memory** of Maes’s PDA’s stores **biometric authentication information** that the biometric processor module 22 uses to authenticate the user in a POS transaction.

[1.3.2] wherein the biometric authentication information has been previously associated with the transaction information;

133. Maes renders [1.3.2] obvious.

134. As discussed at [1.3.1], *supra*, Maes's mobile device's memory 14 stores the user's enrolled credit card information (*transaction information*) together with biometric records for that same user, such as voice data or data for the alternative biometric modalities Maes discloses (e.g., "finger, thumb or palm print, ... a retinal vascular pattern, or a combination thereof"). EX1004, 5:54-60; *supra*, [1.3.1]. Maes discloses that an association between the stored credit card information and biometric authentication information is created during an enrollment process that precedes later authentication event(s) at the time of a transaction.

135. For example, at enrollment, the service provider ties the user's designated account to the user's own credit card information, and that record is centrally stored. EX1004, 6:56-7:35, Fig. 3. Maes explains that "[e]nrollment involves ... providing the service provider with the user's credit card ... information so that such information can be verified with the financial institutions 70 that issued such cards." EX1004, 6:60-7:1. "This information is then stored on a central server 60 of the service provider." EX1004, 6:60-7:1.

136. This same enrollment record includes the user's biometric authentication information that has been captured and stored alongside account and PIN information for the user. For example, Maes discloses that "[a] personal identification number PIN and ... a unique account number 27 is provided by the

service provider,” and “[t]his information, as well as biometric data such as voice prints (models) of the user, are also stored in central server 60 of the service provider for user verification during the client/server mode to obtain a digital certificate.” EX1004, 7:25-32. From these and related descriptions, a POSITA would have understood that the user’s *biometric authentication information* in Maes is stored under, and tied to, the same account and PIN record established for that user’s enrolled credit card information (*transaction information*), thereby forming an association between the biometric authentication information and the transaction information created at enrollment.

137. That the association was formed in advance, rather than at the moment of the transaction, for example, is confirmed by Maes’s description of the “local mode” of operation following enrollment and the “client/server mode” of operation. Maes discloses that “[t]he local mode of operation is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14 (step 200),” using voice commands such as “I want to use my American Express Card.” EX1004, 10:32-36; *see also id.*, Fig. 5 (flowchart depicting “LOCAL MODE” operations), 12:5-29 (describing direct RF transmission embodiment between mobile device and POS terminal in local mode). Maes then requires that “[i]f the requested card information is found in memory, biometric verification must be performed” before the card information can be used. EX1004, 10:49-51; *see also*

id., Fig. 5. The mobile device performs user verification in local mode “by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:58-62; *see also id.*, 10:66-11:8 (“In another embodiment of the present invention, a biometric sensor 40 of any known type may be used in lieu of, or in conjunction with the microphone, to collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data, handwriting data, a retinal vascular pattern data or a combination thereof.”). A POSITA would have recognized that comparing incoming biometric data against “the user’s voice models stored in memory” (or stored data for other biometric modalities) to permit use of enrolled credit card information (*transaction information*) depends on the reference voice data already being bound to that particular user’s credit card information (*transaction information*) before the comparison is made, confirming the prior association between Maes’s biometric authentication information and the enrolled credit card information.

[1.4] a biometric reading device configured to read biometric information;

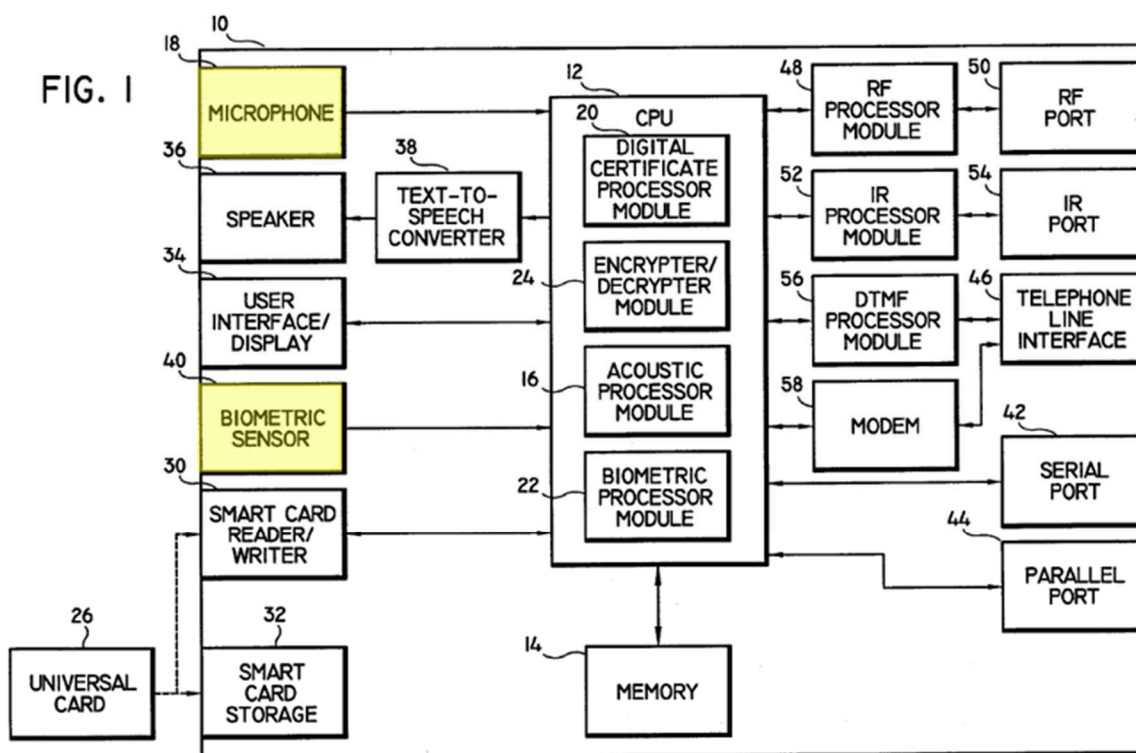
138. Maes renders [1.4] obvious.

139. Maes’s microphone 18 and biometric sensor 40, alternately or together, provide the claimed “*biometric reading device configured to read biometric information.*” Microphone 18 reads voice-based biometric information,

while biometric sensor 40 reads other forms of biometric information. EX1004, 5:53-62, 10:53-61, 11:1-14.

140. For example, Maes explains that its mobile device includes “a microphone and local central processing unit (CPU) for processing voice commands and for processing biometric data to provide user verification.” EX1004, Abstract. “[U]sing voice activated commands to select the desired card, the microphone 18 functions as a biometric sensor for receiving biometric voice data.” EX1004, 10:53-57, Fig. 1.

141. Likewise, with respect to Fig. 1 (reproduced below), Maes describes a “biometric sensor 40 of any conventional type ... for collecting biometric data (other than voice data which is received by the microphone 18) such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification as an alternative to, or in addition to, voice biometric verification.” EX1004, 5:54-60. “This data is then processed by the biometric processor module 22 to provide user verification (*i.e.*, biometric security) prior to accessing the financial and personal information stored in memory 14.” *Id.*, 5:60-63; *see also id.*, Abstract, 5:54-63, 10:49-11:8, Figs. 1, 5.



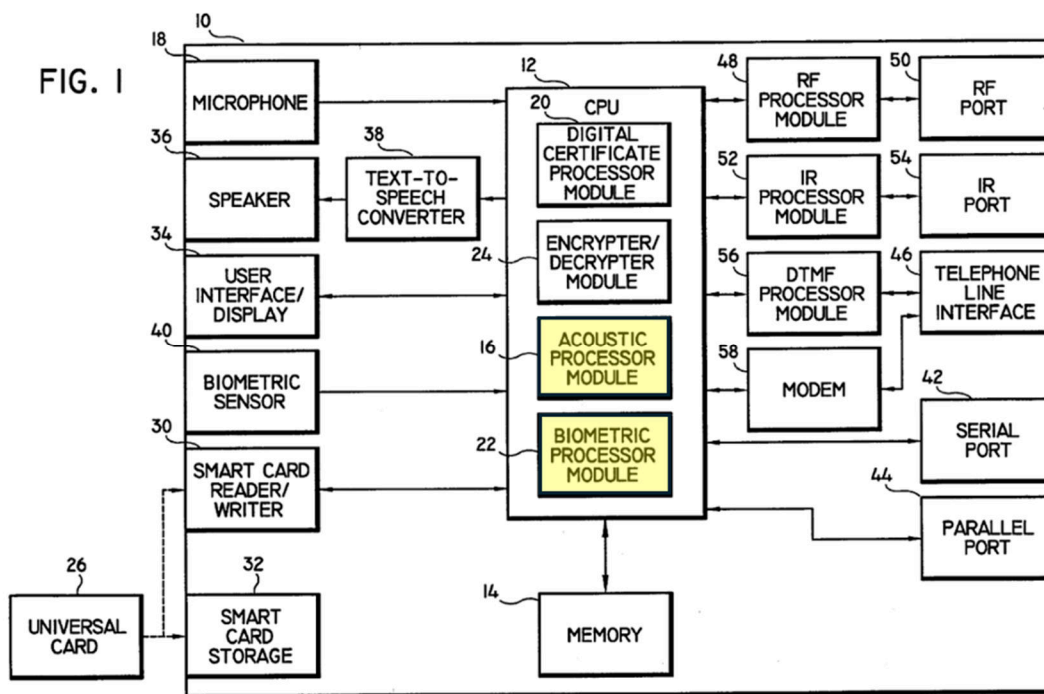
EX1004, Fig. 1 (highlighted).

[1.5] an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and

142. Maes renders [1.5] obvious.

143. Maes's "acoustic processor module 16," alternately or together with its "biometric processor module 22," provide an "**authentication module**" of the mobile device. Maes discloses that "[t]he acoustic processor module 16 is [] used for performing local speaker verification." EX1004, 5:7-8. Maes separately discloses that "the CPU 12 [] includes ... a biometric processor module 22 for

processing biometric data in addition to, or alternative to voice data, to provide user verification.” EX1004, 5:9-14. Maes ties these two modules together as alternately or together providing the same verification determination, stating that “[a]fter the biometric data is processed by the acoustic processing module 16 (when voice verification is utilized) or the biometric processor module 22 (when other biometric verification methods are used), or both, a determination is made as to whether the user is an authorized user (step 208).” EX1004, 11:9-13. A POSITA would have understood from these and related disclosures that either module alone, or the two operating together, can provide the authentication determination recited by [1.5] depending on whether voice-based biometrics, alternate biometric modalities, or both are employed.



EX1004, Fig. 1 (highlighted)

144. As discussed at [1.3.1]-[1.3.2] and [1.4], *supra*, Maes's memory 14 stores credit card information (*transaction information*) previously associated with the user's biometric records. Acoustic processor module 16 and/or biometric processor module 22 (*authentication module*) perform the claimed authentication by comparing biometric data newly read from the user against that previously stored, previously associated biometric record. EX1004, 10:58-62, Figs. 1, 3, 5. The device then conditions release of the selected credit card information for a transaction on the outcome of the comparison between the new and stored biometric records. *Id.*, 10:50-52.

145. In more detail, Maes discloses that “[i]f the requested card information is found in memory, biometric verification must be performed before the card information can be written to the Universal Card 26” for use in a transaction. EX1004, 10:50-52. As depicted in Fig. 5, user verification is similarly required before the card information will be retrieved from memory and decrypted for use in a transaction for those embodiments that involve direct transmission of card information from the mobile device to the POS terminal via short-range RF (without use of the Universal Card). EX1004, 12:5-29, Fig. 5.

146. Maes explains that comparison of the newly read biometric input to the stored biometric is performed by acoustic processor module 16 for the voice modality, stating that “[t]his biometric voice data is then sent to the acoustic processor module 16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:57-62. Maes describes the parallel operation for biometric processor module 22 when other biometric modalities are used, disclosing a biometric sensor 40 “to collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data, handwriting data, a retinal vascular pattern data or a combination thereof.” EX1004, 10:66-11:5. Maes further discloses that “[i]f the user is not verified, the selected card information will not be written” for use in a transaction. EX1004, 11:13-15, Fig. 5. Thus,

successful verification by acoustic processor module 16 and/or biometric processor module 22 allows the selected card information to be released for a transaction.

147. A POSITA would have understood the comparison performed by modules 16 and/or 22 to authenticate that the biometric information just read is associated with the transaction information at least because the comparison is made against the biometric record previously associated with that same user's account and credit card information at enrollment. Maes's mobile device thus authenticates that the biometric information just read is associated with transaction information in a manner that aligns exactly with the Patent Owner's explanation of such authentication to the examiner during prosecution. *See* EX1002, 41-42 ("The device can compare the biometric information input by the user with the stored biometric authentication information, which has already been associated with the transaction information. As such, verification of the user's identity allows the device to also authenticate the user's authorization with respect to the stored transaction information.").

[1.6.1] a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction

148. Maes renders [1.6.1] obvious.

149. Maes's CPU 12 alone or in coordination with RF processor module 48 and RF port 50, provides a "***transaction module***" as claimed. Maes identifies CPU

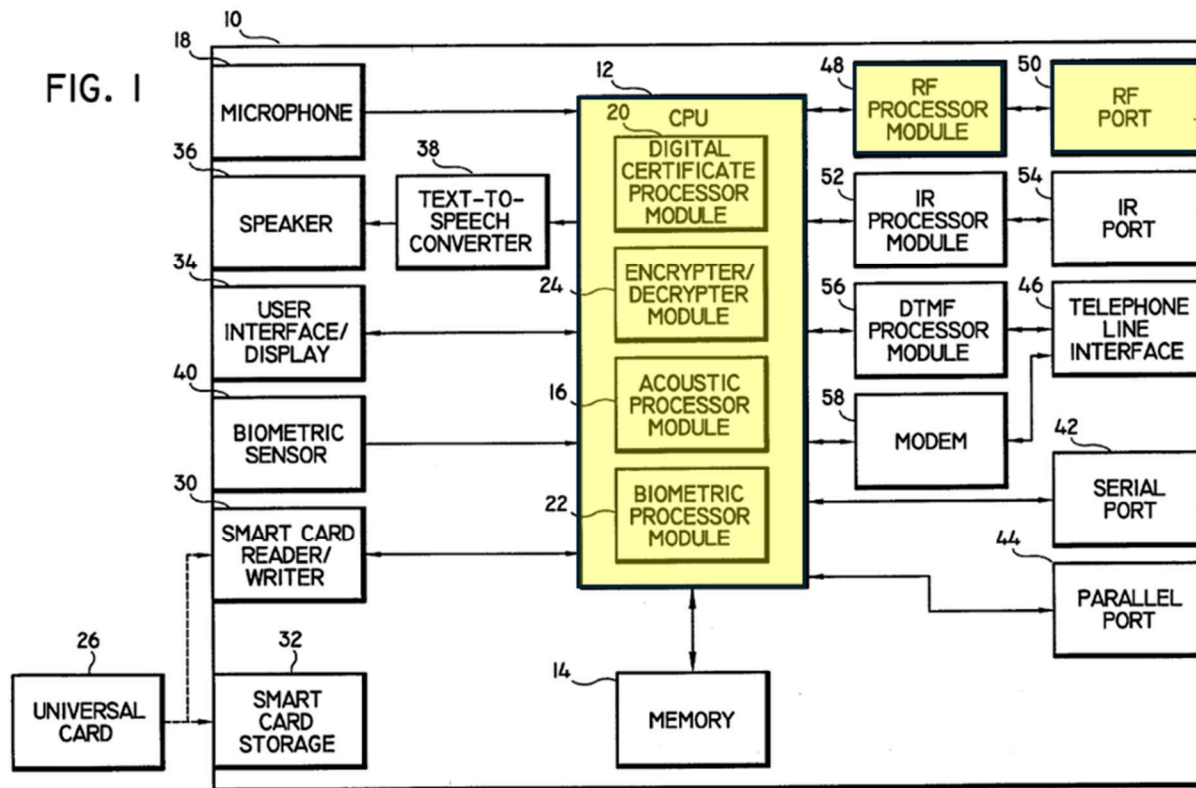
12 as the device's central controller, stating that "[t]he heart of the device is a central processing unit (CPU) 12, which controls the operations of the PDA device 10 via programs stored in a memory 14 and executed by the CPU 12." EX1004, 5:1-4. As discussed at [1.2], *supra*, RF processor module 48 and RF port 50 are short range RF circuitry. *Supra*, [1.2]. For example, Maes discloses that "the device may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques." EX1004, 6:8-15. A POSITA would have understood that CPU 12 directs what data is sent, while RF processor module 48 and RF port 50 carry out the physical wireless transmission, so that CPU 12 acting through this RF pathway provides selected credit card information (*transaction information*) for a transaction *via short range RF circuitry*.

150. Further illustrating this point, Maes discloses that CPU 12 retrieves the selected, stored credit card information from memory and the mobile device transmits it directly to the transaction terminal over the RF pathway. EX1004, 12:5-29; *see also id.*, 13:19-38 ("The selected card information ... would be transmitted to the POS terminal (via ... RF ...)"), Figs. 3, 5. Maes explains that "the invention may interact with electronic fund transfer systems or transaction

terminals having wireless or direct communication capabilities without even having to use the Universal Card 26.” EX1004, 12:5-8. Maes then describes the RF pathway for the transmission, noting that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 ... (i.e., via the ... RF port 50), rather than retrieving and writing card information to the Universal Card 26.” EX1004, 12:9-16. A POSITA would have understood the RF port 50 option in this passage to be the short range RF circuitry pathway, with CPU 12 as the component that retrieves the selected card data from memory and that directs its output through RF processor module 48 to RF port 50 for transmission to the terminal, thereby providing the transaction information via the short range RF circuitry for use in a transaction.

151. Maes further discloses that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. Further, according to Maes, “the PDA device 10 itself actually takes the place of the Universal Card 26 and, consequently, eliminates the need of having to first write the selected card information to the Universal Card 26 and then sweep the Universal Card 26 through the magnetic reader of the POS ... transaction terminal.” EX1004, 12:23-

29. A POSITA would have recognized that CPU 12 provides the selected card information for use in a transaction, including controlling whether and when specific card information is retrieved and transmitted over the RF pathway.



EX1004, Fig. 1 (highlighted)

[1.6.2] when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.

152. Maes renders [1.6.2] obvious.

153. As discussed at [1.6.1], *supra*, Maes's CPU 12, alone or cooperating with RF processor module 48 and RF port 50, discloses the claimed "***transaction module.***" Maes's transaction module retrieves the selected, stored credit card

information and transmits it directly to the POS transaction terminal over the short-range RF link. EX1004, 12:5-16.

154. Element [1.6.2] adds that the provision of the transaction information occurs “when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.” EX1001, claim 1. Maes discloses this exact condition. Indeed, the same portion of Maes that describes the CPU 12’s role in retrieving and transmitting selected credit card information for a transaction further explains that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23, Fig. 5. A POSITA would have understood the converse of this conditional statement, namely, that when the digital certificate is valid and the user is biometrically verified, CPU 12 retrieves and transmits the selected card information. EX1004, Fig. 5 (depicting card information transmitted from mobile device to POS terminal automatically when the user is verified).

155. Maes’s description of its local-mode of operation, which the column 12 direct-transmission embodiment modifies only at the output stage (see [1.6.1], *supra*), confirms that this triggering is automatic, and does not require any intervening user action between verification of the user and transmission of the

selected card information. To this point, Maes discloses that “[i]f the user is verified, the digital certificate (previously obtained in the client/server mode) is retrieved from memory 14 and loaded into the digital certificate processor module 20.” EX1004, 11:15-18. “If the digital certificate is valid (i.e., unexpired) the requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24,” with the selected card information “then decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10 (step 214)” before delivery. EX1004, 11:26-31. Maes’s process culminates in the mobile device’s transmission of selected card information via short-range RF. EX1004, 12:5-29, Fig. 5; *see also id.*, 13:19-38. Here, everything downstream of successfully matching the new biometric to the stored biometric is performed automatically by CPU 12 and its cooperating modules such that the selected card information is transmitted when the new biometric is successfully authenticated as being associated with the transaction information.

[2] The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

156. Maes renders [2] obvious.

157. For example, Maes discloses that “[a] biometric sensor 40 of any conventional type may also be provided for collecting biometric data (other than voice data which is received by the microphone 18) such as a finger, thumb or

palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification as an alternative to, or in addition to, voice biometric verification.” EX1004, 5:54-60; *see also id.*, 10:66-11:5 (“collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data”). A POSITA would have understood biometric sensor 40, configured to collect finger or thumb print data, to be a *fingerprint reading device* as recited in [2]. *Supra*, [1.4].

[3] The mobile device of claim 1, wherein the transaction information is generated based at least in part on credit card information.

158. Maes renders [3] obvious.

159. As discussed in connection with [1.3.1], *supra*, Maes discloses “*transaction information*” as enrolled credit card information stored in a memory of the mobile device and transmitted for use in a transaction. *Supra*, [1.3.1]. Maes discloses that the user enrolls this credit card data at the outset, stating that enrollment “involv[es] ... providing the service provider with the user’s credit card ... information so that such information can be verified with the financial institutions 70 that issued such cards.” EX1004, 6:61-67. Maes discloses that this same credit card information becomes the *transaction information* delivered for a purchase. Indeed, in local mode, “[t]he local mode of operation is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14 (step

200),” using a voice command such as “I want to use my American Express Card.”
EX1004, 10:32-36.

160. Maes further discloses that the process of first loading credit card data into the mobile device includes generating the stored ***transaction information*** from underlying credit card information. Specifically, Maes discloses two mechanisms loading credit card information in memory of the mobile device, including (1) downloading from the central server or (2) “directly reading information contained on such cards through the smartcard reader/writer 30 of the PDA device 10.” EX1004, 7:1-18. The PDA “will compare the user ID of the credit cards with the user ID of the PDA device to verify the user so as to prevent a user from downloading the information from cards owned by another person into the user’s PDA device 10.” EX1004, 7:7-12.

161. From these and related descriptions, a POSITA would have understood that Maes discloses that the card information on the mobile device is ***transaction information generated based at least in part on credit card information***, as recited in claim 3.

[5] The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

162. Maes renders [5] obvious.

163. Maes discloses that “[t]he CPU 12 further includes an encrypter/decrypter module 24 for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:13-17. A POSITA would have understood encrypter/decrypter module 24 to be a “**security block**” as recited in [5]. Indeed, Maes’s encrypter/decrypter module 24 adds security by encrypting the credit card information (**transaction information**) loaded on the device for secure storage in memory 14 and decrypts the credit card information for a transaction when the user is verified and the digital certificate is determined to be valid. EX1004, 5:13-18, 7:51-56, 11:27-29, Fig. 1.

164. Maes discloses that the encryption and thus securing of the credit card information on the device occurs before the credit card information is provided by the transaction module (*e.g.*, CPU 12 alone or in cooperation with RF processor module 48 and RF port 50, as established at [1.6.1]-[1.6.2], *supra*) for delivery over the short range RF link. EX1004, Figs. 3, 5. For example, Maes explains that encrypter/decrypter module 24 “encrypts the personal and financial information before being stored in memory 14.” EX1004, 5:14-17, Fig. 1-3. Maes further explains that the credit card information must be “RETRIEVED AND DECRYPTED” for use in a transaction before being “TRANSMITTED TO TRANSACTION TERMINAL” from the mobile device. EX1004, FIG. 5 (steps

214, 228); *see also id.*, 11:29-33 (“The selected card information is then decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10 (step 214).”), 12:5-29 (“transmitting the selected card information directly from the PDA device”), 5:13-17.

165. From these and related descriptions, a POSITA would have understood that Maes’s encrypter/decrypter module 24 (*security block*) is *configured to secure the transaction information before it is provided by the transaction module*.

[6] The mobile device of claim 5, wherein the security block is a cryptographic block.

166. Maes renders [6] obvious.

167. As discussed at [5], *supra*, Maes’s encrypter/decrypter module 24 (*security block*) performs its securing function specifically through encryption and decryption, stating that it is used “for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.” EX1004, 5:13-17; *see also id.*, 11:29-31 (“[t]he selected card information is then decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10 (step 214).”), 10:11-15 (“may employ any known encryption technique or algorithm for the encryption/decryption process”). A POSITA would have understood a security

block whose disclosed operation is encrypting and decrypting data using cryptographic keys to be a *cryptographic block* as recited in claim [6].

[8] The mobile device of claim 1, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

168. Maes renders [8] obvious.

169. As discussed above, Maes's CPU 12, alone or together with RF processor module 48 and RF port 50 (*transaction module*) provides selected credit card information for a transaction via the short range RF circuitry. *Supra*, [1.6.1]-[1.6.2]. Maes explains that "the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 ... (i.e., via ... the RF port 50), rather than retrieving and writing card information to the Universal Card 26." EX1004, 12:9-16; *see also id.*, 13:34-38 ("via ... RF").

170. While Maes discloses that the selected credit card information (*transaction information*) is transmitted from the mobile device to the POS terminal via RF, nowhere does Maes disclose any corresponding transmission of biometric information. *See e.g.*, EX1004, 12:9-23, 13:25-36, Fig. 5. A POSITA would have understood Maes's silence as to any transmission of biometric information for use in a transaction as reflecting the reality that only Maes's credit

card information (*transaction information*), but not the biometric information, is what the transaction module actually provides via RF in Maes's framework.

171. Maes's broader description of how biometric data is used confirms that its omission of any transmission of biometric information in local mode reflects a specific design choice to keep biometric information on device. Maes discloses that biometric data is captured and consumed entirely within the PDA's own local-mode processing loop: "[t]his biometric voice data is then sent to the acoustic processor module 16 wherein such data is processed (step 206) by comparing the current biometric voice data with the user's voice models stored in memory 14." EX1004, 10:58-62. That comparison takes place using biometric data stored on memory 14 and the CPU 12 processing modules. *Supra*, [1.3.1]. The central server and financial institution then verify the user and determine whether to authorize a transaction based on the selected card information, assurances that the authorization number and card information could not be accessed without user verification and a valid digital certificate, and optionally further based on an electronic information file that accompanies the card information. EX1004, 12:5-13:38, Fig. 5. Neither the central server nor the financial institution processes the biometric information just received from the user involved in the transaction, and thus the mobile device does not provide biometric information to the merchant, the financial institution, or central server. Indeed, there is no need to do so in the

context of Maes's system. At a minimum, a POSITA would have found it obvious not to transmit the biometric information because not transmitting it when the backend systems make no use of it would result in a more efficient and less time-consuming transmission of data over the short-range RF link during a transaction.

[9.pre] A mobile device, comprising:

172. *Supra*, [1.pre].

[9.1] Radio Frequency (RF) cellular circuitry;

173. *Supra*, [1.1].

[9.2] short range RF circuitry;

174. *Supra*, [1.2].

[9.3.1] memory configured to store biometric authentication information and transaction information,

175. *Supra*, [1.3.1].

[9.3.2] wherein the biometric authentication information has been previously associated with the transaction information;

176. *Supra*, [1.3.2].

[9.4] a biometric reading device configured to read biometric information;

177. *Supra*, [1.4].

[9.5] an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory;

178. *Supra*, [1.5].

[9.6.1] a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction

179. *Supra*, [1.6.1].

[9.6.2] when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module; and

180. *Supra*, [1.6.2].

[9.7] a security block configured to secure the transaction information before it is provided by the transaction module.

181. *Supra*, [5].

[10] The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

182. *Supra*, [2].

[11] The mobile device of claim 9, wherein the transaction information is generated based at least in part on credit card information.

183. *Supra*, [3].

[13] The mobile device of claim 9, wherein the security block is a cryptographic block.

184. *Supra*, [6].

[15] The mobile device of claim 9, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

185. *Supra*, [8].

[16.pre] A cellular telephone, comprising:

186. Maes renders [16.pre] obvious.

187. Maes discloses a “portable client PDA,” e.g., PDA device 10 depicted in Fig. 1. EX1004, FIG. 1; *supra*, [1.pre]. Maes further discloses that “the functions and components of the PDA device 10 may be built into a cellular phone, whereby communication with the central server 60 may be achieved through a cellular communication channel, which may be analog or digital (e.g., CDMA, GSM, etc.).” EX1004, 14:12-16. A POSITA would have understood from these and related descriptions that Maes discloses a *cellular telephone*.

[16.1] Radio Frequency (RF) cellular circuitry;

188. *Supra*, [1.1].

[16.2] short range RF circuitry;

189. *Supra*, [1.2].

[16.3.1] memory configured to store biometric authentication information and transaction information,

190. *Supra*, [1.3.1].

[16.3.2] wherein the biometric authentication information has been previously associated with the transaction information;

191. *Supra*, [1.3.2].

[16.4] a biometric reading device configured to read biometric information;

192. *Supra*, [1.4].

[16.5] an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and

193. *Supra*, [1.5].

[16.6.1] a transaction module configured to provide the transaction information for use in a transaction

194. *Supra*, [1.6.1].

[16.6.2] when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module.

195. *Supra*, [1.6.2].

[17] The cellular telephone of claim 16, wherein the biometric reading device is a fingerprint reading device.

196. *Supra*, [2].

[18] The cellular telephone of claim 17, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

197. *Supra*, [5].

[19] The cellular telephone of claim 18, wherein the security block is a cryptographic block.

198. *Supra*, [6].

[20] The cellular telephone of claim 16, wherein the transaction information is generated based at least in part on credit card information.

199. *Supra*, [3].

[23] The cellular phone of claim 16, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

200. *Supra*, [8].

B. Ground 1B: Maes-Dorf Renders Obvious Claims 4, 12, and 21

[4] The mobile device of claim 1, wherein the transaction information is generated based at least in part on rewards card information.

201. MDC renders [4] obvious.

202. As discussed above in Ground 1A, Maes discloses that the card information (***transaction information***) used in a transaction can be generated based at least in part on credit card information. *Supra*, Ground 1A at [3]. Maes further discloses that a range of different types of financial cards can be employed. EX1004, 1:50-54, 2:25-27, 2:50-57, 11:51-57.

203. Dorf further describes the well-known option of attaching a loyalty function to a financial card. *See e.g.*, EX1009, 9:25-10:6, 12:22-27, 20:60-64; *supra*, §VII.C. A POSITA would have understood that the use of a loyalty function as suggested by Dorf with the types of financial cards described in Maes would result in generation of transaction information ***based at least in part on rewards card information***, as recited in claim 4. For example, Dorf describes how a loyalty-point balance associated with the card allows the cardholder to earn loyalty points as rewards for use of the card. EX1009, 9:33-36 (“reward a customer with

loyalty points”), 9:9-13 (“award loyalty points”), 12:22-27. The transaction information in MDC is generated based on rewards card information in the same fashion that transaction information is generated in Maes based on credit card information. *Supra*, §VII.D.

[12] The mobile device of claim 9, wherein the transaction information is generated based at least in part on rewards card information.

204. *Supra*, [4].

[21] The cellular telephone of claim 16, wherein the transaction information is generated based at least in part on rewards card information.

205. *Supra*, [4].

C. Ground 1C: Maes-Shults Renders Obvious Claims 7, 14, and 22

[7] The mobile device of claim 1, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

206. MSC renders [7] obvious.

207. In MSC, Maes’s mobile device includes short-range RF circuitry (*see supra*, Ground 1A at [1.2]), and that circuitry further includes an RFID circuit consistent with Shults’s teachings. *Supra*, §§VII.E-F, Ground 1A at [1.2]; EX1008, [0030].

208. Therefore, a POSITA would have understood that in MSC, the mobile device’s ***short-range RF circuitry comprises an RFID device***. *Supra*, §VII.F; EX1008, [0030].

[14] The mobile device of claim 9, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

209. *Supra*, [7].

[22] The cellular telephone of claim 16, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

210. *Supra*, [7].

D. Ground 2A: Walker-Maes Renders Obvious Claims 1-3, 5-6, 8-11, 13, 15-20, 23[1.pre] A mobile device, comprising:

211. WMC renders [1.pre] obvious.

212. Walker describes “a device 100 for generating a single-use credit card number in accordance with this invention.” EX1007, 5:49-51. Walker further explains that “[t]his device is preferably a smart card,” and that “[t]he device has a keypad 103, a display screen 102, a memory 104 and a central processor 101.” EX1007, 5:51-54.

213. Maes describes “a portable information and transaction processing device (‘personal digital assistant’ or ‘PDA’) in which a user can store his or her credit card[] ... (i.e., financial) information, as well as personal information.” EX1004, 2:23-30. “Moreover, the functions and components of the PDA device 10 may be built into a cellular phone.” EX1004, 14:11-16.

214. In WMC, Walker’s device 100 is implemented as a PDA or cellular phone consistent with Maes’s teachings. EX1007, 5:49-51; EX1004, 2:23-30.

WMC retains the keypad 103, display screen 102, memory 104 and central processor 101 Walker describes. EX1007, 5:51-54.

[1.1] Radio Frequency (RF) cellular circuitry;

215. *Supra*, Ground 1A at [1.1]. The Walker-Maes device includes Maes's RF cellular circuitry.

[1.2] short range RF circuitry;

216. *Supra*, Ground 1A at [1.2]. The Walker-Maes device includes Maes's short-range RF circuitry.

[1.3.1] memory configured to store biometric authentication information and transaction information,

217. WMC renders [1.3.1] obvious.

218. Walker explains that "the device memory 104 includes a database with a list of single-use credit card numbers and a flag for each number indicating whether the number has already been used," and that "[t]he single-use credit card numbers are assigned to the cardholder by the credit card issuer." EX1007, 11:21-25. These pre-stored single-use credit card numbers include *transaction information*. EX1007, 11:21-25. Indeed, Walker describes various techniques for generating single-use numbers, including embedding within each single-use number *transaction information* in the form of a credit-card account number A. EX1007, 11:26-45. Walker allows card issuers to assign account numbers (*transaction information*) for credit card accounts in any fashion, including

assigning different account numbers to different users. *Id.*; *see also id.*, 1:20-21, 6:54-59, 6:66-7:1, 8:20-26, Fig. 8.

219. Walker further explains that “the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder’s fingerprint.” EX1007, 5:58-61. Walker states that “[i]n step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device.” EX1007, 11:47-49. Walker adds that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:49-52. Thus, device 100 determines the validity of an “identifier” that is the biometric data the cardholder enters. EX1007, 11:47-52. A POSITA would have understood, or at minimum found obvious, that device 100 determines whether entered biometric data is valid for the device by comparing it to reference biometric information. EX1007, 11:47-52. It further would have been understood or obvious that memory 104 holds the reference biometric information.

220. To the extent Walker does not expressly recite storing that reference information, Maes does. *Supra*, Ground 1A at [1.3.1]. Maes describes processing biometric data “by comparing the current biometric voice data with the user’s voice models stored in memory 14.” EX1004, 10:57-61. Applying Maes’s suggestion to store the reference biometric authentication information in the

memory of Walker's device would have been obvious to permit local and efficient comparison of a user's current biometric input to the stored reference biometric authentication information, since the biometric authentication information would not need to be retrieved from off-device storage.

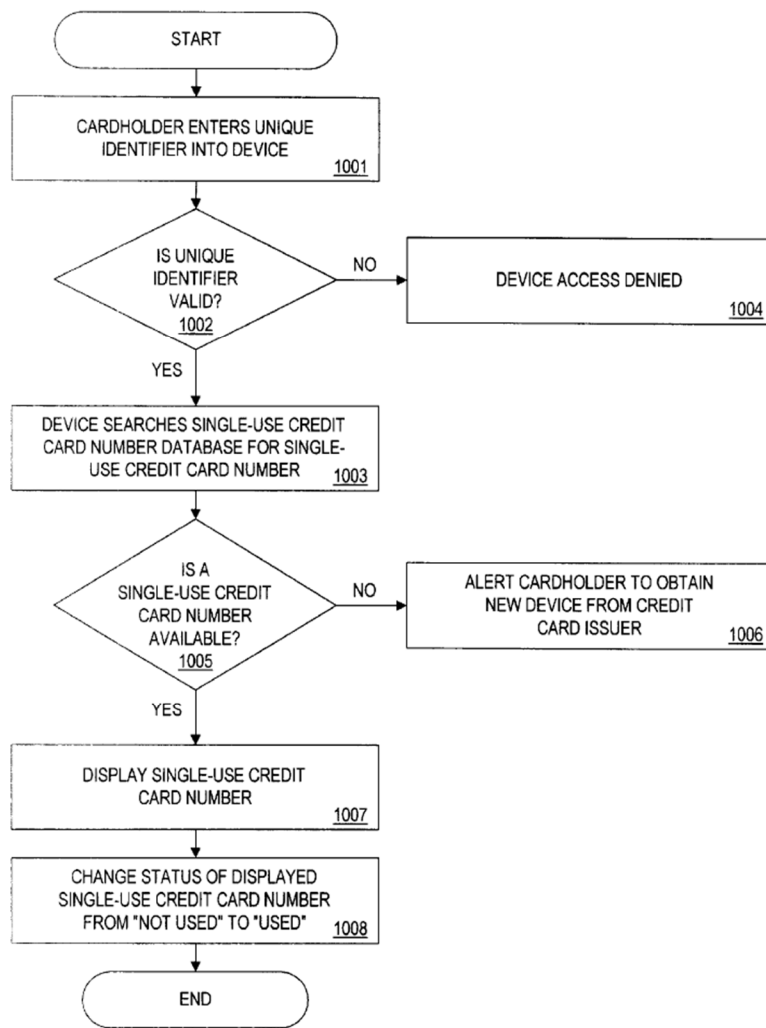
221. Therefore, in WMC, it would have been obvious for the memory (e.g., memory 104) to store both the biometric authentication information and the single-use credit card numbers. EX1007, 11:21-25, 11:47-52; EX1004, 10:57-61.

[1.3.2] wherein the biometric authentication information has been previously associated with the transaction information;

222. WMC renders [1.3.2] obvious.

223. In Walker, the biometric authentication information and the transaction information are stored in advance on the same device for the same user. Walker explains that the single-use credit card numbers including account numbers (*transaction information*) held in memory 104 “are assigned to the cardholder by the credit card issuer.” EX1007, 11:21-25. Memory 104 also holds the biometric authentication information against which device 100 evaluates the identifier the cardholder enters. *Supra*, [1.3.1]. Because Walker refers throughout to a single cardholder who possesses device 100, holds the numbers assigned to that cardholder, and enters an identifier valid for that device, a POSITA would have understood that the cardholder who enters that identifier is the same cardholder to whom the issuer assigned the stored numbers. EX1007, 11:21-25, 11:47-52.

224. Walker further explains that “[i]f the identifier is valid, the device searches the single-use credit card number database in the device memory 104 for a single-use credit card number (step 1003).” EX1007, 11:52-54. Because step 1003 searches a database of numbers held in memory 104, and step 1002 evaluates the entered identifier against biometric authentication information held in memory 104, a POSITA would have understood that both are present in memory 104 before the cardholder enters an identifier at step 1001 (which precedes steps 1002 and 1003). EX1007, 11:21-25, 11:47-54. The biometric authentication information and single-use card number database including the account numbers are also associated insofar as Walker only permits access to the device, and therefore to the account numbers, if the user is biometrically authenticated by comparison of a user’s current biometric to the reference biometric stored in memory. EX1007, 5:58-61, 6:19-29, 11:46-52. Likewise, per Maes, in WMC, the biometric authentication information is used in the transaction-time user verification operation. The stored biometric authentication information thus functionally gates access to the single-use card numbers (including the account number in the single-use numbers) based on the association. It also would have been obvious for the device to store data linking the biometric authentication information to the single-use numbers (including the account number) to enable more efficient authentication and access to the single-use numbers.



EX1007, FIG. 10.

225. Maes corroborates Walker’s approach. In Maes, “[i]f the requested card information is found in memory, biometric verification must be performed before the card information can be written to the Universal Card 26.” EX1004, 10:49-51. Because Maes’s PDA device 10 holds the user’s card information in memory 14 and compares that user’s biometric data against biometric data stored in memory 14, a POSITA would have recognized that Maes’s stored biometric data

has been previously associated with Maes's stored card information. EX1004, 2:23-30, 10:49-51, 10:57-61. *Supra*, Ground 1A at [1.3.2].

226. Therefore, in WMC, memory 104 stores, in advance and for the same cardholder, the biometric authentication information and the transaction information. EX1007, 11:21-25, 11:47-54; EX1004, 10:49-51. Accordingly, the biometric authentication information has been previously associated with the transaction information.

[1.4] a biometric reading device configured to read biometric information;

227. WMC renders [1.4] obvious.

228. Walker explains that "the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." EX1007, 5:58-61. Walker further states that "[i]n step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device." EX1007, 11:47-49. Because biometric interface 105 receives the cardholder's fingerprint as input to device 100, a POSITA would have understood that biometric interface 105 reads biometric information and is therefore a biometric reading device. EX1007, 5:58-61, 11:47-49.

229. Maes corroborates Walker's approach. In Maes, "[a] biometric sensor 40 of any conventional type may also be provided for collecting biometric data."

EX1004, 5:54-60. A POSITA would have recognized that Maes's biometric sensor 40 is a biometric reading device. EX1004, 5:54-60. *Supra*, Ground 1A at [1.4].

230. Therefore, in WMC, biometric interface 105 is a biometric reading device configured to read biometric information. EX1007, 5:58-61, 11:47-49; EX1004, 5:54-60.

[1.5] an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and

231. WMC renders [1.5] obvious.

232. During prosecution, the applicant explained that the device compares the biometric information the user inputs against stored biometric authentication information that was previously associated with the transaction information, writing that "[t]he device can compare the biometric information input by the user with the stored biometric authentication information, which has already been associated with the transaction information." EX1002, 41. The applicant added that "verification of the user's identity allows the device to also authenticate the user's authorization with respect to the stored transaction information." EX1002, 41. The applicant placed that comparison on the device itself, explaining that "in other embodiments, the biometric reading device is included in the mobile device, thus

enabling the authentication process to be performed entirely on the device.”

EX1002, 41-42.

233. WMC performs those steps. The biometric authentication information stored in memory 104 has been previously associated with the transaction information stored in memory 104. *Supra*, [1.3.2].

234. Per Walker, WMC includes the component that performs that comparison, explaining that “[t]he device has a keypad 103, a display screen 102, a memory 104 and a central processor 101.” EX1007, 5:52-54. Walker further explains that “[i]n step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device,” and that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:47-52. Because device 100 determines at step 1002 whether the biometric data entered at step 1001 is valid, and makes that determination against the biometric authentication information held in memory 104, a POSITA would have understood that central processor 101 compares the biometric information read by biometric interface 105 against the biometric authentication information stored in memory. EX1007, 5:51-54, 11:47-52. *Supra*, [1.3.1].

235. Per Maes, WMC performs that comparison again when the cardholder attempts a transaction and withholds the transaction information unless the

comparison succeeds. *Supra*, §VII.H. Maes describes “a biometric processor module 22 for processing biometric data in addition to, or alternative to voice data, to provide user verification.” EX1004, 5:8-14. Maes explains that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. Because Maes prohibits the stored card information from being retrieved and transmitted to transaction terminal 80 unless the user is biometrically verified against the biometric authentication information stored in memory 14, a POSITA would have understood that Maes performs its biometric verification when the user attempts to perform a transaction and permits the stored card information to be provided only when that verification succeeds. EX1004, 12:18-23. *Supra*, Ground 1A at [1.5].

236. In WMC, when the cardholder attempts to perform a transaction, central processor 101 compares the biometric information read by biometric interface 105 against the biometric authentication information stored in memory 104 and prohibits the transaction information from being provided if that comparison does not succeed. EX1007, 5:51-54, 11:47-52; EX1004, 12:18-23. Further, in WMC, a successful comparison confirms that the biometric information read by biometric interface 105 matches the biometric authentication information

in memory 104. EX1007, 11:47-52. That biometric authentication information was previously associated with the transaction information in memory 104. EX1007, 11:21-25. *Supra*, [1.3.2]. Central processor 101 therefore authenticates that the biometric information read by biometric interface 105 is associated with the transaction information and does so based at least in part on the biometric authentication information stored in memory 104 (*supra*, [1.3.1]). EX1007, 11:47-52; EX1004, 12:18-23. A POSITA would therefore have understood that central processor 101 (which performs the biometric comparison) is an authentication module.

237. Therefore, in WMC, central processor 101 provides an authentication module configured to authenticate, during a transaction, that the biometric information read by biometric interface 105 is associated with the transaction information, based at least in part on the biometric authentication information stored in memory 104. EX1007, 5:51-54, 11:47-52; EX1004, 12:18-23.

[1.6.1] a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction

238. WMC renders [1.6.1] obvious.

239. Walker explains that “[i]f a single-use credit card number is available (step 1005), it is displayed on the device display screen 102 (step 1007)”. EX1007, 11:55-56. Walker further explains that “[i]n step 1101, the cardholder provides the

merchant with a single-use credit card number displayed on the device (see step 1007 of FIG. 10).” EX1007, 12:21-23. Because device 100 retrieves the single-use credit card number from memory 104 (step 1003) and that number is provided to the merchant to complete the transaction (step 1007), a POSITA would have understood that device 100 provides the transaction information (the account number in the single-use credit card number) for use in a transaction. EX1007, 11:52-56, 12:21-23.

240. Per Maes, WMC transmits the transaction information over a short range RF link. Maes explains that “the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ... POS transaction terminal through an established communication link L2 (step 228, FIG. 3) (i.e., via the serial port 42, the parallel port 44 modem 42, the IR port 54 or the RF port 50), rather than retrieving and writing card information to the Universal Card 26.” EX1004, 12:9-16. Maes further explains that “the device may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, for processing incoming RF information received by the RF port 50, and for generating transmission signals which are outputted from the RF port 50 using conventional constructions and techniques.” EX1004, 6:8-15. RF port 50 and RF processor module 48 are short range RF circuitry. *Supra*, [1.2].

241. In WMC, device 100 provides the single-use credit card number retrieved at step 1003 to the transaction terminal over RF port 50, in place of displaying it on display screen 102 at step 1007. EX1007, 11:52-56; EX1004, 6:8-15, 12:9-16. *Supra*, §VII.H. Because central processor 101 passes that number to RF processor module 48, which generates the transmission signals output from RF port 50, a POSITA would have understood that those components are a transaction module. EX1004, 6:8-15.

242. Therefore, in WMC, a transaction module provides the transaction information via short range RF circuitry for use in a transaction. EX1007, 11:52-56, 12:21-23; EX1004, 6:8-15, 12:9-16.

[1.6.2] when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.

243. WMC renders [1.6.2] obvious.

244. In Walker, device 100 retrieves the stored transaction information only after the cardholder's biometric information is determined valid, with Walker explaining that "[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004)," and that "[i]f the identifier is valid, the device searches the single-use credit card number database in the device memory 104 for a single-use credit card number (step 1003)." EX1007, 11:49-54. *Supra*, [1.5].

245. Per Maes, WMC makes a complementary determination when the cardholder attempts a transaction. *Supra*, §VII.H. Maes explains that “the CPU 12 of the PDA device 10 will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified and/or if the digital certificate is not valid (step 226).” EX1004, 12:18-23. Because Maes prohibits the stored card information from being retrieved and transmitted to transaction terminal 80 unless the user is biometrically verified against the biometric authentication information stored in memory 14, a POSITA would have understood that Maes performs its biometric verification when the user attempts to perform a transaction and permits the stored card information to be provided only when that verification succeeds. EX1004, 12:18-23.

246. In WMC, the transaction module provides the single-use credit card number over RF port 50 only when the authentication (performed by central processor 101 for that transaction) of the cardholder’s biometric information succeeds at the time of the transaction. EX1007, 11:52-56; EX1004, 12:18-23. *Supra*, [1.5], [1.6.1]. Therefore, in WMC, the transaction module provides the transaction information (the account number in the single-use credit card number) when central processor 101 successfully authenticates that the cardholder’s biometric information matches the biometric authentication information previously

associated with that transaction information (*successfully authenticated as being associated with the transaction information by the authentication module*).

EX1007, 11:49-54; EX1004, 12:18-23.

[2] The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

247. WMC renders [2] obvious.

248. In WMC, Walker's biometric interface 105 is the biometric reading device. *Supra*, [1.4]. Walker explains that "the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." EX1007, 5:58-61. Because biometric interface 105 receives the cardholder's fingerprint as the biometric record input to device 100, a POSITA would have understood that biometric interface 105 is a fingerprint reading device. EX1007, 5:58-61.

249. Maes corroborates Walker's approach. Maes explains that "a biometric sensor 40 of any known type may be used in lieu of, or in conjunction with the microphone, to collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data, handwriting data, a retinal vascular pattern data or a combination thereof." EX1004, 10:66-11:5. Because Maes's biometric sensor 40 collects fingerprint data, a POSITA would have recognized that sensor 40 is a fingerprint reading device. EX1004, 10:66-11:5. *Supra*, Ground 1A at [2].

250. Therefore, in WMC, the biometric reading device is a fingerprint reading device. EX1007, 5:58-61; EX1004, 10:66-11:5.

[3] The mobile device of claim 1, wherein the transaction information is generated based at least in part on credit card information.

251. WMC renders [3] obvious.

252. The single-use credit card numbers incorporate the cardholder's credit card account number, which is WMC's transaction information. EX1007, 11:21-25, 11:32-36. *Supra*, [1.3.1]. Walker explains that "the credit card company would decide upon the size of the nonce (N bits), the account number (A bits), and the size of the IV (m bits) so that $n+a+m=r$," and that "[t]he account number would include those bits assigned by the central authority." EX1007, 11:32-36. A POSITA would have understood that a cardholder's credit card account number is credit card information.

253. Therefore, in WMC, the transaction information is generated based at least in part on credit card information. EX1007, 11:32-36.

[5] The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

254. *Supra*, Ground 1A at [5].

[6] The mobile device of claim 5, wherein the security block is a cryptographic block.

255. *Supra*, Ground 1A at [6].

[8] The mobile device of claim 1, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

256. WMC renders [8] obvious.

257. WMC's transaction module provides the single-use credit card number's account number (transaction information) via the short range RF circuitry for use in the transaction. *Supra*, [1.6.1].

258. In WMC, neither the transaction module nor any other component of the mobile device transmits the biometric information for use in a transaction. Walker explains that “[t]he device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004).” EX1007, 11:49-52. Because device 100 determines whether the identifier the cardholder enters is valid *for the device*, a POSITA would have understood and found obvious that the biometric data entered at step 1001 is evaluated within device 100 and is not output from device 100. EX1007, 11:47-52. *Supra*, [1.5]; *supra*, Ground 1A at [8].

[9.pre] A mobile device, comprising:

259. *Supra*, Ground 2A at [1.pre].

[9.1] Radio Frequency (RF) cellular circuitry;

260. *Supra*, Ground 2A at [1.1].

[9.2] short range RF circuitry;

261. *Supra*, Ground 2A at [1.2].

[9.3.1] memory configured to store biometric authentication information and transaction information,

262. *Supra*, Ground 2A at [1.3.1].

[9.3.2] wherein the biometric authentication information has been previously associated with the transaction information;

263. *Supra*, Ground 2A at [1.3.2].

[9.4] a biometric reading device configured to read biometric information;

264. *Supra*, Ground 2A at [1.4].

[9.5] an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory;

265. *Supra*, Ground 2A at [1.5].

[9.6.1] a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction

266. *Supra*, Ground 2A at [1.6.1].

[9.6.2] when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module; and

267. *Supra*, Ground 2A at [1.6.2].

[9.7] a security block configured to secure the transaction information before it is provided by the transaction module.

268. *Supra*, Ground 2A at [5].

[10] The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

269. *Supra*, Ground 2A at [2].

[11] The mobile device of claim 9, wherein the transaction information is generated based at least in part on credit card information.

270. *Supra*, Ground 2A at [3].

[13] The mobile device of claim 9, wherein the security block is a cryptographic block.

271. *Supra*, Ground 2A at [6].

[15] The mobile device of claim 9, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

272. *Supra*, Ground 2A at [8].

[16.pre] A cellular telephone, comprising:

273. WMC renders [16.pre] obvious.

274. Maes explains that “the functions and components of the PDA device 10 may be built into a cellular phone, whereby communication with the central server 60 may be achieved through a cellular communication channel, which may be analog or digital (e.g., CDMA, GSM, etc.).” EX1004, 14:12-16. *Supra*, Ground 1A at [16.pre].

275. In WMC, Walker's device 100 is implemented as a PDA built according to Maes's teachings. *Supra*, [1.pre]. Because Maes describes the functions and components of PDA device 10 being built into a cellular phone, a POSITA would have understood that such a device 100 is a cellular telephone. EX1004, 14:12-16. *Supra*, [1.1].

[16.1] Radio Frequency (RF) cellular circuitry;

276. *Supra*, Ground 2A at [1.1].

[16.2] short range RF circuitry;

277. *Supra*, Ground 2A at [1.2].

[16.3.1] memory configured to store biometric authentication information and transaction information,

278. *Supra*, Ground 2A at [1.3.1].

[16.3.2] wherein the biometric authentication information has been previously associated with the transaction information;

279. *Supra*, Ground 2A at [1.3.2].

[16.4] a biometric reading device configured to read biometric information;

280. *Supra*, Ground 2A at [1.4].

[16.5] an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and

281. *Supra*, Ground 2A at [1.5].

[16.6.1] a transaction module configured to provide the transaction information for use in a transaction

282. *Supra*, Ground 2A at [1.6.1].

[16.6.2] when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module.

283. *Supra*, Ground 2A at [1.6.2].

[17] The cellular telephone of claim 16, wherein the biometric reading device is a fingerprint reading device.

284. *Supra*, Ground 2A at [2].

[18] The cellular telephone of claim 17, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

285. *Supra*, Ground 2A at [5].

[19] The cellular telephone of claim 18, wherein the security block is a cryptographic block.

286. *Supra*, Ground 2A at [6].

[20] The cellular telephone of claim 16, wherein the transaction information is generated based at least in part on credit card information.

287. *Supra*, Ground 2A at [3].

[23] The cellular phone of claim 16, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

288. *Supra*, Ground 2A at [8].

and 21

E. Ground 2B: Walker-Maes-Dorf Renders Obvious Claims 4, 12,

[4] The mobile device of claim 1, wherein the transaction information is generated based at least in part on rewards card information.

289. WMDC renders [4] obvious for reasons analogous to Ground 1B, at [4]. In WMDC, the single-use card numbers are associated with a loyalty program for a rewards card, and the single-use card number is thus generated based at least in part on rewards card information. EX1009, 9:25-10:6, 12:22-27, 20:60-64.

[12] The mobile device of claim 9, wherein the transaction information is generated based at least in part on rewards card information.

290. *Supra*, Ground 2B at [4].

[21] The cellular telephone of claim 16, wherein the transaction information is generated based at least in part on rewards card information.

291. *Supra*, Ground 2B at [4].

and 22

F. Ground 2C: Walker-Maes-Shults Renders Obvious Claims 7, 14,

[7] The mobile device of claim 1, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

292. WMSC renders [7] obvious for reasons analogous to Ground 1C, at [7]. EX1008, [0030].

[14] The mobile device of claim 9, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

293. *Supra*, Ground 2C at [7].

[22] The cellular telephone of claim 16, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

294. *Supra*, Ground 2C at [7].

IX. CONCLUSION

295. For all the reasons I have noted in the foregoing paragraphs, claims 1-23 of the '807 Patent are obvious in view of the references discussed above.

296. I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

APPENDIX A



Seth James Nielson's Vita

(512) 387-4310

seth@crimsonvista.com

July 2026

Academic Degrees

2009 **Ph.D. Computer Science**, Rice University, Houston, TX
2004 **M.S. Computer Science**, Brigham Young University, Provo, UT
2000 **B.S. Computer Science**, Brigham Young University, Provo, UT

Certifications

CISSP
GCFE

CEO and Founder of Crimson Vista, Inc.: Directing global cybersecurity strategy, industry technical partnerships, and the scaling and operations of forensic and engineering operations.

Summary of Expertise and Experience

100+ Forensic and Incident Response Engagements: Leading specialized teams in reconstructing cyber intrusions, investigating trade secret misappropriation, and analyzing complex data artifacts on behalf of, for example, Fortune-50 organizations.

25+ years of professional experience: Working in industry as a subject-matter expert in software engineering, cybersecurity, and computer networks with breadth and depth in architectures, programming languages, protocols, cryptography, and evaluation.

12 Years of Academic Leadership and Research: Currently serving as Adjunct Associate Professor at the University of Texas at Austin; formerly Director of Advanced Research Projects and Research Scientist at Johns Hopkins University Information Security Institute.

10 Years as a Qualified Testifying Expert: Recognized expert in technical matters of patent infringement, validity, copyright, DMCA, industry standards, digital forensics and cybersecurity incidents.

Summary of Core Competencies

Strategic Leadership & Governance	Cybersecurity	Software Engineering	Computer Networks
CEO operations including strategy, partnerships, and training	Security design, analysis, and test including areas of cryptography, IOT, networks, malware, privacy, and others	Engineering of tools, products, and services in secure communications, software test, SDK, distributed file systems and more	Network protocols analysis, traffic analysis and packet capture for wired and wireless networks
Cybersecurity and compliance thought	Forensics and incident response across areas	Evaluation of root-cause-of-failure,	Email and social media security analysis,

leadership, business strategy, and planning for start-ups to boards	of cryptocurrency, digital devices, and source code	reasonable estimates, SDLC, code quality, and testing	threat analysis, and defenses
Training and program design for executives, teams, practitioners, and lawyers	Audit & Compliance for HIPAA, SOC-2, CMMC Level 2, and others	Source code reviews, evaluation, and analysis in C, C++, Python, Java, Go, Ruby, RTL/VHDL/Verilog, JavaScript, etc	Distributed ledger, cryptocurrency, and smart-contract test, design, and analysis

Current Appointments

CEO

Crimson Vista, Inc.

Adjunct Assistant Professor

University of Texas at Austin

Professional Service

International Cryptographic Module Conference, 2018-2026 Program Committee

Professional Advising

2019-2024

Advisory Board

Syccure, Inc.

Non-profit and Community Engagement

2026-

Member

FBI's Infragard

2025

Corporate Contribution

The Digital Harbor Foundation

2021-2025

Founding Director

The Crypto Done Right Foundation

2019-2021

Cyberlab Advisory Board

The SEED School of Maryland

Grants and Research Awards

Decentralizing Zero-Trust Infrastructure to Combat Advanced Persistent Threats and Malicious Insiders (Senior Personnel), NSF 2020 SBIR solicitation. Award number 2051989, Curuvar LLC.

Mitigation of Ransomware, DoD 2018.B STTR solicitation (Army), Topic: A18B-T010, Crimson Vista, \$150,000 (2019)

An Enabling Repository of Cryptographic Knowledge (Co-PI), Cisco Grant, Johns Hopkins University Information Security Institute, \$150,000 (2017-2021)

Patents

Distributed Authentication Between Network Nodes. U.S. Patent 11,032,252, filed January 2, 2019 and issued June 8, 2021. (*Co-inventor*)

Systems and methods for security data in motion. U.S. Patent 8,745,372, filed November 24, 2010 and issued June 3, 2014. (*Co-inventor*)

Systems and methods for security data in motion. U.S. Patent 8,745,379, filed August 20, 2012 and issued June 3, 2014. (*Co-inventor*)

Systems and methods for security data. U.S. Patent 8,677,14, filed January 27, 2012 and

issued March 18, 2014 (Co-inventor)

Academic Awards

Brown Fellowship

John and Eileen Tietze Fellowship

University Research Funding

Sel4 Security Appliance Capstone, funded by Crimson Vista to Brigham Young University Department of Computer Science. 2021

Publications

Books

Cyberfiduciary, Navigating SEC Mandates for Cybersecurity. Cristina Dolan, Seth James Nielson (July 2026).

Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner. Seth James Nielson (December 2023).

Practical Cryptography in Python, Learning Correct Cryptography by Example. Seth James Nielson, Christopher K. Monson (October 2019).

Refereed Publications

Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices. Joseph Kosturko, Eric Schlieber, Sean Futch, Seth James Nielson, In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security* (September 2018).

Potential Forensic Analysis of IoT Data: An Overview of Amazon Echo, Z-wave, and Home Router Data Extraction and Analysis. Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy Leschke, In *Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, UK, pp. 705-710 (June 2017).

PLAYGROUND: Preparing Students for the Cyber Battleground. Seth James Nielson, *Computer Science Education*, volume 26, issue 4, pp. 255-276 (January 2017).

Design Dysphasia and the Design Patterns Maintenance Cycle. Seth James Nielson and Charles D. Knutson, *Information & Software Technology*, volume 48, number 8, pp. 660- 675 (August 2006).

A Taxonomy of Rational Attacks. Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, In *Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, New York (February 2005).

OO++: Exploring the Multiparadigm Shift. Seth J. Nielson and Charles D. Knutson. *Proceedings of the Workshop on Multiparadigm Programming with Object-Oriented Languages (MPOOL 2004)*, Oslo, Norway (June 2004).

Effective Bandwidth for Traffic Engineering. Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, TX, (May 2001)

Testimony Before Government Bodies

Testimony in support of Maryland SB 151/HB 211 Criminal Law - Crimes Involving Computers – Ransomware. Testimony given to the Judicial Proceedings Committee of the Maryland Senate and the Judiciary Committee of the Maryland House of Delegates (January/February 2019)

Invited Talks, Panels, and Technical Training

Strategies for CC Compliance for Systems with LLMs. Seth James Nielson, Presented in the International Common Criteria Conference 2026 (ICCC 2026), Rome Italy (October 2026)

Cyber Risk & Resilience – Conversations with Industry Leaders. Seth James Nielson, Panel Moderator, Columbia University Technology Management Program, SPS (November 2025).

Psychology & Incentives: How Social Engineering Exploits Privacy & Behavior. Seth James Nielson and Maria Jose Castro Landaeta, RSAC 365 Webinar (January 2024).

Data Security: Four Approaches to a Better Defensive Posture. Seth James Nielson, 2023 Enterprise Data World, Anaheim, CA (September 2023).

Securing Your Data Assets Against Hackers. Seth James Nielson, 2021 Enterprise Data World, Boston, MA. (April 2021).

The Cybersecurity of IP. Seth James Nielson, 2020 Essential Cybersecurity Law, Austin, TX (Virtual). (July 2020).

Security and Privacy for Data Architects. Seth James Nielson, 2019 Data Architecture Summit, Chicago, IL (October 2019).

Crypto Done Right, One Year In. Lessons Learned and Next Steps. Seth James Nielson. Presented in the International Cryptographic Knowledge Base 2019 (ICMC 2019), Vancouver, Canada (May 2019).

Hardening US Unmanned Systems Against Enemy Counter Measures. Panel Discussion. Accepted invitation to 7th Annual DoD Unmanned Systems Summit, Alexandria, VA (April 2019).

A Gentle Introduction to Blockchain. Seth James Nielson. 2019 Enterprise Data World, Boston, MA (March 2019).

A Gentle Introduction to Blockchain. Seth James Nielson, 2018 Data Architecture Summit, Chicago, IL (October 2018).

Detecting Malicious Sandboxes. Seth James Nielson. Workshop on Defensive Deception and Trust in Autonomy, San Diego, CA (August 2018).

Towards a Crowd-Sourced Cryptographic Knowledge Base. Seth James Nielson and Debra Baker, Presented in the International Cryptographic Knowledge Base 2018 (ICMC18), Ottawa, Canada (May 2018).

The PyPy Sandbox. Seth James Nielson. Presented in the National Centers of Academic Excellence Tech Talk, Online (March 2018).

Theses

Designing Incentives for Peer-to-Peer Systems. *PhD Thesis.* (defended 10/2009)

OO++ Design Patterns, GOF Revisited. *Master's Thesis.* (defended 8/2004)

Technical Reports

ChatGPT WANTS To Break Rules. Seth James Nielson, Saige V. Nielson, and Jade Ashford., Crimson Vista Technical Report, CVTR-2025-001 (October 2025)

The BitTorrent Anonymity Marketplace. Seth James Nielson and Dan S. Wallach, arXiv Technical Report 1108.2718, (August 2011)

Building Better Incentives for Robustness in BitTorrent. Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, arXiv Technical Report 1108.2716, (August 2011)

Attacks on Local Searching Tools, Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011).

White Papers and Trade Publications

Techniques for Discovering Unauthorized Copying in Software. Seth James Nielson, Crimson Vista White Paper, (January 2022).

Evaluation of the MarkMonitor AntiPiracy System. Aviel D. Rubin, Seth J. Nielson, Christopher K. Monson, , Produced for the Center for Copyright Information (December 2013).

Guidelines for Source Code Review in Hi-Tech Litigation. Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, Harbor Labs White Paper (September 2013).

Undergraduate Advising

Independent Research and Capstones (University of Texas Austin)

Adversarial Robustness in Large Language Model Development: A Research Synthesis and Policy Recommendation, Malavika Subramaniam, CS 370, Independent Study (Spring 2026)

Replicating Graph Neural Network-Based Vulnerability Detection: Study Using Code Property Graphs, Seohyeon Lee, CS 370, Independent Study (Spring 2026)

Benchmarks Lie: Empirical Quantification of the Synthetic-to-Real Vulnerability Detection Gap in Code LLMs, Ari Sharma, CS 370, Independent Study (Spring 2026)

A Reproduction of Alpha Beta Crown Results with Cutting Plane Optimizations, Kyler Larsen, CS 370, Independent Study (Spring 2026)

A Comparative Benchmarking Study of AES Modes on CPU and GPU Architectures, Alexis Lance, CS 370, Independent Study (Spring 2026)

Automated Partitioning of Software During Compilation, Charlotte White, CS 370, Independent Study (Summer 2024).

Automated Patching of Unsafe C Functions, Nishaanth Saaketh Joopelli, CS 370, Independent Study (Summer 2024).

Analysis of Image Provenance Techniques, Tanuj Tekkale, CS 370, Independent Study (Summer 2024).

Individual Voice Recognition using Machine Learning. Andrew Dang, CS 370, Independent Study (Summer 2023).

Malware Classification with SVM. Monique Tran. CS 370, Independent Study (Summer 2023).

SMART CONTRACTS: Different approaches to introduce external (off-chain) data.

Gonzalo Tamariz-Martel Sánchez (June 2022).

Graduate Advising

Capstones for Masters of Science in Security Informatics (Johns Hopkins)

Research on defense next-generation malware on the Windows platform. Weizhou Wang, Runjie Zhang (December 2018).

Open Source HSM Side Channel Analysis. Yu-Tsern Jou, Ying Liu, Menghan Bai (December 2018).

Side Channel Attack on HSM Based on Machine Learning. Bowen Shi, Hong Ma, Mengqi Qin (December 2018).

An Exploration of the Usability of HTTPS. Dylan Richmond, Matthew Shonman, Jingcheng Yang (December 2018).

Using Selective RAM Journaling to Fight Ransomware. Steven Cheng, Venkata Aditya Bollapragada, and Antara Sargam (December 2018).

Fault Tolerance System for IoT. Yongqiang Fan, Haiwen Sun, (December 2018).

IoT Discovery. Weike Chen, Harry Luo, Prashanth Venkateswaran (August 2018).

Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices. Joseph “Jay” Kosturko, Eric Schlieber, Sean Futch (May 2018).

Anti-Honeypot Detection in Advanced Botnet Attacks. Chao Lei, Wenjun Li (December 2017).

Securing ADS-B Based Airborne Collision Avoidance Systems. Ritvik Sachdev, Purushottam Kulkarni, Praveen Malhan (December 2017).

Security-Testing-Orientated Internet of Things(IoT) Simulator. Ningyuan Bao, Mengying Hu (December 2017).

AIS Data De-anonymization. Zehuan Li, Shanshan Yang, Liangjia Fu (December 2017).

Forensic Data Collection from IoT Devices. Chanyang Shin, Prerit Chandok, Aurin Chakravarty (December 2017).

Replication of CryptoDrop. Kevin Manzotti, Kashif Memon, Rahul Durgad (December 2016).

Detecting XSS attacks using BRO IDS. Harshneel More, Jingmiao Wang, Yuanqi Zhu (December 2016).

Feasibility, Security and Privacy Analysis of EMVCo Payment Tokenization Technology for Identity Enabled Transactions. Asmaa Aljohani, Gyan Namdhari, Yue Zhu (December 2016).

The Emperor Has No Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter. Richard Eaton (May 2015).

Investigating the Heartbleed Vulnerability. Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu (2015).

Security Techniques for Developing iOS Applications. Kartik Thapar (February 2015).

De-anonymizing BitCoin. Jie Feng, Jianxiang Peng, Likai Zhang (January 2014).

In the News

“Johns Hopkins Researchers and OnBoard Security Team Up to Protect Drones,”
Robotics Tomorrow, 3/16/2018

“Rice University Computer Scientists Find a Flaw in Google's New Desktop Search Program.” *New York Times*, 12/20/2004

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-2025)

Network Security and Privacy (2020-2021)

Johns Hopkins University

Advanced Network Security (2017 - 2019)

Network Security (2014 – 2019)

Rice University

Data Structures and Algorithms (Spring 2008)

Selected Projects

Machine Learning and AI

- Designed Empirical Validation Inspection for LLM (DEVILLM) Initiative (Crimson Vista, 2026-)
- AI/ML detection of software vulnerabilities (University of Texas at Austin, 2026)
- ChatGPT LLM exploitation analysis and evaluation (Crimson Vista, 2025)
- AI Agent Analysis/Engineering (Crimson Vista, 2025-)
- AI Governance (Crimson Vista, 2024-)
- LLM red team testing (Crimson Vista, 2024-)
- Investigation of use of unauthorized data in AI training (Crimson Vista, 2024)

Software Research and Development

- Insider-resistant Storage Service. Prototype complete. (2025-2026)

Forensic Analysis (e.g., Code/IP Theft)

- Analysis of email artifacts to support provenance (Crimson Vista, 2026-)
- Analysis of web site contents over time (Crimson Vista, 2026-)
- Reverse engineering of software (1990's MS-DOS architecture) (Crimson Vista, 2026-)
- Forensic examination of exfiltrated data via fraudulent API access (Crimson Vista, 2025-)
- Neutral party forensic data collection: windows, macs, iphones, cloud (Crimson Vista, 2025-2026)
- Forensic investigation of potential CTO/CIO theft/destruction (Crimson Vista, 2025-2026)
- Trusted images research (UT Austin, 2024)
- Investigation of email transmissions, reception (Crimson Vista, 2024-2025)
- Investigation of stolen digital documents, provenance, handling (Crimson Vista, 2023-2025)
- Investigation of cryptocurrency transfers and fraud (Crimson Vista, 2023-)
- Investigation of website content development and provenance (Crimson Vista, 2023-2024)
- Investigation of server, laptop, and hard drives for indica of tampering (Crimson Vista, 2023)
- Investigation of voting machine software for vulnerabilities (Crimson Vista, 2022-2025)
- Investigation of altered/forged emails (Crimson Vista, 2022)

- CLE training related to source code analysis/trade secrets (Source Code Discovery, 2021)
- Investigation of IP/code theft related to MTA, spear-phishing, and email (Crimson Vista, 2019-2021)
- Investigation of code theft related to housing and rental software (Crimson Vista, 2019-2022)
- Investigation of code development for security vulnerabilities/intrusion (Crimson Vista, 2020)
- Investigation of code theft related to digital mobile radios (Crimson Vista, 2017-2021)
- Investigation of code theft related to financial trading software (Crimson Vista, 2016-2017)
- Investigation of code theft related to e-commerce (Harbor Labs, 2015)
- Investigation of IP theft related to domain anti-abuse (Harbor Labs, 2015)
- Investigation of IP theft related to high-frequency trading (Harbor Labs, 2010-2011)

Intrusion and Incident Response

- Akira Ransomware light-weight scanning tools and services (Crimson Vista, 2026-)
- Akira Ransomware response and recovery (Crimson Vista, 2025-)
- Post-incident response handling within VCISO framework (Crimson Vista, 2023-)
- Post-incident impact analysis for major bank (Crimson Vista, 2020-2021)
- Post-incident recovery management on behalf of insurance provider (Crimson Vista, 2019)

Applied Cryptography

- Analysis of ransomware intrusion cryptographic artifacts (Crimson Vista, 2024-)
- Multi-party key sharing and secrets (Crimson Vista, 2024-)
- Cryptography training modules (UT Austin, 2022-2025)
- Analysis of compromised password hashes (Crimson Vista, 2020)
- “Crypto Done Right”, Cryptographic Knowledge Base Non Profit (2020-2024)
- “Crypto Done Right”, Cryptographic Knowledge Base with Cisco (Johns Hopkins, 2017-2020)
- Simulated implementation of Vehicle-to-Vehicle authentication (Crimson Vista, 2018-2019)
- Cryptographic protocol analysis and design for Syccure, Inc. (Crimson Vista, 2017-2023)
- Timing attacks on Hardware Security Modules with Diamond Key Security (Johns Hopkins, 2018)
- Technical consulting for U.S. Dpt. of Justice (Antitrust Division, Transportation, Energy & Agriculture) (Crimson Vista, 2018)
- Aircraft/drone anti-collision protocol security with OnBoard Security (Johns Hopkins, 2017)
- Cryptographic communication library for Security First Corp (ISE, 2010-2011)
- Encryption library, file system encryption, GPU for Security First Corp (ISE, 2005-2011)

Security Operations, Compliance, Oversight

- CMMC compliance consulting (Crimson Vista, 2025-)
- Security operations for MSPs (Crimson Vista, 2025-)
- MDM management and endpoint security (Crimson Vista, 2025-)
- Ransomware Defensive Operations (Crimson Vista, 2025-)
- BYOD security, Identity and Access Management, oversight (Crimson Vista, 2025-)
- Security and compliance audit of medical offices (Crimson Vista, 2025-)
- Identity and Access Management (Crimson Vista, 2025-)
- Terrorism analysis of social media and public data (Crimson Vista, 2025)
- Corporate board advisory (Crimson Vista, 2025-)

- Risk Assessment (Crimson Vista, 2024-)
- Penetration Testing (Crimson Vista, 2024-)
- AI Governance (Crimson Vista, 2024-)
- SEC cybersecurity disclosures (Crimson Vista, 2024-)
- GDPR, Privacy, PII analysis (Crimson Vista, 2024-)
- Security analysis of Twitter cybersecurity operations/practices (Crimson Vista, 2022)
- Virtual Chief Information Security Officer for IperionX (Crimson Vista, 2022-2023)

IoT Devices and IoT Security

- Wireless communications, black box analysis, reverse engineering (Crimson Vista, 2025-)
- Medical implant analysis (Crimson Vista, 2024-2025)
- Robotic automation system (Crimson Vista, 2024-2025)
- Traffic lights and systems software analysis (Crimson Vista, 2023-2024)
- Vulnerability and exploitation analysis of voting machine hardware (Crimson Vista, 2023-2025)
- High-security appliance based on formal methods (Crimson Vista, BYU, 2021)
- Hadoop security research (Crimson Vista, 2021-2022)
- IoT data sensors for agricultural operations (Crimson Vista, 2020-2023)
- Contributor, reviewer for the Institute of Assured Autonomy (Johns Hopkins, 2019)
- IoT data aggregation security with Armored Things (Johns Hopkins, 2018-2019)
- Automated IoT device profiling with the Physics Lab (Johns Hopkins, 2018)
- Physical forensics from IoT devices (Johns Hopkins 2017)

Network Security

- Ransomware Detection, Testing and Simulation (Crimson Vista, 2025-)
- MPLS/VRF analysis (Crimson Vista, 2025-)
- Bluetooth-enabled alert system security analysis (Crimson Vista, 2024)
- Web security, cookies, XSS, XSRF training modules (UT Austin, 2023-2024)
- Phishing samples analysis (Crimson Vista, 2022-2023)
- WiFi transmission analysis, packet capture (Crimson Vista, 2023-2024)
- Security-Focused Data Discovery Methods and Practice (Crimson Vista, 2022-2023)
- Analysis of weaknesses in two-factor authentication (Crimson Vista, 2022-2023)
- Analysis of bots on Twitter in terms of prevalence, stealth, and impact (Crimson Vista, 2022)
- Secure distributed computing (Curuvar, 2021-2023)
- Hadoop deployment and security considerations (Crimson Vista, 2021-2022)
- SSO technology evaluation and test (UT Austin, Crimson Vista, 2021-2022)
- Information risk assessment with respect to data breach (Crimson Vista, 2020-2021)
- Data breach analysis with respect to password authentication (Crimson Vista, 2020-2021)
- Network security curriculum design for Law and Policy (University of Texas at Austin, 2020-2024)
- Network security curriculum design for undergraduates (University of Texas at Austin, 2020-2021)
- Network security curriculum design (Johns Hopkins, 2013-2019)
- Security analysis of financial services vendor for Fortune-100 client (Crimson Vista, 2018-2019)
- Analysis of secure e-mail transmission for confidential client (Crimson Vista, 2018-2019)
- Cloud storage system security evaluation for confidential client (Harbor Labs, 2015)
- Secure gateway security and compliance evaluation for SecurityFirst Corp (Harbor Labs, 2015)

- Gateway caching security/privacy engineering (Google, 2005)

Malware and Viruses

- Ransomware training modules (UT Austin, 2022-2023)
- Ransomware recovery research and development (Crimson Vista, 2018-2019)
- Advanced malware and malware defenses analysis (Johns Hopkins, 2018)
- Malware Analysis for Confidential Client (Crimson Vista, 2016)

Privacy

- Investigation of biometric tracking in commercial systems (Crimson Vista, 2024-2025)
- Investigation of location tracking in mobile devices (Crimson Vista, 2021-2025)
- Investigation of biometric tracking/transmission in devices and systems (Crimson Vista, 2021-2022)
- Development of an auditing tool for cookies and other web tracking (Crimson Vista, 2020, 2024)
- Audit of a large hospital network for cookies and web tracking (Confidential client, 2020)
- Development of a privacy curriculum for data architects (Crimson Vista, 2019)
- Anonymization of threat indicators with the Applied Physics Lab (Johns Hopkins, 2017)
- Analysis of anti-piracy vendor for Center for Copyright Information (Harbor Labs, 2013-2014)

Miscellaneous Security Technologies

- Distributed ledger technology for secure state replication (Curuvar, 2021-2023)
- Blockchain technology for sale and/or licensing of intellectual property (Crimson Vista, 2021-2022)
- Blockchain technology analysis for a start-up (Crimson Vista, 2019-2020)
- Analysis of cyber security norms for a confidential Fortune 100 client (Crimson Vista, 2018-2019)
- Analysis of vulnerabilities in portable chemical manufacturing system (Johns Hopkins, 2018)
- Open-Source Contribution and Sponsorship for The PyPy Project (Crimson Vista, 2018-2019)
- Blockchain and smart contract design for confidential start-up (Crimson Vista, 2018)
- Medical device system security evaluation for confidential client (Harbor Labs, 2015)

Software Engineering and Software Analysis

- Arduino microprocessor software for controlling hardware (Crimson Vista, 2025)
- Legacy software patching for modern applications (Crimson Vista, 2025)
- WiFi OS/Firmware analysis of MAC randomization, etc (Crimson Vista, 2024-2025)
- WiFi VHDL/Verilog analysis of Cyclic Shift, etc (Crimson Vista, 2024-2025)
- Automotive source code analysis (Crimson Vista, 2024-)
- Medical implant source code analysis (Crimson Vista, 2024-2025)
- WiFi VHDL/Verilog analysis of AX features (Crimson Vista, 2024)
- Automated least-privilege compilation/language research (UT Austin 2024-2025)
- Review of failed software project, root cause analysis, attribution (Crimson Vista, 2024-2025)
- Review of development practices, error handling, and robustness (Crimson Vista, 2023-2024)
- Open-source licensing analysis, build, and test (Crimson Vista, 2023-)
- GitHub analysis and statistics for effort estimation (Crimson Vista, 2022)
- Software theft analysis and tool design for various clients (Crimson Vista, 2018-)

- Cyber insurance investigations for Clyde & Co (Crimson Vista, 2018-2019)
- Distributed code coverage analysis tool for a confidential Fortune 100 client (ISE, 2011)
- Software engineering for Metrowerks Inc. (2001-2003, formerly Lineo Inc.)
- Code Languages: C, C++, Java, Python, Ruby, Scala, RTL/VHDL/Verilog, JavaScript, Go

Employment History (Last Title Only)

CEO, Crimson Vista, Inc. (2016-).

Adjunct Assistant Professor, University of Texas at Austin (2020-).

Founder and Partner, Source Code Discovery, LLC. (2019-2021).

Director of Advanced Research Projects, Johns Hopkins University (2016-2019).

Adjunct Associate Research Scientist, Johns Hopkins University (2014-2019).

Principal, Harbor Labs, LLC. (2011-2015).

Senior Security Analyst, Independent Security Evaluators (2005-2011).

Summer Intern, Google Inc. (2005).

Software Engineer II, Metrowerks (2001-2003).

Expert Testimony

On behalf of Apple Inc in Cardware Inc. v Apple Inc. (1:25-cv-00446-ADA)

Counsel: DLA Piper, LLP
 Venue: Western District of Texas, Austin Division
 Subject Matter: Payment tokenization technology
 Reports: 1 report March 2026, 1 report April 2026
 Deposition: 1 deposition June 2026

On behalf of LCAO Tech in LCAO Tech v Quimbik (CGC-24-615393)

Counsel: Kronenberger Rosenfeld, LLP
 Venue: Superior Court of the State of California, County of San Francisco, Unlimited Civil
 Subject Matter: Software engineering sufficiency, industry norms and customs, performance evaluation
 Deposition: 1 deposition April 2026
 Trial: May 2026

In support of Unified's Request for Ex Parte Reexamination of 9,871,693

Counsel: Unified Patents
 Venue: PTAB
 Subject Matter: Remote service management, abnormal event processing
 Reports: 1 declaration, May 2026

On behalf of Fortinet in Netskope v. Fortinet (3:22-CV-01852-TLT)

Counsel: Quinn Emanuel
 Venue: Northern District of California, San Francisco Division
 Subject Matter: Cloud-based security, proxies, threat detection
 Reports: 1 report January 2026, 1 report February 2026
 Deposition: 1 deposition March 2026

On behalf of Samsung in OS-New Horizon Personal Computing Solutions v Samsung (5:24-CV-00634-JRG-RSP)

Counsel: Goodwin Proctor
 Venue: Eastern District of Texas, Marshall Division
 Subject Matter: Biometric sensors, hardware security, lifesign detection
 Reports: 1 report February 2026

Deposition: 1 deposition February 2026

In support of Unified's Request for Ex Parte Reexamination of 11,503,105

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security, content delivery networks
Reports: 1 declaration, February 2026

On behalf of Vizio in Software Freedom Conservancy v Vizio (30-2021-01226723-CU-BC-CJC)

Counsel: Quinn Emanuel
Venue: Superior Court of the State of California, County of Orange
Subject Matter: Open source use in industry, nature and contents of artifacts, build issues
Deposition: 1 deposition December 2025

On behalf of Nielsen Consumer Inc in Nielsen Holdings Limited v Nielsen Consumer Inc. (2025-0651-NAC)

Counsel: Ropes and Gray
Venue: Court of Chancery of the State of Delaware
Subject Matter: Cybersecurity issues in data sharing agreement
Reports: 1 report July 2025
Deposition: 1 deposition July 2025
Trial: July 2025

On behalf of Samsung in Secure Wifi v Samsung (2:24-CV-00047-JRG)

Counsel: Blank Rome
Venue: Eastern District of Texas, Marshall Division
Subject Matter: Source code analysis of Wifi modules
Reports: 1 report July 2025
Deposition: 1 deposition July 2025

On behalf of Axonics in Alfred E. Mann Foundation for Scientific Research v Axonics

Counsel: Tensegrity
Venue: JAMS Arbitration
Subject Matter: Software completeness, correctness, comparison
Reports: 1 report April 2025, 1 report May 2025, 1 report June 2025
Deposition: 1 deposition June 2025, 1 deposition November 2025

In support of Unified's Request for Ex Parte Reexamination of 8,782,283

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, May 2024

On behalf of OANN in Dominion v. OANN

Counsel: Jackson Walker
Venue: United States District Court for the District of Columbia
Subject Matter: Electronic Voting Security
Reports: 3 reports, December 2024, January and March 2025
Deposition: 1 deposition April 2025

On behalf of USAA in PacID v. USAA

Counsel: Fish and Richardson
Venue: ITC

Subject Matter: Secure communication protocols
Reports: 6 reports, March 2025

On behalf of the State of Texas in State of Texas v. Google

Counsel: Norton Rose Fulbright
Venue: District Court of Victoria County Texas
Subject Matter: Biometric Data Storage
Reports: 1 report, February 2025

In support of Unified's Request for Ex Parte Reexamination of 7,249,262

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, February 2024

On behalf of Proofpoint in Proofpoint Inc. v. Abnormal Security

Counsel: McDermott Will & Emery, LLP
Venue: Case No. CGC-21-597059 (Superior Court of California, County of San Francisco)
Subject Matter: Email Machine Learning
Reports: 1 report submitted October 2024
Deposition: 1 deposition October 2024

On behalf of LG Electronics in TOT Power Control v LG Electronics; C.A No. 21-1304-MN

Counsel: DLA Piper
Venue: District of Delaware
Subject Matter: Outer loop power control, source code
Reports: 1 report September 2024
Deposition: 1 deposition November 2024

On behalf of Dexcom in Dexcom v Abbott Diabetes Care; C.A. No. 22-605-KAJ

Counsel: Quinn Emanuel
Venue: District of Delaware
Subject Matter: Glucose alerts source code
Reports: 1 report September 2024

On behalf of Axonics in In the Matter of Certain Video Processing Devices and Components Thereof; Investigation No. 337-TA-1396

Counsel: Tensegrity
Venue: ITC
Subject Matter: Medical implant wireless transmission source code
Reports: 2 reports September 2024
Deposition: 1 deposition October 2024
Trial: December 2024

On behalf of Apple in Carbyne v. Apple; Civil Action No. 1:23-cv-00324

Counsel: Ropes and Gray
Venue: West District of Texas, Austin Division
Subject Matter: Authentication, Secure Storage, Secure Processing, Access
Reports: 1 report August 2024, 1 report September 2024
Deposition: 1 deposition October 2024
Trial: Evidentiary hearing November 2024

In support of Unified's Request for Ex Parte Reexamination of 9,032,038

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, November 2024

In support of Unified's Request for Ex Parte Reexamination of 7,594,009

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, October 2024

On behalf of Commure in Commure v. Canopy Works; Case No. 3:24-cv-02592-AMO

Counsel: Quinn Emanuel
Venue: Northern District of California
Subject Matter: Security norms and customs related to wireless security
Reports: 1 declaration August 2024, 1 report March 2025
Deposition: 1 deposition September 2024

On behalf of Samsara In the Matter of Certain Vehicle Telematics, Fleet Management, and Video-based Safety Systems, Devices, and Components Thereof, Investigation No. 337-TA-1393

Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Automotive tracking, safety, analysis source code
Reports: 1 report August 2024, 1 report September 2024, 1 report November 2024
Deposition: 1 deposition September 2024
Trial: March 2025

In support of Unified's Request for Ex Parte Reexamination of 10,601,780

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, August 2024

On behalf of BOKF in Dynapass v BOKF

Counsel: Fish and Richardson
Venue: Eastern District of Texas, Marshall Division
Subject Matter: Multifactor Authentication, Financial Systems
Reports: 1 report May 2024

On behalf of Samsung in Samsung v Maxell

Counsel: DLA Piper
Venue: PTAB; Eastern District of Texas Texarkana Division
Subject Matter: Biometrics
Reports: 1 declaration April 2024, 1 report December 2024
Deposition: 1 deposition December 2024, 1 deposition February 2025
Trial: May 2025

On behalf of Forescout Technologies in Fortinet v Forescout Technologies

Counsel: Winston & Strawn
Venue: Northern District of California

Subject Matter: Network security architecture and devices
Reports: 1 report March 2024
Deposition: 1 deposition May 2024

On behalf of Threat Modeler Software in Iriusrisk v Threat Modeler Software

Counsel: Rimon
Venue: PTAB
Subject Matter: Threat modeling
Reports: 1 declaration January 2024, 1 declaration February 2024
Deposition: 1 deposition March 2024, 1 deposition April 2024

On behalf of Motorola Solutions in Motorola Solutions v. Hytera Communications

Counsel: Kirkland and Ellis
Venue: Northern District of Illinois, Eastern Division
Subject Matter: Source code forensics
Reports: 1 declaration January 2024
Deposition: 1 deposition February 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 7,586,871

Counsel: Univied Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, February 2024

On behalf of the State of Texas in State of Texas v. Google

Counsel: Norton Rose Fulbright
Venue: District Court of Victoria County Texas
Subject Matter: Location tracking
Reports: 1 report, January 2024
Deposition: 1 deposition May 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 9,264,441

Counsel: Rothwell, Figg, Ernst, and Manbeck
Venue: PTAB
Subject Matter: Network security devices and operations
Reports: 1 declaration, January 2024

On behalf of Dennis Zeedyk in the United States vs. Dennis Zeedyk (2023-Present)

Counsel: Saul Euwing
Venue: Northern District of Indiana South Bend Division
Subject Matter: Website forensics
Reports: 1 report November 2023

On behalf of OpenAI in OpenAI v Open Artificial Intelligence and Guy Ravine (2023-Present)

Counsel: Quinn Emanuel
Venue: Northern District of California
Subject Matter: Forensic investigation of website and related assets
Reports: 3 reports issued October 2023, January 2025, February 2025
Deposition: 1 deposition March 2025

On behalf of Palo Alto Networks in Centripetal Networks v Palo Alto Networks (2021-Present)

Counsel: Norton Rose Fulbright and Ropes & Gray

Venue: Eastern District of Virginia
Subject Matter: Network security devices
Reports: 3 reports issued August 2023, September 2023, and October 2023
2 related declarations for EPR submitted July 2024
Deposition: 1 deposition October 2023
Trial: January 2024

On behalf of Anchor Semiconductor in *Elite v. Anchor* (2022-Present)

Counsel: Venable
Venue: Northern District of California
Subject Matter: Forensic investigation of alleged sabotage and data destruction
Reports: 1 report July 2023

In support of Unified Patents in *Ex Parte Reexamination of U.S. Patent 9,438,614*

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Machine learning and intrusion detection systems
Reports: 1 declaration Apr 2023

On behalf of Trend Micro in *Trend Micro v. TaaSera Licensing* (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 4 declarations Apr 2023

On behalf of Salesforce in *WSOU Investments v. Salesforce* (2022-Present)

Counsel: Quinn Emanuel
Venue: Western District of Texas
Subject Matter: Source code related to transmission of marketing emails
Reports: 1 report March 2023
Deposition: 1 deposition August 2023

On behalf of Trend Micro in *Trend Micro v. Webroot* (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 5 declarations Feb-Mar 2023, 5 declarations September 2023

On behalf of Fox News in *Dominion Voting Systems v. Fox News* (2022-2023)

Counsel: Winston and Strawn
Venue: Superior Court of the State of Delaware
Subject Matter: Voting machine security including forensic investigation
Reports: 1 Report December 2022
Deposition: 1 deposition February 2023

On behalf of Public Storage in *Estch v. Public Storage* (2022-2023)

Counsel: Orrick
Venue: Eastern District of Texas
Subject Matter: VoIP, authentication, authorization
Reports: 1 Report January 2023
Deposition: 1 deposition January 2023

On behalf of Lenovo/Motorola Mobiliy in Maxell Ltd v. Lenovo/Motorola Mobility (2022-2023)

Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Authentication
Reports: 1 Declaration November 2022
2 Reports February 2023
Deposition: 1 deposition March 2023

On behalf of Elon R Musk in Twitter Inc v. Elon R Musk (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Court of Chancery of the State of Delaware
Subject Matter: Evaluation of Security in light of Whistleblower Report
Reports: 1 Report October 2022

On behalf of Bissell, Inc. in Bissell Inc. v. Tineco Intelligent Technology Co. Ltd., (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: ITC
Subject Matter: Forensic evaluation of source code
Reports: 1 Report submitted September 2022
Deposition: 1 deposition November 2022
Trial: December 2022

On behalf of Hakkasan USA in Hakkasan USA v Endurance American Specialty Insurance (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: District of Nevada (Clark County)
Subject Matter: Forensic evaluation of emails
Reports: 1 Report submitted May 2022
Deposition: 1 deposition July 2022

On behalf of JTC in Seimens vs JTC (2021-2022)

Counsel: Peckar and Abramson, PC
Venue: American Arbitration Association
Subject Matter: Software Engineering Efforts
Reports: 1 Report submitted in July 2021
1 Report submitted in September 2021
Deposition: 1 deposition October 2021
Arbitration: March 2022

On behalf of Samsung in Samsung v. Proxense (2021-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Western District of Texas (Waco)
Subject Matter: Authentication, Authorization, Device-to-device
Reports: 1 declaration submitted October 2021
Deposition: 1 deposition October 2022

On behalf of Bitglass in Netskope, Inc. v. Bitglass Inc. (2021-2022)

Counsel: Irell and Manela, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Authentication, Single-Sign-On
Reports: 1 declaration submitted September 2021
1 declaration submitted March 2021

On behalf of The State of Arizona in Arizona v. Google (2021-2022)

Counsel: Ruttenberg IP Law
Venue: Superior Court of the State of Arizona (Maricopa)
Subject Matter: Privacy, Location tracking, Data collection
Reports: 1 declaration submitted August 2021

On behalf of TLC in TLC v. Koninklijke Philips N.V., US Philips Corporation (2019-2021)

Counsel: Perkins Coie LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Cryptographic protocols
Reports: 1 declaration submitted February 2021

On behalf of Magic Micro in Monsoon v. Magic Micro (2020-2021)

Counsel: Gutnicki, LLP
Venue: International Centre for Dispute Resolution
Subject Matter: Blockchain, file storage
Reports: 1 declaration submitted October 2020
1 declaration submitted November 2020
Arbitration: December 2020

On behalf of Juniper in Juniper Networks Inc. v. Huawei Digital Technologies Co. (2020-2021)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Network perimeter defense against malware
Reports: 1 declaration submitted June 2020
1 declaration submitted July 2021
Deposition: 1 deposition April 2021

On behalf of DivX in Netflix v. DivX (2020-2023)

Counsel: Lowenstein & Weatherwax, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Encryption of streaming media
Reports: 1 declaration submitted May 2020
1 declaration submitted December 2020
1 declaration submitted April 2021
Deposition: 1 deposition January 2021, 1 deposition February 2021

On behalf of Juniper in Juniper Networks Inc. v. Implicit LLC (2019-2020)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Packet classification
Reports: 1 declaration submitted February 2020

On behalf of the Dealership class in Dealer Management Systems Antitrust Litigation (2019-Present)

Counsel: Milberg Phillips Grossman LLP
Venue: Case No. 18-cv-00864 (Northern District of Illinois)
Subject Matter: Cybersecurity, risk assessment, third-party access
Reports: 1 report submitted November 2019
Deposition: 1 deposition January 2020

On behalf of Symantec in the Trustees of Columbia University in the City of New York v. Symantec Corporation. (2018-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. Civil Action No. 3:13-cv-00808-JRS (Eastern District of Virginia)
Subject Matter: Deception technologies, Honeypots
Reports: 1 report submitted October 2019
Deposition: 1 deposition January 2020
Trial: April 2022

On behalf of Proofpoint in Proofpoint Inc. v. Vade Secure (2019-2021)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. 3:19-cv-04238 (Northern District of California)
Subject Matter: Cloud-based email, malware detection, AI
Reports: 1 report submitted September 2019, 1 report submitted December 2019
1 report submitted February 2021, 1 report submitted April 2021
Deposition: 1 deposition April 2021
Trial: August 2021

On behalf of Bitdefender in Finjan Inc. v. BitDefender Inc. (2018-2021)

Counsel: Susman Godfrey LLP
Venue: Case No. 4:17-cv-4790-HSG (Northern District of California)
Subject Matter: Web threat detection, malware, gateways
Reports: 1 report submitted July 2019, 1 report submitted August 2019
Deposition: 1 deposition October 2019

On behalf of HTC in Koninklijke Philips N.V., US Philips Corporation v. HTC Corp., HTC America Inc. (2019-2020)

Counsel: Perkins Coie LLP
Venue: Case No. 4:18-cv-01887-HSG (Northern District of California)
Subject Matter: Cryptographic protocols
Reports: 1 report submitted May 2019, 1 report submitted June 2019
Deposition: 1 deposition August 2019

On behalf of Juniper in Juniper Networks Inc. v. Finjan Inc. (2018-2019)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Malware, firewall/gateway, network security
Reports: 4 declarations submitted October 2018
Deposition: 1 deposition June 2019

On behalf of Redbox in Disney Enterprises, Inc., LucasFilm Ltd, LLC, and MVL Film Finance LLC v. Redbox Automated Retail, LLC. (2018)

Counsel: Robins Kaplan LLP
Venue: Case No. 2:17-cv-08655-DDP (AGRx) (Central District of California, Western Division)
Subject Matter: DRM, cloud security, media streaming
Reports: 1 declaration submitted May 2018

On behalf of Trend Micro in Trend Micro, Inc. v. Security Profiling, LLC (2017-2018)

Counsel: The Marbury Law Group, PLLC
Venue: Inter Partes Review Case No. IPR2017-02191 and IPR2017-02192
Subject Matter: Automated security patches
Reports: 2 declarations submitted September 2017
Deposition: 1 deposition June 2018

On behalf of TeleSign in Twilio Inc. v. TeleSign Corporation (2016-2021, multiple cases)

Counsel: Shook, Hardy & Bacon LLP
Venue: Inter Partes Review Case No. IPR2016-01688, IPR2016-00360, IPR2017-01976 IPR2017-01977, IPR2017-01978
Case No. 5:16-cv-6925-LHK (Nor. District of California, San Jose Div.)
Subject Matter: Telecommunications security
Reports: 1 declaration submitted August 2016, May 2017, and July 2017
Deposition: 1 deposition November 2016, 1 deposition July 2017, 1 deposition August 2017

On behalf of Blue Coat in Finjan Inc. v. Blue Coat Systems LLC (2017-2018)

Counsel: Originally Wilson, Sonsini, Goodrich and Rosati PC; later Morrison & Foerster LLP
Venue: Case No. 15-cv-03295-BLF-SVK (Nor. District of California, San Div.)
Subject Matter: Firewalls, gateway, security devices, malware
Reports: 1 report submitted April 2017
Deposition: 1 deposition April 2017
Trial: February 2017 (Tech tutorial), November 2017

On behalf of Sedosoft in Sedosoft Inc. v Mark Burchett LTD and NFSx9 LLC (2016)

Counsel: McInnes and McLane LLP
Venue: Case No. Civil Action No. 1:15-cv-10244-RGS (District of Massachusetts)
Subject Matter: Code theft
Reports: 1 report submitted May 2016 and August 2016

On behalf of USAA in Asghari-Kamrani, et al. v. United Services Automobile Association, Inc.

Counsel: Fish and Richardson PC
Venue: Inter Partes Review Case No. IPR2015-01842, and CBM2016-00063, CBM2016-00064
Subject Matter: Applied cryptography, authentication
Reports: 1 report submitted September 2015, 1 report submitted April 2016
Deposition: 1 deposition March 2017

On behalf of WTS Paradigm in WTS PARADIGM, LLC v EDGEAQ, LLC (2015-2016)

Counsel: Quarles & Brady LLP
Venue: Case No. 3:15-CV-330 (Western District of Wisconsin)
Subject Matter: Software-assisted product configuration, presentation, and ordering
Reports: 1 report submitted March 2016
Deposition: 1 deposition April 2016

On behalf of Mr Leon Stambler in Mr. Leon Stambler v Mastercard IPR (2015-2016)

Counsel: Flachsbar & Greenspoon, LLC
Venue: CBM2015-00044
Subject Matter: Authentication, authentication codes
Reports: 1 declaration submitted October 2015
Deposition: 1 deposition December 2015

On behalf of Trusteer/IBM in Trusted Knight Corporation v. International Business Machines Corporation and Trusteer, Inc. (2015)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: C.A. No. 14-1063 LPS-CJB (District of Delaware)
Subject Matter: Key logging, protections against

Reports: 1 declaration submitted July 2015

On behalf of Sensus in Sensus USA, Inc. v. Certified Measurement, LLC (2015)

Counsel: Feldman Gale PA
Venue: Inter Partes Review Case No. IPR2015-01262, IPR2015-01311, IPR2015-01439, IPR2015-01454
Case number 3:14-cv-01069 (District of Connecticut)
Subject Matter: Applied cryptography, certification of data
Reports: 1 declaration submitted June 2015, 4 declarations submitted July 2015

On behalf of Chad Eichenberger in Chad Eichenberger v. ESPN (2015)

Counsel: Edelson PC
Venue: Case No. 2:14-cv-00463 (Western District of Washington)
Subject Matter: Consumer privacy
Reports: 1 declaration submitted January 2015

On behalf of Microsoft Corporation in Microsoft Corporation v. Optimum Content Protection LLC. (2014)

Counsel: Sidley Austin LLP
Venue: Inter Partes Review No. IPR2015-00048
Subject Matter: DRM, data streaming, protection
Reports: 1 declaration submitted October 2014

On behalf of Fortinet in Fortinet v. Sophos (2014-2015, multiple cases)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: Inter Partes Review No. IPR2015-00618
Case No. 3:13-cv-05831-EMC (DMR) (Nor. District of California, SF div.)
Case No. 1:14-cv-00100-GMS (District of Delaware)
Subject Matter: Antivirus, anti-malware
Reports: 2 declarations submitted September 2014, 1 submitted September 2015
1 report submitted October 2015, November 2015
Deposition: 1 deposition October 2014, 1 deposition October 2015
Trial: December 2015 (Tech tutorial)

On behalf of Afiliat in Afiliat PLC v Architelos Inc and Alexa Raad (2015)

Counsel: Haynes Boone LLP
Venue: Case No. 1:15-cv-00014-LMB-JFA (Eastern District of Virginia)
Subject Matter: Domain name system anti-abuse
Reports: 1 report submitted April 2015, May 2015
Deposition: 1 deposition June 2015
Trial: August 2015

On behalf of Telit in M2M v. Motorola, Telit (2015-2016)

Counsel: Pearl Cohen Zedek Latzer Baratz LLP
Venue: Case No. 12-033-RGA (District of Delaware)
Subject Matter: Authentication
Reports: 1 declaration submitted May 2014,
1 report submitted July 2014, August 2014
Deposition: 1 deposition June 2015

On behalf of Rmail/Rpost in Rmail Limited, v. Amazon.com, Inc., and Paypal and Rmail Limited, Rpost Communications Limited, and Rpost Holdings Inc., v.DocuSign, Inc. (2013-2014)

Counsel: Hudnell Law Group PC

Venue: Case No. 2:10-CV-258-JRG (Lead Case)
Case No. 2:11-CV-299-JRG (Member Case) (E.D. Texas)
Subject Matter: Email security
Reports: 2 reports April 2013, 1 declaration June 2013
Deposition: 1 deposition May 2013 (2 days)

On behalf of Via Vadis in Via Vadis v. Skype (2012-2014)

Counsel: WTP Law
Venue: Via Vadis v. Skype, Case No. 11-507 (RGA) (District of Delaware)
Subject Matter: P2P communications
Reports: 1 affidavit December 2012