

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Francisco Martinez de Velasco Cortina, et al.
U.S. Patent No.: 10,762,187 Attorney Docket No.: 50095-0313IP1
Issue Date: September 1, 2020
Appl. Serial No.: 14/659,502
Filing Date: March 16, 2015
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

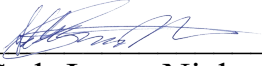
By: 
Seth James Nielson, Ph.D.

Table of Contents

I.	INTRODUCTION	4
II.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	4
III.	OVERVIEW OF CONCLUSIONS FORMED	16
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 '187 PATENT	23
	A. Overview of the '187 Patent	23
	B. Prosecution History of the '187 Patent.....	26
	C. Claim Construction	27
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 Niwa.....	35
	D. The Maes-Niwa Combination (MNC).....	37
	E. Overview of Bjorn	42
	F. The Maes-Bjorn Combination	45
	G. Overview of Walker.....	53
	H. The Maes-Walker Combination	54
	I. Overview of Shults	56
	J. The Maes-Niwa-Shults Combination (MNSC)	57
	K. The Maes-Bjorn-Shults Combination (MBSC).....	60
	L. The Maes-Walker-Shults Combination (MWSC)	61
VIII.	MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '187 CLAIMS UNPATENTABLE	61
	A. Ground 1A: Maes-Niwa Renders Obvious Claims 1-6, 8-13 and 15-21	61
	B. Ground 1B: Maes-Niwa-Shults Renders Obvious Claims 7 and 14	111
	C. Ground 2A: Maes-Bjorn Renders Obvious Claims 1-6, 8-13, and 15-21..	112
	D. Ground 2B: Maes-Bjorn-Shults Renders Obvious Claims 7 and 14....	128
	E. Ground 3A: Maes-Walker Renders Obvious Claims 1-6 and 15-21....	128
	F. Ground 3B: Maes-Walker-Shults Renders Obvious Claim 7.....	136

IX. CONCLUSION.....	136
---------------------	-----

I. INTRODUCTION

1. I have been retained by Fish and Richardson P.C. to offer technical opinions related to U.S. Patent No. 10,762,187 (“the ’187 patent”) (EX1001) with respect to an inter partes review (“IPR”) petition of the ’187 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 ’187 patent.

2. I have been asked to provide my independent analysis of the ’187 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 ’187 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 ’187 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 '187 Patent (EX1001), and relevant excerpts of the prosecution history (EX1002) of the '187 Patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references and documents:

- EX1001 U.S. Patent No. 10,762,187 to de Velasco Cortina, et al. (the “'187 Patent”)
- EX1002 The Prosecution History of the '187 Patent (the “Prosecution History”)
- EX1004 U.S. Patent No. 6,016,476 to Maes et al. (“Maes”)
- EX1005 U.S. Patent No. 6,453,301 to Niwa (“Niwa”)
- EX1006 U.S. Patent No. 6,035,398 to Bjorn (“Bjorn”)
- 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”)
- EX1010 U.S. Patent No. 6,434,159 to Woodward, et al.
 (“Woodward”)
- EX1021 U.S. Patent No. RE36,788E (“Mansvelt”)
- EX1022 U.S. Patent No. 6,098,053 (“Slater”)
- EX1023 U.S. Patent No. 10,706,412 (“the ’412 Patent”)
- EX1035 U.S. Patent No. 5,698,836 to Fujioka (“Fujioka”)
- EX1036 U.S. Provisional Application No. 60/304,216 to Williamson,
 et al. (“Berardi Prov.”)
- EX1037 U.S. Patent Application Publication No. 2004/0049451 to
 Berardi, et al. (“Berardi App.”)
- EX1038 U.S. Patent No. 6,213,391 to Lewis (“Lewis”)
- EX1039 U.S. Patent No. 5,832,090 to Raspotnik (“Raspotnik”)

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 ’187 Patent at the time of the earliest possible priority date of the ’187 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 '187 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 '187 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-Niwa Renders Obvious Claims 1-6, 8-13 and 15-21

Ground 1B: Maes-Niwa-Shults Renders Obvious Claims 7 and 14

Ground 2A: Maes-Bjorn Renders Obvious Claims 1-6, 8-13, and 15-21

Ground 2B: Maes-Bjorn-Shults Renders Obvious Claims 7 and 14

Ground 3A: Maes-Walker Renders Obvious Claims 1-6 and 15-21

Ground 3B: Maes-Walker-Shults Renders Obvious Claim 7

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 1-21 ("the Challenged Claims") of the '187 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 '187 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.

V. LEGAL STANDARDS

A. Terminology

36. 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 '187 Patent was filed March 16, 2015, 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 '187 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 '187 Patent as the point in time for claim interpretation purposes.

B. Legal Standards

37. 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.

38. 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

39. 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.

40. 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.

41. 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

42. 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.

43. 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."

44. 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.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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 '187 PATENT

A. Overview of the '187 Patent

50. The '187 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, 1:7-12 (describing the “Field of the Invention”).

51. As shown in the '187 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, 2:3-9.

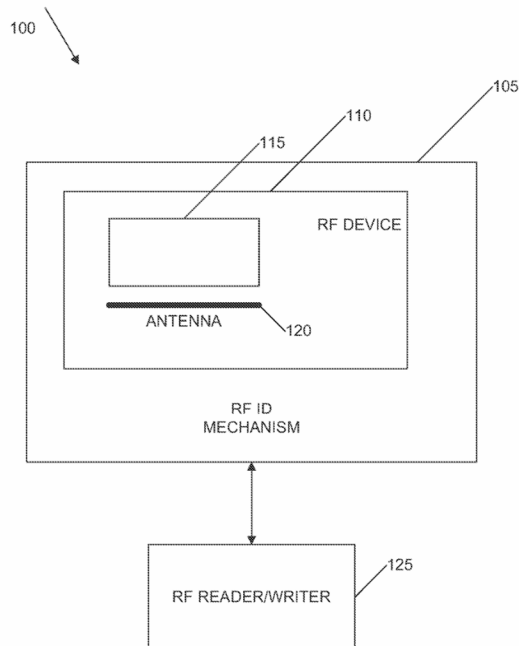


FIG. 1

EX1001, Fig. 1.

52. In some embodiments the “RF identification mechanism is a card”; however, as the ’187 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, 2:45-55.

53. An “RF device ... has a unique identifier ... and the information contained on it is protected by sundry cryptographic methods.” EX1001, 8:35-39. “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 '187 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, 8:39-48.

54. 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, 13:6-16.

55. “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, 13:17-20. “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, 13:20-26.

56. As the '187 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, 14:4-10.

57. 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, 13:43-49.

B. Prosecution History of the ’187 Patent

58. During prosecution of the application for the ’187 Patent, the Examiner rejected the independent claims as allegedly obvious over Walker (EX1007) in combination with certain secondary references. In making these rejections, the Examiner mapped Walker’s generated single-use credit card number, which is created using key-based encryption involving a nonce, private key, and account number, directly to the claimed “*key*.” EX1002, 33, 37.

59. The applicant appealed the Examiner’s rejection based on Walker arguing that Walker was distinguishable based on Walker’s timing requirement of key generation. EX1002, 28, 51-52. The applicant contended that Walker uses biometric authentication solely to grant initial access to a smartcard device, and that only after access is granted does Walker’s system prompt the user and wait for an affirmative response before generating a single-use number. EX1002, 28, 50-51. The applicant argued that this sequence failed to teach generating a key when

(upon) successful biometric authentication as required by the claims. *See* [1.5.2], [8.6.2], [15.4]; EX1002, 28, 51. Notably, however, the Applicant never contested the Examiner's mapping of Walker's single-use number to the claimed key, relying exclusively on the timing sequence to overcome the rejection. EX1002, 28, 51.

60. The Board agreed with the Applicant's arguments on appeal, finding that Walker's mandatory user prompt creates a necessary delay between the end of biometric authentication and the generation of the single-use card number. EX1002, 28-29. Consequently, the Board determined that Walker does not teach generating a key when biometric information is authenticated, resulting in the allowance and issuance of the '187 Patent. EX1002, 2, 29-30.

61. As this Declaration demonstrates, however, the Examiner's decision to allow the '187 Patent following the Board's reversal of the rejection based on Walker did not include combinations with relevant prior art. There is no indication that the Examiner had reviewed Maes (EX1004), Niwa (EX1005), or Bjorn (EX1006) before allowing the '187 Patent. The prior-art combinations based on these references (and Walker) presented herein demonstrate prior disclosure of the exact feature the Board found missing from Walker alone.

C. Claim Construction

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

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

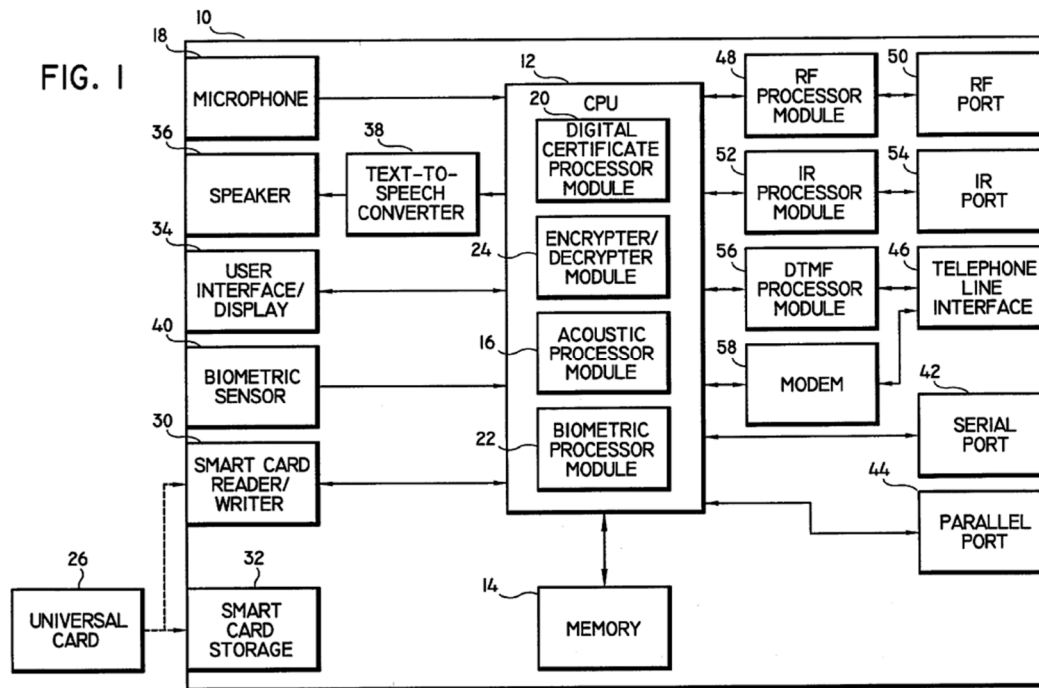
64. Should the Patent Owner or the Board provide further remarks on construction, I may supplement my analysis in response to their remarks.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Maes

65. 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.

66. 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.



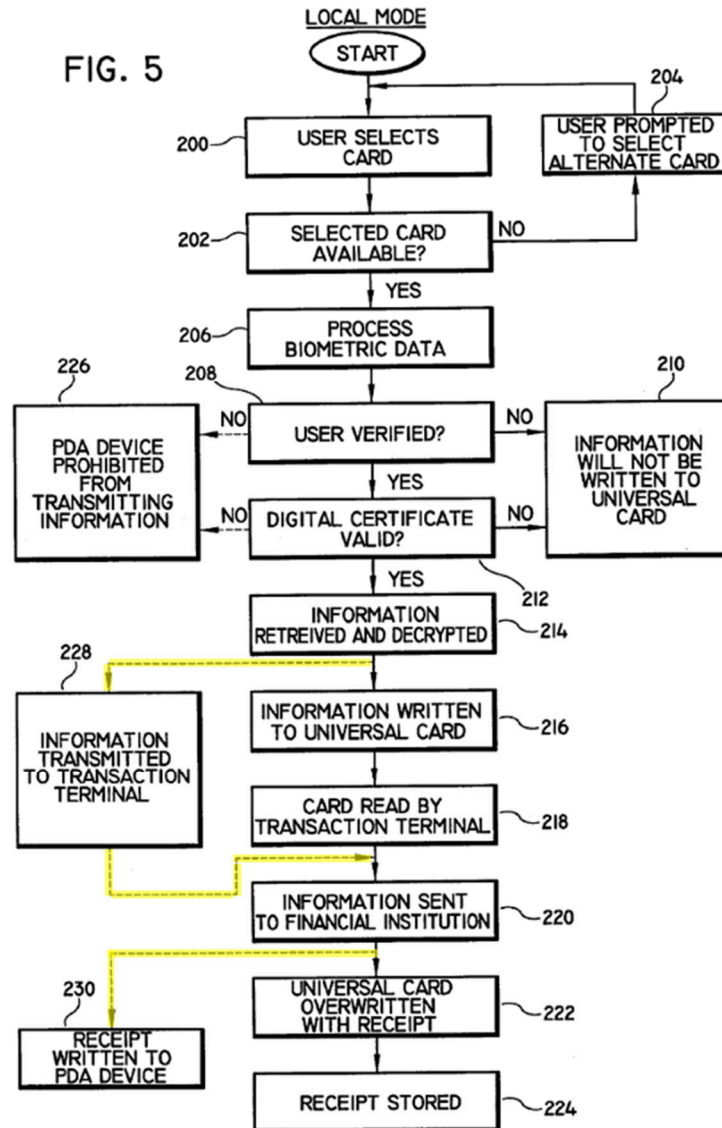
EX1004, Fig. 1.

67. 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 EARM cards”¹). The Universal Card “contains a unique ... number

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

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.

68. 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.



EX1004, Fig. 5 (highlighting added).

69. 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”).

70. 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.

71. 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.

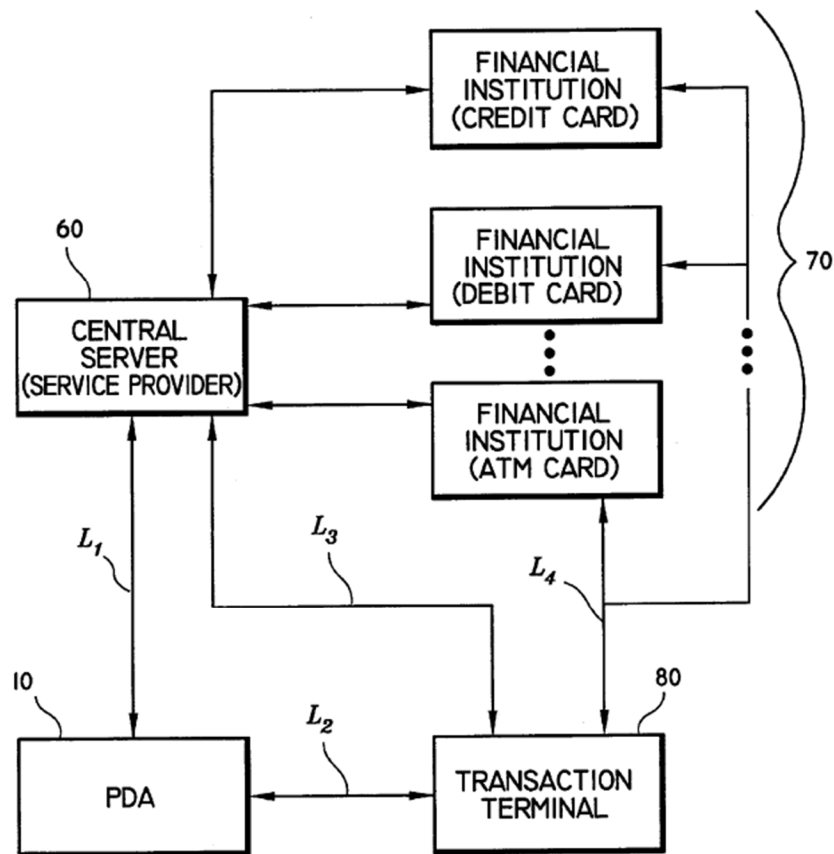


FIG. 3

EX1004, Fig. 3.

72. 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.

73. “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.

74. 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

75. Grounds 1A-3B below demonstrate that the Challenged Claims of the ’187 Patent would have been obvious to a POSITA before the Critical Date based on prior-art combinations involving Maes, Niwa, Shults, Bjorn, and Walker. Each of these references is analogous art in the same field as the ’187 Patent (e.g., secure transactions and communications) and/or reasonably pertinent to problem(s) purportedly addressed by the ’187 Patent (e.g., verifying or authenticating users in secure transactions). See EX1001, 13:17-26, 13:43-49, 14:4-10; EX1004, 1:10-17; EX1005, 5:51-6:58, Abst.; EX1006, 1:5-51, Abst.; EX1008, [0003], [0009], [0030], Abst.; EX1007, 1:6-10, 3:59-4:4, Abst.

C. Overview of Niwa

76. Like Maes, Niwa describes “[a] method of authorizing a commercial transaction between a customer and a provider of goods or services over a network, wherein the provider of goods or services requests that the customer provide authentication by activating a fingerprint identification device, and the provider of goods or services receives at least an authentication code of the customer over the network from the fingerprint identification device.” EX1005, Abstract.

77. Niwa explains that “[t]he card issues an authorization code only when the fingerprint of the customer 52 matches the stored fingerprint.” EX1005, 4:32-34.

78. In Niwa, “[d]ata transfer is ... conducted between the fingerprint identification device 50 . . . and the provider of goods and/or services 60, 62 or 64 (action 112).” EX1005, 5:63-67. “The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:67-6:3. Niwa states that “[m]ost preferably, the data of this transfer are in encrypted form.” EX1005, 6:3-4.

79. At the point of sale, Niwa further explains that “[i]nstead, the data (*e.g.*, at least one of the authentication code, payor bank identification number, customer account number, delivery address, etc.) would be provided to, for example, the merchant 70 and/or service provider 72 at the point of sale (action 112).” EX1005, 6:54-58.

80. At Niwa's "action 116, the provider . . . preferably transfers data to the payor bank 10, which data preferably includes at least one of the authentication code, payor bank identification number, customer account number, and purchase amount." EX1005, 6:13-17. Niwa teaches that "[m]ost preferably, the payor bank 10 analyzes the authentication code (action 124) to verify its validity prior to authorizing the transaction." EX1005, 6:23-25.

D. The Maes-Niwa Combination (MNC)

81. Maes's PDA transmits selected card information for a secure transaction over an RF link to a point-of-sale (POS) terminal. EX1004, 12:5-29; *supra*, §VII.A. Maes further teaches that the user can provide an authorization number for the transaction to the merchant, which the merchant in turn provides to a central server for use in verifying the user and authorizing the transaction. EX1004, 12:39-54, 12:65-13:5. In particular, Maes discloses an example use case where the user verbally conveys the authorization number to the merchant, such as where the merchant lacks an electronic POS terminal. EX1004, 12:39-54, Fig. 6.

82. To the extent Maes does not expressly disclose that the authorization number is transmitted from the PDA to the POS terminal over an RF link, Niwa complements Maes in teaching that not only payment information but also an authentication code (analogous to Maes's authorization number for the purpose of this combination) can be electronically transmitted to a merchant. *Supra*, §VII.C.

In particular, Niwa describes a “[d]ata transfer ... conducted between [a] fingerprint identification device 50 . . . and [a] provider of goods and/or services 60, 62 or 64” where “[t]he data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:63-6:4, Fig. 3 (step 112). ²For a POS transaction, “the data (e.g., at least one of the authentication code, payor bank identification number, customer account number, delivery address, etc.) would be provided to, for example, the merchant 70 ... at the point of sale.” EX1005, 6:54-58.

83. A POSITA would have found it obvious to implement Maes’s system in accordance with Niwa’s suggestion for transmitting payment information and an authorization number from a user device to a merchant for use in a transaction over a common electronic channel. In the resulting Maes-Niwa Combination (MNC), Maes’s PDA transmits not only the selected card information but also the authorization number to the merchant’s POS terminal over an electronic channel in the form of Maes’s RF link. The merchant then provides both the selected card information and the authorization number to a financial institution to authorize the transaction in accordance with Maes’s teachings. EX1004, 12:55-13:5.

84. Multiple reasons would have prompted a POSITA to pursue MNC.

² All emphasis in this Declaration is added unless otherwise noted.

85. First, a POSITA would have been motivated to make the combination to make beneficial use of the authorization number not only in transactions where the merchant lacks an electronic card reader, but also in transactions involving electronic POS terminals. Maes explains that “[s]ince the authorization number is a function of the unexpired digital certificate that was obtained from the central server 60 ..., the central server 60 inform[s] the merchant the user was properly verified.” EX1004, 13:1-5. The authorization number can be similarly used to aid in verifying the user regardless of whether the authorization number is conveyed to the merchant verbally or over an electronic channel such as Maes’s RF link. The authorization number would be used in place of the existing “encrypted information file” when transmitting over an RF link. Maes already discloses, “the selected card information, as well as the encrypted information file, would be transmitted to the POS terminal (via the Universal Card, RF or IR) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details.” EX1004, 13:34-38. A POSITA would have understood that the authorization number could be used in place of the encrypted information file for faster transmission and verification. Maes also discloses offloading authentication to a server. “The merchant will then transmit the Universal Card number 27 and the displayed authorization number to the central server 60. Since 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 inform the merchant that the user was properly verified (step 318).” EX1004, 12:66-13:5. Thus, Maes already discloses transmitting the number from the POS to a central server. A POSITA would have understood that this number could be used in place of the “encrypted information file.”

86. Second, a POSITA would have been motivated to pursue MNC to improve the security of the transaction. Verbal communication of the authorization number at the POS risks exposing the number to unauthorized bystanders who may be listening for or who may otherwise overhear the number when spoken to the merchant. Transmitting the authorization number electronically as taught in Niwa obviates the need to verbally communicate the authorization number, thereby preventing any bystanders or aural listening devices from obtaining an audibly conveyed number.

87. Moreover, per Niwa, all information electronically transmitted in a transaction including card information and the authorization number can be encrypted, further improving security. EX1005, 4:43-47, 6:3-4 (data “remain[s] encrypted when transmitted from the device 50 to any other device”); EX1004, 5:1-4, 5:14-17, 6:9-14, 13:33-38 (discussing information transmitted in encrypted form); *infra*, [1.5.1]. Niwa’s teaching to apply encryption to an authentication code or authorization number when transmitted electronically (over RF in MNC)

provides an independent basis for combining Maes and Niwa, even beyond Niwa's antecedent of transmitting these items electronically. Encrypting the transmission would have been obvious and beneficial to prevent unauthorized entities from intercepting and reading the transmitted information for the transaction in the clear.

88. Third, a POSITA would have been motivated to pursue MNC to improve the efficiency of the transaction at the point of sale. By electronically transmitting the authorization number over the same communication channel (*i.e.*, Maes's RF link) that carries the selected card information, the user need only utilize a single communication modality to convey all necessary information for the transaction to the merchant (either at once or in separate phases). In any event, electronic transmission of the authorization number eliminates the time and effort involved in the user manually reading the authorization number to the merchant. This would predictably yield a more frictionless experience for users at the POS, which a POSITA would expect would beneficially increase usage of Maes's payment technology.

89. Fourth, a POSITA would have pursued MNC because it involves nothing more than the predictable application of a known technique (*e.g.*, Niwa's electronic data transfer) to a known device ready for improvement (*e.g.*, Maes's PDA device in its direct-RF-transmission embodiments) to yield predictable results

(e.g., RF transmission containing both the card information and authorization number, forwarded to financial institution for validation).

90. A POSITA also would have reasonably expected success implementing the combination. Well before the '187 Patent's Critical Date (July 9, 2002), it was known how to transmit a range of information over short-range RF links like those described in Maes. Maes further explains that the PDA device 10 generates its RF "transmission signals which are outputted from the RF port 50 using conventional constructions and techniques." EX1004, 6:9-15. Adding an additional data field to carry the authorization number, which the PDA has already generated upon local verification, would be a trivial engineering exercise. Indeed, Maes already discloses the option of transmitting multiple information items including "[t]he selected card information, as well as [an] encrypted information file" in an RF transmission. EX1004, 13:34-38.

E. Overview of Bjorn

91. Bjorn describes "cryptographic key generation using biometric data." EX1006, 1:1-2. Bjorn explains that its techniques "relate[] to cryptography, and more specifically, to the generation of a unique cryptographic key using biometric data." EX1006, 1:5-7.

92. In Bjorn, a message is created from a received fingerprint and "[a] message digest function is applied to the message to create a cryptographic key."

EX1006, 1:42-46, 1:50-51. Bjorn states that “[f]or one embodiment, a one-way hash function or message digest function is used to create the hash.” EX1006, 3:45-47. Bjorn further notes that “[g]iven the hash it is computationally impossible to find a message with that hash.” EX1006, 3:49-52.

93. With reference to Fig. 3 (reproduced below), Bjorn explains that “[a]t block 320, a template is created for the user.” EX1006, 4:21-23. “For one embodiment, the fingerprint template is a digital image of the fingerprint.” EX1006, 8:32-33. “At block 325, the template is hashed.” EX1006, 4:25. Bjorn adds that “[f]or one embodiment, this hash is the cryptographic key.” EX1006, 4:25-26. Bjorn further states that “[t]his cryptographic key is identified with the specific fingerprint, and thus with a specific user.” EX1006, 4:28-30. “At block 335, the template is stored,” although “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48. Bjorn notes that “the template is stored in a database, or other more centralized location.” EX1006, 4:47, 4:51-53.

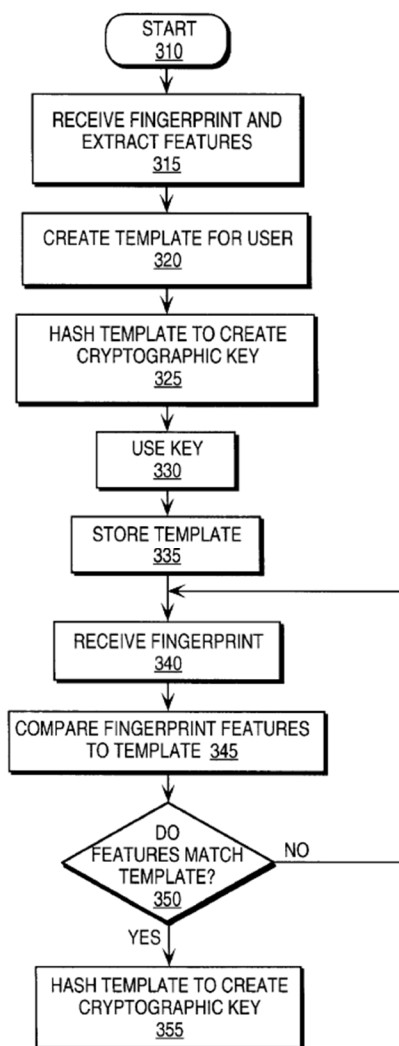


FIG. 3

94. According to Bjorn, “if [a] new fingerprint matches the template” then the system “appl[ies] the message digest function to the template to generate the cryptographic key.” EX1006, claim 3. Thus, “[a]t block 355, the template is again hashed to create a cryptographic key.” EX1006, 5:10-11. Bjorn explains that “[s]ince the template was used to generate the first cryptographic key, the same key is generated.” EX1006, 5:11-12. Bjorn’s cryptographic key can then be used in a cryptographic function to encrypt or decrypt desired data item(s). EX1006, 4:38-

45 (“At block 330, the cryptographic key is used. ... For example, the key may be used to sign a document with the user’s private key.”); *see also id.*, 5:15-6:23 & Fig. 4 (describing alternate embodiment in which the cryptographic key is generated from aspects of the fingerprint other than those from which the template is formed), Figs. 5-8 (describing uses of the key with a digital certificate).

F. The Maes-Bjorn Combination

95. The Maes-Bjorn Combination (“MBC”) integrates, in Maes, Bjorn’s technique for generating a cryptographic key from biometric data such as a user’s fingerprint. *Supra*, §VII.E. In MBC, Maes’s encrypted information file (see EX1004, 13:19-39), which Maes’s PDA device 10 transmits to the merchant’s POS terminal along with payment information for a POS transaction, is modified to include a cryptographic key generated in accordance with Bjorn’s techniques (e.g., as described with respect to Figs. 3 or 4 of Bjorn) in response to biometric authentication of the user (e.g., in response to determining that the user’s fingerprint obtained at the POS matches a stored template (e.g., “a digital image of the fingerprint”), per Bjorn steps 350 or 460). EX1006, 8:32-34; EX1004, 13:19-39. In the combined Maes-Bjorn device (the “Maes-Bjorn Combination” or “MBC”), Bjorn’s block-355/470 key regeneration is triggered by the local biometric verification Maes already performs on the PDA. EX1006, 5:3-12, Figs. 3-4; EX1004, 5:54-57, 11:9-13.

96. Multiple reasons would have motivated a POSITA to implement the combination, and a POSITA would have reasonably expected success. Indeed, the proposed combination is a natural extension of what Maes and Bjorn each already teach on their own. Maes expressly describes the encrypted information file as containing “unique identifying information pertaining to the consumer including, but not limited to, such as the consumer’s name and account number.” EX1004, 13:26-32. Maes further explains that the purpose of this encrypted information file is to enable “the financial institution (*e.g.*, credit card company) [to] verify the identity of the consumer during a purchase transaction.” EX1004, 13:20-24. Maes thus contemplates that additional unique identifying information, beyond the illustrative examples of name and account number, may be included in the encrypted information file to authenticate the consumer to the financial institution.

97. Bjorn’s cryptographic key is precisely such unique identifying information. Bjorn teaches “generat[ing] a unique cryptographic key using biometric data,” specifically from a user’s fingerprint, creating a message from the fingerprint, and applying a message digest function to the message to produce the key. EX1006, 1:5-8, 4:26-33, Abstract. Because the fingerprint of each user is unique, and because “[t]his cryptographic key is identified with the specific fingerprint, and thus with a specific user,” EX1006, 4:29-31, Bjorn’s key represents “unique identifying information” tied to the individual consumer as

contemplated in Maes. A POSITA would have recognized that including Bjorn's cryptographic key in Maes's encrypted information file supplements and improves upon the "name and account number" examples already contemplated by Maes with a biometric identifier. *See* EX1004, 13:26-30. Bjorn's cryptographic key alternately represents an obvious substitution for information such as the "name" of the user given in Maes since the cryptographic key, like name data, serves to identify the user.

98. For example, Maes explains that the encrypted information file enables "the financial institution (*e.g.*, credit card company) [to] verify the identity of the consumer during a purchase transaction." EX1004, 13:22-24. A POSITA would have recognized that including Bjorn's cryptographic key in the information file strengthens the financial institution's ability to verify the user. Maes discloses example contents of the file including "name and account number," but this information would be readily available to an unauthorized holder of a lost or stolen card, and that information thus does not, by itself, confirm that the person presenting the card is the person authorized to use it. EX1004, 13:22-24, 13:30-32. Because Bjorn's cryptographic key is instead derived from the user's fingerprint, rather than from the card, it uniquely identifies the authorized user in a way that cannot be readily obtained by an unauthorized holder of the card. EX1006, 4:28-30. A POSITA would therefore have recognized that including Bjorn's key in the

encrypted information file supplies the financial institution with an additional identifier not otherwise obtainable from the card itself, better ensuring that MBC will not authorize a transaction unless the person presenting the card is in fact the authorized user associated with the payment card account, thereby enhancing the financial institution's ability to "verify the identity of the consumer during a purchase transaction," as described in Maes. EX1004, 13:22-24; EX1006, 4:28-30.

99. Moreover, both Maes and Bjorn independently teach fingerprint-based authentication. Maes discloses that its biometric sensor may collect biometric data derived from "a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric verification." EX1004, 5:53-58; *see also id.*, 11:1-5 (biometric data including "finger, thumb or palm print data"). Bjorn is similarly directed to fingerprint-based cryptographic key generation. EX1006, Abstract; 1:5-8. Because Maes already contemplates fingerprint biometrics as one of its verification modalities, incorporating Bjorn's fingerprint-based cryptographic key into Maes's system would not require any conceptual departure from what Maes already teaches; it merely uses the fingerprint data Maes already contemplates collecting for an additional, complementary purpose taught by Bjorn.

100. A POSITA also would have turned to Bjorn because Bjorn's approach improves security by maintaining no persistent copy of the key on the user device,

teaching that “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48. The key must therefore be produced each time it is required. EX1006, 5:8-12. Regenerating the key only upon a successful fingerprint verification ensures that the key exists only when the authorized user is confirmed, which advances Maes’s aim of biometric security that “protects against the unauthorized access to the user’s financial and personal information” and reduces the risk of the key leaking to unauthorized parties. EX1004, 4:9-10.

101. Maes additionally describes an enrollment process in which the service provider stores biometric information for the user on the central server for later verification. EX1004, 7:24-31 (“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”). Maes teaches that this biometric data could include fingerprint data. EX1004, 5:53-59. Because Maes’s enrollment already stores the user’s biometric data at the service provider, and because Maes contemplates that data being fingerprint data, a POSITA would have understood that enrolling a user’s fingerprint template as taught in Bjorn requires no change to Maes’s enrollment architecture. EX1004, 5:56-59, 7:28-31; EX1006, 3:14-15. In MBC, Maes’s POS terminal transmits the encrypted information file to the financial institution, at which the comparison occurs. EX1004, 13:34-38. Because, in Maes, the financial institution verifies the consumer during the transaction (“the

financial institution (*e.g.*, credit card company) can verify the identity of the consumer during a purchase transaction”), a POSITA would have stored the user’s template for comparison at that institution, which Bjorn teaches may be “a database, or other more centralized location.” EX1004, 13:22-24; EX1006, 4:47, 4:51-53.

102. Bjorn teaches that hashing the stored template reproduces the same key, explaining that “[a]t block 355, the template is again hashed to create a cryptographic key,” and that “[s]ince the template was used to generate the first cryptographic key, the same key is generated.” EX1006, 5:10-12. For example, as part of the determination whether to authorize a requested transaction, the financial institution could beneficially verify that the user had successfully passed local biometric verification by comparing the cryptographic key contained in the encrypted information file with the reference key regenerated from the enrolled template. *See* EX1004, 13:34-38, 13:47-56; EX1006, 5:10-12, 4:28-30 (“This cryptographic key is identified with the specific fingerprint, and thus with a specific user.”). In MBC, to determine whether to authorize a transaction, the financial institution regenerates the reference key from the enrolled template and compares it against the cryptographic key contained in the encrypted information file. EX1004, 13:34-38; EX1006, 5:10-12.

103. Including Bjorn's fingerprint-derived cryptographic key in the encrypted information file thus materially strengthens verification of the user's identity in the authorization process by enabling the financial institution to confirm the identity of the person presenting the card, and not merely to validate the card, addressing the exposure Maes identifies. EX1004, 2:1-13, 12:61-63.

104. This independent server-side verification also mitigates an attack vector left open by local verification alone. In Maes's local mode, user verification is performed on the PDA by comparing captured biometric data against stored biometric authentication information. EX1004, 10:59-11:5. An attacker who gains access to the PDA could conceivably alter the reference biometric information stored on the device, allowing an unauthorized user to pass local verification. Requiring an additional layer of biometric verification at the financial institution using Bjorn's cryptographic key transmitted in Maes's encrypted information file would frustrate this attack, because the enrolled template held by the financial institution or service provider is independent of the PDA and cannot be altered by a party who has compromised only the PDA. *See* EX1006, 1:35-37 ("what is needed is a secure cryptographic key that is easily usable by the user, but not accessible to third parties.").

105. A POSITA would have been further motivated to integrate Bjorn's techniques in Maes because Bjorn's key is, by design, a fully functional

cryptographic key usable in standard cryptographic operations, including the encryption and decryption operations Maes already contemplates. Bjorn expressly teaches that its fingerprint-derived key can serve as a private key in a public-key cryptosystem, that it can be used to sign or encrypt documents, and that it is generated using well-known message digest functions such as MD5. EX1006, 3:56-58, 4:31-33, 4:36-45.

106. Maes, in turn, relies on encryption and decryption for various purposes throughout its system. For example, Maes teaches storing the digital certificate on the PDA in encrypted form such that the digital certificate is decrypted by the encrypter/decrypter module before use. EX1004, 9:52-56; *see also id.*, 5:15-19. Similarly, selected card information is encrypted while stored on the PDA and is decrypted for use during a transaction. *Id.*, 11:29-34. Maes expressly contemplates using “any known encryption technique or algorithm for the encryption/decryption process.” EX1004, 10:11-14.

107. Because Maes leaves the choice of encryption technique open, a POSITA would have been motivated to select Bjorn’s cryptographic key for one or more of these encryption/decryption operations. Doing so would provide a meaningful security benefit since Bjorn’s key can only be regenerated when a user successfully passes fingerprint verification. EX1006, 5:1-13. Using that key to encrypt the digital certificate ensures that the digital certificate can only be

decrypted when the authorized user provides a matching fingerprint. This links biometric verification to the ability to use the digital certificate for any transaction, which aligns with Maes's express design objectives. *See* EX1004, 3:31-40 ("biometric security to provide user verification prior to accessing and writing the selected financial and personal information"), *id.*, 9:52-56 (digital certificate is decrypted and validated before transaction). In MBC, a hacker who bypasses local biometric verification on the PDA would still be unable to decrypt the digital certificate without a valid fingerprint capable of regenerating Bjorn's cryptographic key.

108. A POSITA would have reasonably expected success in pursuing MBC. Both Maes and Bjorn are directed to the same general field (*e.g.*, secure electronic transactions employing biometric authentication and cryptographic techniques), and each uses conventional, well-understood technical components: fingerprint sensors, hash functions such as MD5, and standard encryption/decryption modules. *See* EX1006, 3:24-35, 3:44-58 (hash functions including MD5), 4:19-20; EX1004, 5:15-19 (encrypter/decrypter module), 10:11-14 ("any known encryption technique or algorithm").

G. Overview of Walker

109. Walker discloses a portable smart card device for generating transaction-specific, single-use credit card numbers to enhance security in credit

card transactions. EX1007, Abstract 1:6-10, Fig. 1. The device's memory stores a private cryptographic key, a nonce, an initialization variable (IV), and the cardholder's unchanging account number. EX1007, 5:49-60, 6:61-7:3, 8:9-36. To generate a single-use number, the device retrieves the nonce and IV, encrypts the nonce using the private key and IV to produce an encrypted nonce, increments the IV, and concatenates the encrypted nonce, IV, and account number into a single-use credit card number that is transmitted to the merchant and forwarded to the issuer's central processor for authorization. EX1007, 8:9-36; Fig. 8. Because a valid single-use number cannot be generated or reused without the private key and an unused IV, Walker's scheme protects against fraudulent number generation and replay of intercepted transaction data. EX1007, 6:61-7:3, 7:37-45, 10:10-21.

H. The Maes-Walker Combination

110. The Maes-Walker Combination ("MWC") implements Maes's biometrically verified RF-based transactions with a single-use credit card number as taught in Walker.

111. Maes discloses a portable device that stores a user's financial account information and, upon biometric verification, transmits "selected card information" directly to a point-of-sale transaction terminal via an established RF communication link. EX1004, 12:19-34. Maes recognizes that consumer financial cards are vulnerable when unauthorized users gain access to the account

information they carry, and expressly seeks to protect against “the unauthorized use of lost or stolen cards.” EX1004, 2:1-5. Maes’s proposed solution conditions access to the stored card information on biometric verification and confirmation that the PDA holds a valid digital certificate. While these techniques reduce the likelihood of unauthorized use of the PDA to initiate a transaction, Maes still contemplates transmitting the underlying card information in the clear over the RF link. EX1004, 6:24-29; 12:19-34.

112. Walker identifies a known vulnerability with transmitting payment information in the clear, as Maes suggests. Namely, because conventional credit card numbers are static, a third party who intercepts or “sniffs” a transmitted account number from an open channel may use that number to potentially commit fraud by initiating unauthorized transactions, including through “replay” of previously captured data. EX1007, 2:55-64. Walker thus sought to improve security by generating a transaction-specific single-use payment number, incorporating an encrypted nonce and incrementing an initialization variable, so that a captured number cannot be reused and an interceptor gains no benefit from learning the account holder’s static account number in isolation. EX1007, 3:59-64, 6:30-38, 6:61-7:3, 7:36-45, 10:10-21.

113. Given Maes’s express concern with protecting transmitted financial information from unauthorized use and Maes’s disclosure of transmitting that

information over an RF link to a transaction terminal, a POSITA would have recognized that Maes's RF transmission of card information was subject to vulnerabilities like those Walker's single-use number was designed to solve. A POSITA would have been motivated to apply Walker's technique for generating a single-use number to Maes's system such that the single-use number would be transmitted by the PDA over the RF link to improve the security of the transaction. Indeed, the combinations involves the predictable use of a known technique to improve a similar device (*e.g.*, a portable transaction device transmitting payment information over an RF link) in the same way, yielding the predictable benefit of preventing replay and misuse of intercepted transaction data. A POSITA would have reasonably expected success, especially as the underlying cryptographic techniques used in generating the single-use card number were well known before the Critical Date.

I. Overview of Shults

114. 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].

115. 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].

J. The Maes-Niwa-Shults Combination (MNSC)

116. 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.

117. 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.

118. Although Maes broadly describes the PDA having short-range RF circuitry, Maes does not expressly disclose the specific type of RF circuitry applied in the PDA. Shults does. Specifically, Shults describes a hand-held apparatus in the

form of “a portable cellular telephone or a personal digital assistant.” EX1008, [0009]. Shults further explains that “the electronic identity ... is provided by a radio-frequency identification (RFID) circuit 104.” EX1008, [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].

119. A POSITA would have found it obvious to implement the RF circuitry in Maes’s PDA 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.

120. First, a POSITA would have been motivated to use RFID in Maes’s PDA 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].

121. Second, a POSITA would have been motivated to implement RFID in Maes’s PDA 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.” Adding Shults’s circuit 104 allows MNC’s PDA device 10 to transact with existing point-of-sale systems having “electronic scanner equipment 314,” without substantial (or even any) modification to those systems. EX1008, [0037].

122. Third, a POSITA would have been motivated to use RFID in Maes’s PDA 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].

123. Fourth, a POSITA would have been motivated to implement RFID in Maes’s PDA 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 PDA 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 in the PDA’s RF circuitry. EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031].

124. The resulting Maes-Niwa-Shults Combination (MNSC) includes the PDA device 10 (per Maes), whose RF circuitry (which uses “conventional constructions and techniques”) further includes Shults’s RFID circuit 104 (per Shults). Supra, §VII.D; EX1004, 6:9-15, 12:10-15; EX1008, [0030], [0031]. MNSC’s PDA operates as in MNC, including transmitting the selected card information to the POS transaction terminal via the RF port 50. Supra, §VII.D; EX1004, 12:10-15.

125. A POSITA would have reasonably expected success applying RFID to Maes’s PDA, 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].

K. The Maes-Bjorn-Shults Combination (MBSC)

126. The Maes-Bjorn-Shults Combination (MBSC) is MBC (Ground 2A), further modified in view of Shults’s teachings such that Maes’s PDA’s RF circuitry is implemented using an RFID device. Supra, §VII.F; EX1008, [0030]. For the reasons described in §VII.J, which relate only to Maes and Shults, a POSITA would have been motivated to add Shults’s RFID circuit to Maes’s PDA and would have reasonably expected success. Supra, §VII.J.

127. MBSC's PDA device 10 otherwise operates as in MBC, including transmitting the encrypted key and payment information to the POS device via the short range RF circuitry. Supra, §VII.F, Ground 2A at [1.5.5].

L. The Maes-Walker-Shults Combination (MWSC)

128. The Maes-Walker-Shults Combination (MWSC) is MWC (Ground 3A), further modified in view of Shults's teachings such that Maes's PDA's RF circuitry is implemented using an RFID device. Supra, §VII.F; EX1008, [0030]. For the reasons described in §VII.J, which relate only to Maes and Shults, a POSITA would have been motivated to add Shults's RFID circuit to Maes's PDA and would have reasonably expected success. Supra, §VII.J.

129. MWSC's PDA device 10 otherwise operates as in MWC, including transmitting the encrypted key and payment information to the POS device via the short range RF circuitry. Supra, §VII.H, Ground 3A at [1.5.5].

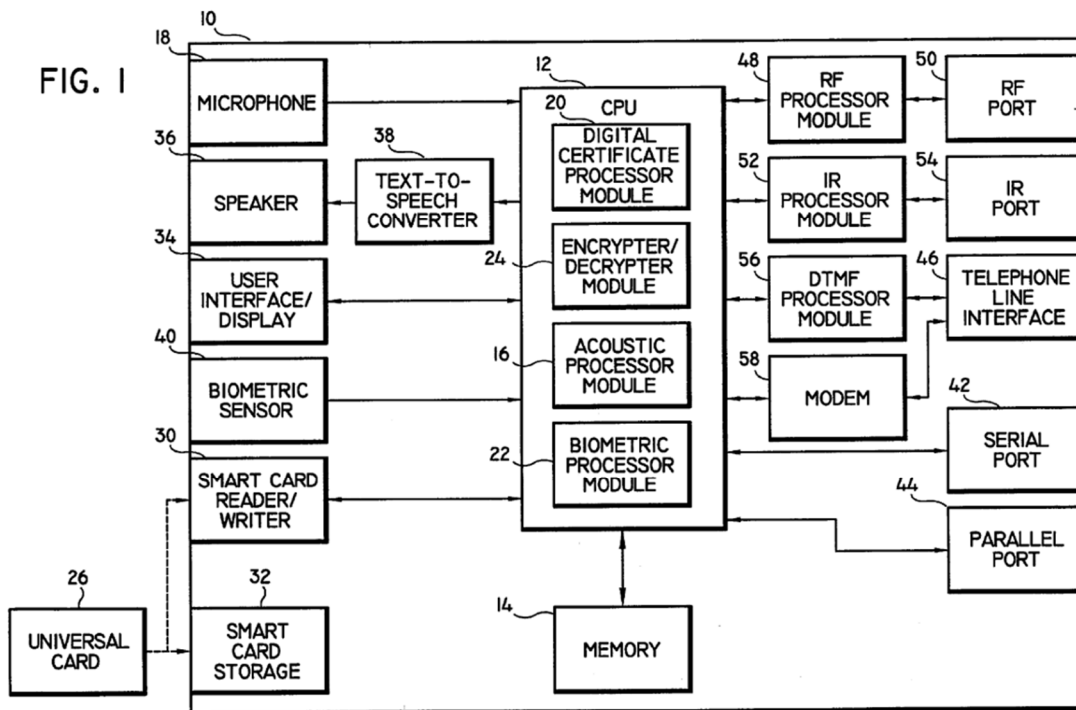
VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '187 CLAIMS UNPATENTABLE

A. Ground 1A: Maes-Niwa Renders Obvious Claims 1-6, 8-13 and 15-21

[1.pre] A mobile device, comprising:

130. MNC renders [1.pre] obvious.

131. Maes discloses a "portable client PDA" (*mobile device*), e.g., PDA device 10 depicted in Fig. 1 below. EX1004, Abstract, 4:65-6:27.



EX1004, Fig. 1.

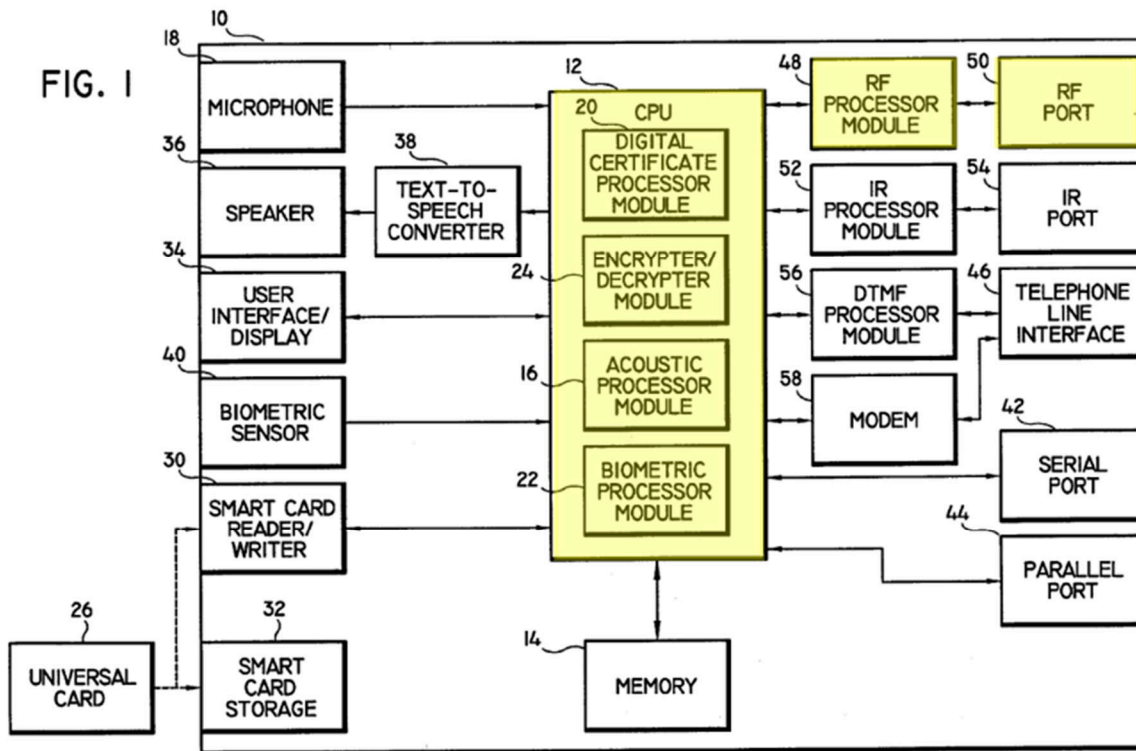
132. Maes's PDA "provide[s] direct communication capability with peripheral devices (such as POS ... terminals) and is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication." EX1004, Abstract; *see also id.*, 6:8-19, 12:5-29, Fig.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

[1.1] short range radio frequency (RF) circuitry;

133. MNC renders [1.1] obvious.

134. Maes's PDA (*mobile device*) "is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) ... communication." EX1004, Abstract.

135. 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 PDA 10 includes *short range radio frequency (RF) circuitry* such as RF port 50, RF processor module 48, and/or CPU 12.



EX1004, Fig. 1 (highlighted).

136. A POSITA would have understood Maes's RF circuitry to be *short-range* circuitry. Maes describes the RF link L2 as a direct wireless channel between the PDA held by the user and the POS transaction terminal 80. EX1004, 12:5-29. Maes expressly treats 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, 12:16-17, 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.

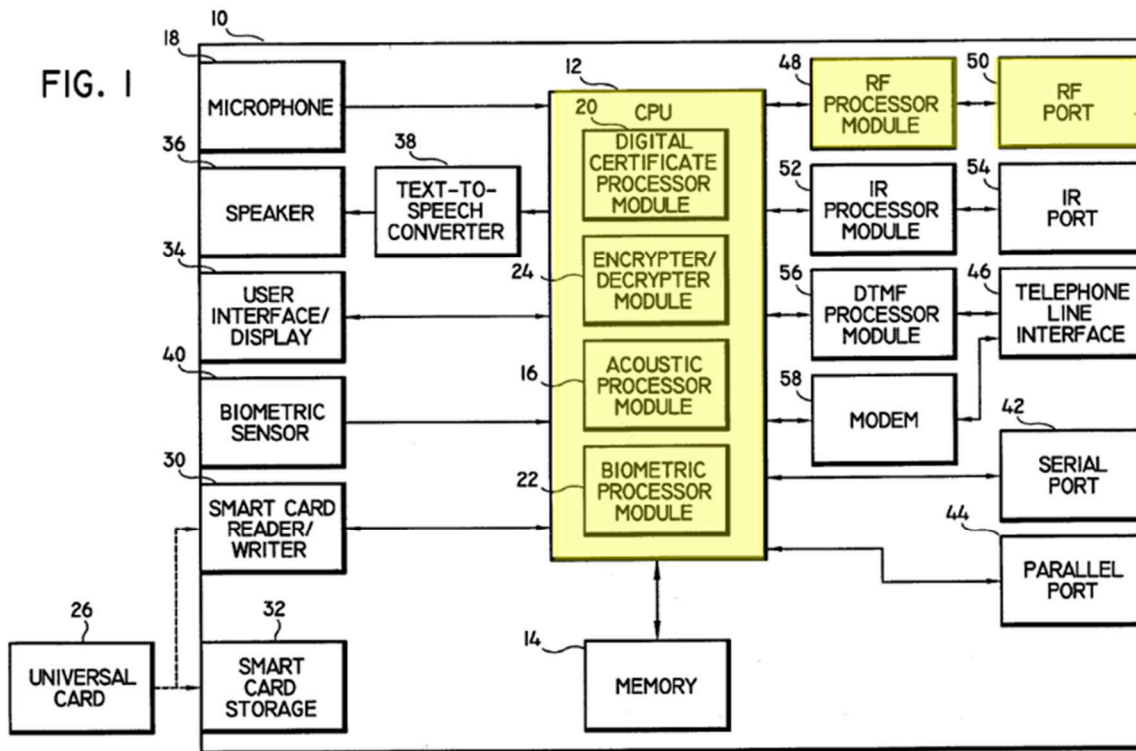
EX1004, 7:65-8:14. Accordingly, Maes's RF circuitry that is used for a direct link between the PDA and a nearby transaction terminal is *short range*.

[1.2] memory configured to store biometric authentication information and payment information;

137. MNC renders [1.2] obvious.

138. Maes discloses that the PDA (*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").

139. In more detail, and 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).

140. The “financial information” stored in Maes’s memory 14 includes information for at least one credit card (payment 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 cards ... 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. Maes’s “selected card information” thus provides payment information stored in a memory (e.g., memory 14) of the PDA device 10 (mobile device) as claimed. Supra, §VI.C.

141. The “personal information” stored in memory 14 further includes ***biometric authentication information***, such as a voice or fingerprint 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 Maes’s PDA 10 memory (e.g., memory 14) stores ***biometric authentication information*** used by the biometric processor module 22 to authenticate the user attempting a transaction. Additionally or alternatively, it would have been obvious to store

biometric authentication information in the memory of the PDA for each of the biometric modalities contemplated in Maes, as doing so would beneficially allow the biometric processor module 22 to authenticate a user in local mode by comparing the input from biometric sensor 40 to reference biometric data for those modalities stored in the memory (just as Maes expressly discloses comparison of a spoken input into microphone 16 to the user's stored voice data).

[1.3] a biometric module configured to read biometric information;

142. MNC renders [1.3] obvious.

143. Maes's microphone 18 and biometric sensor 40, alternately or together, provide a "*biometric module configured to read biometric information,*" as claimed. Microphone 18 reads voice-based biometric information, while biometric sensor 40 reads other forms of biometric information.³ EX1004, 5:53-62, 10:53-61, 11:1-14.

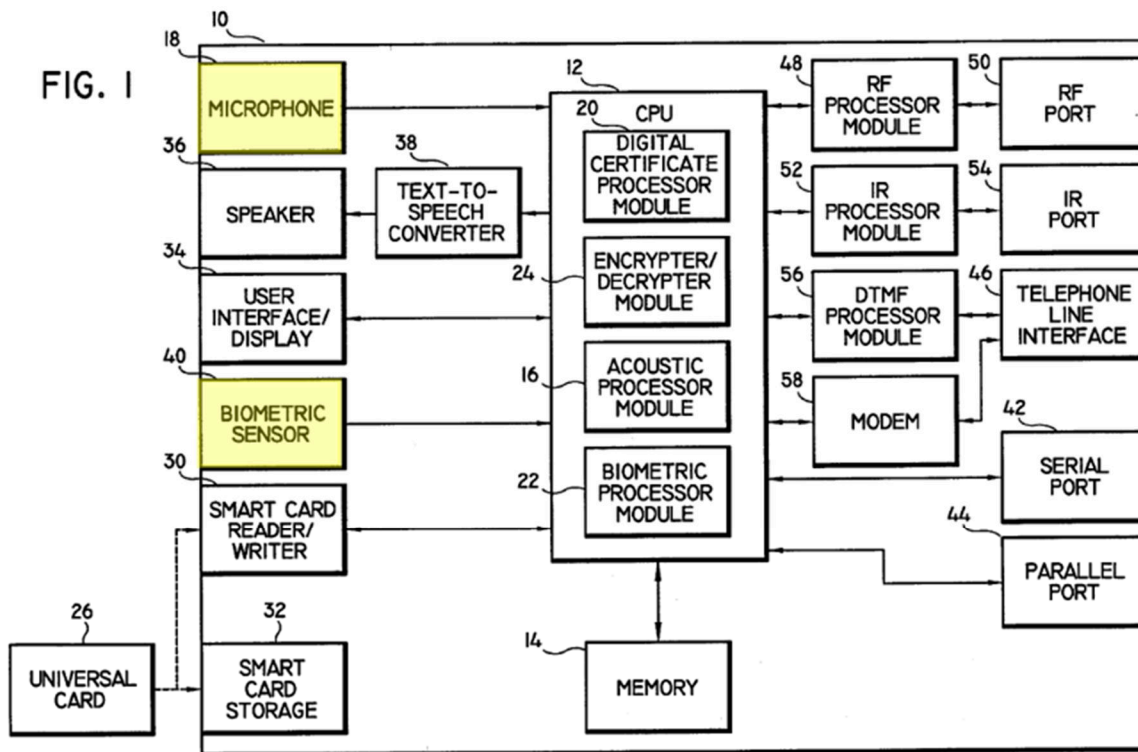
³ To the extent the claimed "biometric module" has a computational processing component, Maes further discloses that acoustic processor module 16 processes voice data read from microphone 18 and biometric processor module 22 processes other forms of biometric data read from biometric sensor 40. EX1004, 5:5-7, 5:58-62, 10:57-61. In this case, the microphone 18 together with acoustic processor module 16 and/or biometric sensor 40 together with biometric processor

144. For example, Maes explains that the PDA 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.

145. 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.*,

module 22 provide alternate mappings to the claimed “*biometric module*,” and indeed, it also would have been obvious to implement these components as a single unit since they already cooperate with each other to perform the functions disclosed in Maes. Notably, Maes confirms that its functional components can be configured and arranged in different manners within the CPU 12 or special-purpose processors may be provided for different functions. EX1004, 4:45-64, 5:17-24.

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).

[1.4] an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

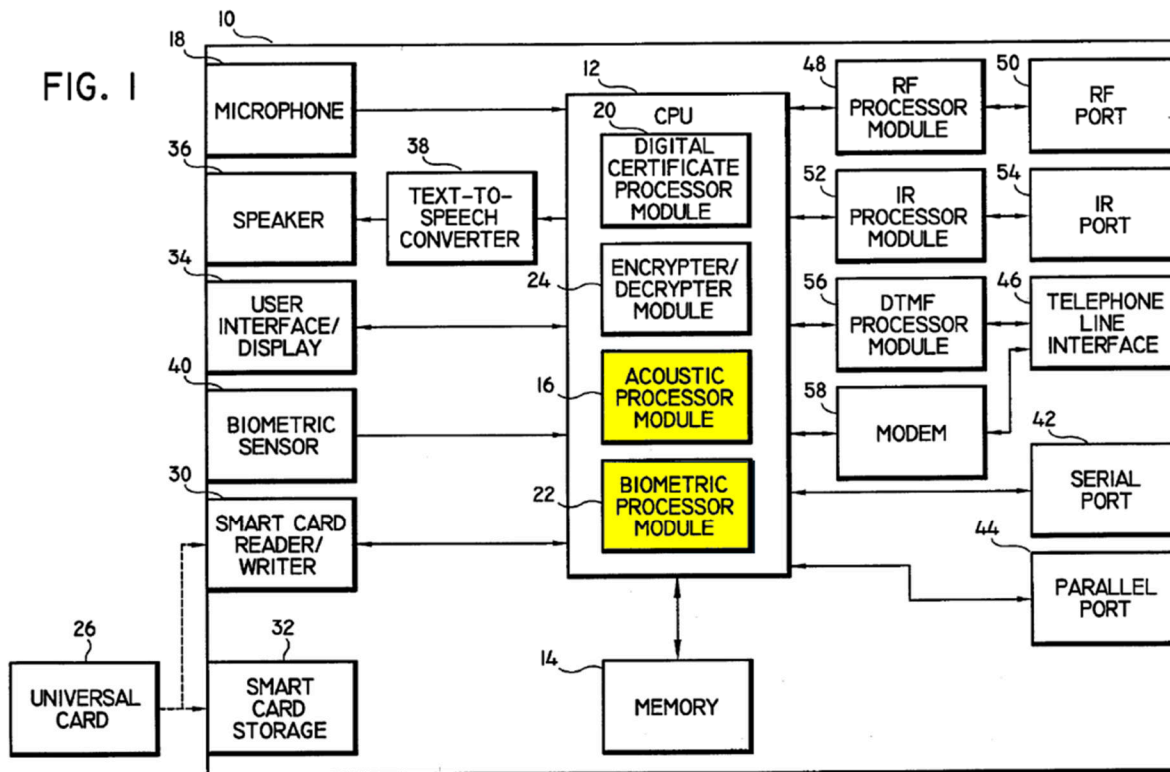
146. MNC renders [1.4] obvious.

147. Maes’s “acoustic processor module 16,” alternately or together with “biometric processor module 22,” provide an “**authentication module**” of the

mobile device.⁴ 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; *see also id.*, 5:53-63, 10:48-11:14, Fig. 5. 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.

⁴ To the extent the “authentication module” is a single unit, Maes’s modules 16 and 22 are both implemented together on CPU 12. It also would have been obvious to implement both modules 16 and 22 as a combined unit in CPU 12 since both perform similar authentication functions as described above.

148. Maes explains that voice data read from microphone 18 is “sent to the acoustic processor module 16” for comparison “with the user’s voice models stored in memory 14.” EX1004, 10:57-61; *generally id.*, 10:48-11:8, Fig. 5. Similarly, “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” EX1004, 10:66-11:8. “After 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; *see also id.*, 5:60-63.



EX1004, Fig. 1 (highlighted).

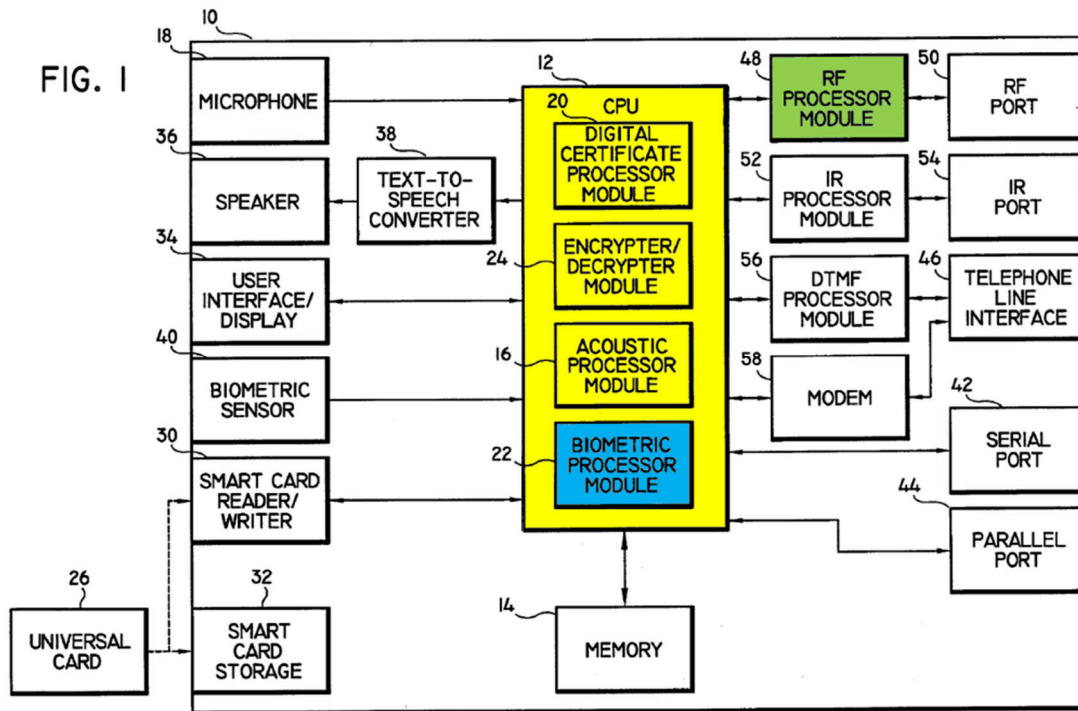
149. From these and related disclosures, a POSITA would have understood that Maes's PDA device 10 determines whether the biometric information read from the microphone 18 and/or the biometric sensor 40 corresponds to biometric authentication information stored in memory. EX1004, 6:56-7:35, 10:49-51, 14:42-46, Figs. 1, 3, 5.

[1.5.1] a secure module configured to:

150. MNC renders [1.5.1] obvious.

151. Maes's CPU 12, including encrypter/decrypter module 24, and in cooperation with RF processor module 48, provides a "*secure module*" as claimed.⁵

⁵ To the extent the "secure module" is a single unit, it would have been obvious to combine CPU 12 (including encrypter/decrypter module 24) with RF processor module 48. Both CPU 12 and RF processor module 48 are processing devices, and it was well known how to centralize processing functions on a single processing device before the Critical Date. *Id.* Maes acknowledges that different processing functions may be separated or combined. its functional components can be configured and arranged in different manners within the CPU 12 or special-purpose processors may be provided for different functions. EX1004, 4:45-64, 5:17-24. Combining these processing components in a single processor would have been beneficial for many implementations of MNC to reduce the hardware complexity and expense associated with separate processors.



EX1004, Fig. 1 (highlighted).

152. Maes discloses 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, Fig. 1.

153. Maes’s CPU 12 is secure. For example, the CPU 12 requires successful biometric verification and a valid digital certificate before allowing access to and transmission of the user’s financial and personal information. EX1004, 5:60-63, 12:19-23. Maes explains that CPU 12 enforces that condition on transmission, 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, 12:19-23. Maes further explains that “[t]he CPU 12 also includes ... a biometric processor module 22 for processing biometric data ... to provide user verification.” EX1004, 5:8-14. This verification precedes access to the information held on the PDA, as biometric 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.” EX1004, 5:60-63.

154. Maes’s CPU 12 including encrypter/decrypter module 24, in cooperation with RF processor module 48, performs the operations recited in [1.5.2] through [1.5.5] for reasons addressed further below. *Infra*; [1.5.2]-[1.5.5]; EX1004, 5:1-4, 5:14-17, 6:9-14, 12:63-65. Maes thus provides a “secure module” at least to the same extent as disclosed in the ’187 Patent itself. Cf. EX1001, 14:32-34, 14:55-60 (’187 specification providing the security-related functions in a chip including a security management unit and a cryptographic block (but never expressly naming any component as a “secure module”)).

[1.5.2] generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

155. MNC renders [1.5.2] obvious.

156. Maes’s PDA generates an “authorization number” when the user is biometrically authenticated. EX1004, 5:60-63; 12:43-49, 12:63-65. According to

Maes, “[t]he merchant can verify that local verification of the user has been properly obtained” by transmitting the “authorization number to [a] central server 60.” EX1004, 12:55-13:1. “Since 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 id.*, 6:56-7:35, Fig. 3.

157. Maes’s “authorization number” provides a “key” as claimed.⁶ Indeed, Maes discloses that the “authorization number” (key) is derived from a digital certificate and generated by the PDA when the biometric information (e.g. voice,

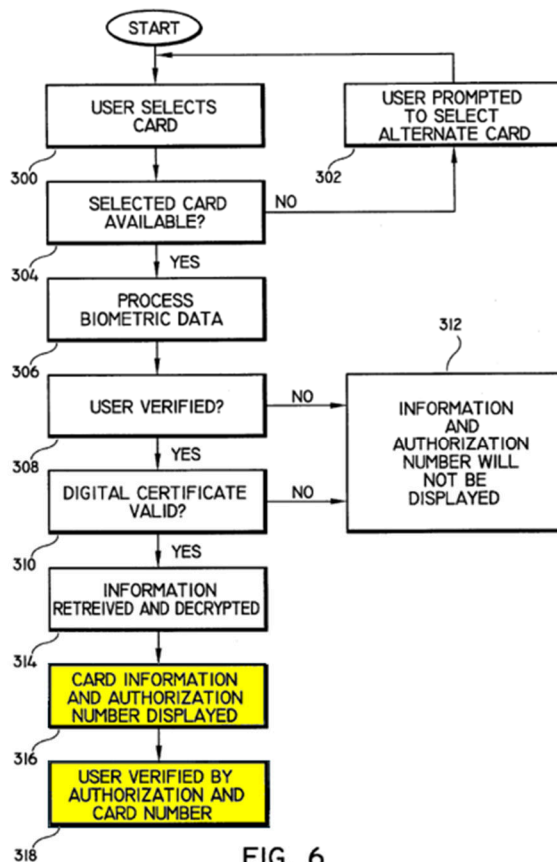
⁶ The ’187 Patent specification never expressly identifies any “key” that meets all the claimed functions, including being (i) generated when the read biometric information is determined to correspond to stored biometric authentication information (Element [1.5.2]), (ii) encrypted (Element [1.5.3]), (iii) provided for use in a transaction (Element [1.5.5]), and (iv) validated by a central database along with payment information (Element [8.8]). *See* EX1001, 2:32-39, 10:65-11:4, 12:5-18, 13:3-7, 14:55-61, 22:21-26 (describing cryptographic keys in contexts different from what is claimed). Maes’s authorization number in MNC nonetheless fulfills each of these claim requirements and functions as a key for authorizing a transaction. EX1004, 6:47-55, 12:30-13:5.

fingerprint, or other biometric input) read by the biometric reading device (e.g., microphone 18 or biometric sensor 40) is determined by the authentication module (e.g., acoustic processor module 16 or biometric processor module 22) to correspond to the biometric authentication information (e.g., reference voice data or other reference biometric data) stored in memory (e.g., memory 14). EX1004, 12:63-13:5 (“the merchant will be requested to provide the authorization number (which is generated upon user verification), in addition to the expiration date of the credit card ... [s]ince the authorization number is a function of the unexpired digital certificate that was obtained ... in the client/server mode, the central server 60 inform the merchant that the user was properly verified”), 6:42-55 (“an authorization number, which is unique to the current digital certificate, will be displayed on the PDA device 10 upon user verification”), 12:30-39 (“a merchant can confirm that the user passed local verification by using ... an authorization number which is based on the current valid digital certificate and generated upon user verification”), 14:47-67 (“User B then obtains the authorization number produced by the PDA device of User A upon local verification”).

158. For instance, Maes discloses that “if the user is biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314).” EX1004, 12:40-47; *see also id.*, Figs. 5-6. “The desired credit card

information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316)” and is “communicated to the merchant in order to process the transaction.” EX1004, 12:47-54. “If the selected card information corresponds to a credit card that was previously enrolled (*i.e.*, registered) with the service provider” the merchant will “upon transmitting the selected card information ... be requested to provide the authorization number (which is generated upon user verification), in addition to the expiration date of the credit card.” EX1004, 12:61-66. And, “[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 inform the merchant that the user was properly verified (step 318).” EX1004, 13:1-5. Maes makes clear that the authorization number is a precondition to approval of a requested transaction because when the merchant transmits the selected card information to the financial institution, “the merchant will be requested to provide the authorization number (which is generated upon user verification), in addition to the expiration date of the credit card.” EX1004, 12:63-66. The merchant obtains that number by transmitting it to the central server 60, which confirms that the user was properly verified, EX1004, 12:66-13:5, so that even though the financial institution renders the ultimate authorization decision and the service provider uses the authorization number to verify the user, the transaction is not ultimately approved unless the

authorization number is generated upon user verification and supplied to the financial institution.



EX1004, Fig. 6 (highlighted).

159. In MNC, Maes's CPU 12—an aspect of the “*secure module*” (*supra*, [1.5.1]) —generates the authorization number (*key*). EX1004, 5:1-4, 12:63-65. This would have been understood or at least obvious to a POSITA since “[t]he heart of the device is [the] 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.

[1.5.3] encrypt the key

160. MNC renders [1.5.3] obvious.

161. Maes's authorization number provides a "key" generated by the PDA upon biometric verification of the user. EX1004, 12:43-49, 12:63-13:5; *supra*, [1.5.2], *supra* §VII.D.

162. Further, Niwa describes a "[d]ata transfer ... conducted between [a] fingerprint identification device 50 (or other fingerprint identification circuitry if employed) and [a] provider of goods and/or services 60, 62 or 64 (action 112)." EX1005, 5:63-67; *see also* [1.5.5], *infra*. "The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address." EX1005, 5:67-6:4. "Most preferably, the data of this transfer are in encrypted form." EX1005, 5:63-6:4; *see also id.*, 2:38-47, 4:42-47, 4:59-63, 7:47-52, 8:44-49, 10:12-14.

163. As described above in the combination overview, MNC implements Maes's system in accordance with Niwa's suggestion for transmitting payment information and an authorization number (analogous to Niwa's authentication code) for a secured transaction from a user device over a common electronic channel, such that Maes's PDA would transmit the selected card information and authorization number to a POS terminal over the RF link. *Supra*, §VII.D. Further, per Niwa, to improve security and prevent unauthorized access to underlying

information used in the transaction, it would have been obvious for the data transferred from the PDA including the selected card information and the authorization number (key) “are in encrypted form.” EX1005, 5:63-6:4; see also id., 2:38-47, 4:42-47, 4:59-63, 7:47-52, 8:44-49, 10:12-14. A POSITA would have known how to encrypt information for transmission over the RF link, and would have recognized the security benefits of doing so, as Maes relatedly teaches that information transmitted over an RF link including information “containing unique identifying information pertaining to the consumer” can be encrypted in an RF transmission. EX1004, 13:24-38.

164. In MNC, a POSITA would have understood that Maes’s encrypter/decrypter module 24 (a component of Maes’s CPU 12 and the “*secure module*” (*supra*, [1.5.1])) would encrypt information for the transaction that is to be transmitted from the PDA. EX1004, 5:14-17; EX1005, 6:3-4. At the very least, it would have been obvious for encrypter/decrypter module 24 to perform this function since Maes identifies encrypter/decrypter module 24 as providing encryption services to the PDA. EX1004, 5:14-17.

[1.5.4] [encrypt] ... the payment information stored in memory; and

165. MNC renders [1.5.4] obvious.

166. Maes explains that “[t]he CPU 12 further includes an encrypter/decrypter module 24” (an aspect of the “*secure module*” (*supra*, [1.5.1]))

“for encrypting the personal and financial information before being stored in memory 14 and for decrypting such information when accessed by the user.”

EX1004, 5:14-17, Fig. 1.

167. Thus, Maes discloses and renders obvious encrypting the payment card information (*payment information*) stored in memory. EX1004, 5:14-17.

[1.5.5] provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

168. MNC renders [1.5.5] obvious.

169. Maes discloses 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 RF port 50).” EX1004, 12:10-15; *see also id.*, 13:34-38 (transmit “via ... RF”)⁷, 3:33-36; 6:6-14; 8:6-8; 8:8-14; 12:5-29; 12:14-17; 14:59-65, 12:5-29, Figs. 1, 5, 6.

⁷ At col. 13:34-38, Maes states that the selected card information and encrypted information file “would be transmitted to the POS terminal (via the Universal Card, RF or IR).” In Maes, only the PDA device (not the Universal Card) has RF transmission capabilities. *See e.g.*, EX1004, 6:6-14, 12:5-29, Fig. 1.

170. Maes also discloses conveying the “authorization number” to the merchant “in order to process the transaction.” EX1004, 12:43-54 (“When operating the PDA device 10 in the local mode, if the user is biometrically verified (step 308) and the PDA device 10 contains an unexpired digital certificate (step 310), the selected card information is retrieved from memory 14 and decrypted (step 314). The desired credit card information, as well as an authorization number, is then displayed on the user interface/display 34 (step 316). This information can then be verbally communicated to the merchant in order to process the transaction.”), 12:66-13:5 (“The merchant will then transmit ... the displayed authorization number to the central server 60.”), Fig. 6.

171. Like Maes, Niwa discloses a “[d]ata transfer ... conducted between [a] fingerprint identification device 50 (or other fingerprint identification circuitry if employed) and [a] provider of goods and/or services 60, 62 or 64 (action 112).” EX1005, 5:63-67; *see also* [1.5.5], *infra*. “The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address.” EX1005, 5:67-6:4; *see also id.*, 2:38-47, 4:42-47, 4:59-63, 7:47-52, 8:44-49, 10:12-14.

172. Niwa’s authentication code is analogous to Maes’s authorization number. Indeed, both are generated only if the user successfully passes biometric authentication, and both are used by the payor bank or similar financial institution

to assess the legitimacy of a transaction request and to determine whether to authorize the requested transaction. EX1005, 6:23-26; EX1004, 12:30-13:5. Niwa further teaches that the authentication code can be electronically transferred and provided to the merchant together with other payment information for a transaction. EX1005, 6:48-58.

173. As described above in the combination overview, MNC implements Maes's system in accordance with Niwa's suggestion for transmitting payment information and an authorization number (analogous to Niwa's authentication code) for a secured transaction from a user device over a common electronic channel, such that Maes's PDA would transmit (in encrypted form) the selected card information (payment information) and authorization number (key) to a POS terminal over the RF link (via the short range RF circuitry). Supra, §VII.D; EX1004, 12:5-29, 13:33-38.

173A. Maes describes RF transmission of data for a transaction in two separate places, each corresponding to a different implementation of Maes's transaction framework. The first is at EX1004, 12:5-29. There, Maes teaches 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," and that "the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the

ATM or 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, 12:5-8, 12:10-16. Maes is explicit about what this substitution means, stating that in this implementation “the PDA device 10 itself actually takes the place of the Universal Card 26.” EX1004, 12:24-25. Maes then describes the authorization-number implementation, in which, for transactions processed with a mechanical sweeper or conducted remotely, “a merchant can confirm that the user passed local verification by using the unique Universal Card number 27 (FIG. 2) together with an authorization number which is based on the current valid digital certificate and generated upon user verification.” EX1004, 12:35-39. The authorization number and card information are displayed on the PDA and “can then be verbally communicated to the merchant in order to process the transaction,” EX1004, 12:47-51, after which “[t]he merchant will then transmit the Universal Card number 27 and the displayed authorization number to the central server 60,” which confirms to the merchant that the user was properly verified. EX1004, 12:66-13:5. Because the PDA in the RF implementation stands in for the Universal Card, a POSITA would have understood that the data the Universal Card would otherwise convey to the terminal, including both the selected card information and the unique Universal Card number 27, would instead be transmitted by

the PDA itself over RF. Accordingly, when Maes's authorization-number implementation is adapted so that the PDA transmits to the POS terminal via RF, it would have been obvious to transmit the Universal Card number 27 along with the selected card information, permitting the user to be verified in exactly the manner Maes already describes. The verification performed by the central server is the same whether the Universal Card number and authorization number reach the merchant verbally, by mechanical imprint, or by RF, and only the manner of conveyance differs.

173B. The second place Maes describes RF transmission is EX1004, 13:19-38, which sets out a variation affording "an additional level of security for user verification, whereby the financial institution (e.g., credit card company) can verify the identity of the consumer during a purchase transaction." EX1004, 13:20-24. In that variation, the PDA downloads the selected card information in encrypted form "as well as an encrypted file containing unique identifying information pertaining to the consumer," such as the consumer's name and account number, and "[t]he selected card information, as well as the encrypted information file, would be transmitted to the POS terminal (via the Universal Card, RF or IR) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details." EX1004, 13:30-31, 13:34-38. The financial institution, which "would possess the requisite key (provided by the service provider upon

enrollment),” decrypts “the transmitted information to verify the identity of the user” and then “provide[s] an authorization number for the transaction to the merchant if the consumer was verified.” EX1004, 13:53-58. A POSITA would have recognized that the authorization number of EX1004, 12:35-13:5 and the encrypted information file of EX1004, 13:29-38 serve similar functions in Maes’s framework. Each is a vehicle by which a party remote from the point of sale, whether the service provider’s central server 60 in the first instance or the processing financial institution in the second, confirms the identity of the user before the transaction is authorized. A POSITA would therefore have understood that either the authorization number, the encrypted information file, or both could be transmitted over the RF link to accomplish that remote verification. Each carries its own strengths, in that the authorization number is compact, is tied to an unexpired digital certificate, and is verified through the service provider the PDA is already enrolled with, while the encrypted information file carries richer identifying data that only the keyholding financial institution can read. Selecting between them is precisely the sort of ordinary design choice a POSITA would have made in implementing Maes, with predictable results either way. Further, it was well known in the art to verify a user with multiple pieces of information rather than one, and Maes itself repeatedly endorses layering verification mechanisms. *See, e.g.*, EX1004, 12:35-39 (unique Universal Card number 27 used “together with an authorization number”). A POSITA

would thus have found it obvious to transmit either or both the authorization number and the encrypted information file over the RF link.

174. Additionally, before the Critical Date, radio-frequency readers were known and in use at point-of-sale systems. For example, Shults describes an identification apparatus that is “scanned at a point-of-sale system with an RFID or barcode reader,” so that “the appropriate identity is provided to the point-of-sale system.” EX1008, Abstract. In Shults, the apparatus includes “a radio-frequency identification (RFID) circuit 104” having a “receive antenna 202, which receives an appropriately coded interrogation signal from an electronic scanner at a point of sale system.” EX1008, [0030]. Shults distinguishes that electronic scanner from an optical one, explaining that “where customers or users traditionally have distant contact with the point-of-sale system (such as a gasoline station) an electronic scanner may be appropriate.” EX1008, [0038]. Shults claims a scanner comprising “a radio-frequency transmitter” and “a radio-frequency receiver, the transmitter and receiver to interrogate the identification apparatus.” EX1008, claim 23.

Raspotnik likewise discloses “point of sale reader/writers 14a that are used in entrance gates, and vending machines, and the like, that are accessed by the transponder 11.” EX1039, 4:14-17. Raspotnik explains that such a reader/writer “communicates with the transponder 11 by means of an RF link comprising an RF antenna 17 and the RF antenna 16 in the transponder 11.” EX1039, 4:8-10. A

POSITA would therefore have understood that a point-of-sale device could be equipped with a radio-frequency reader to receive information transmitted from a user's portable device.

175. Before the Critical Date, it was well known for a portable device to verify its user locally, generate a code reflecting that verification, and transmit the code to a transaction terminal over a short-range wireless link. For example, Lewis describes a portable card in which “the biometric identification device is preferably on board the card, rather than contained in the ATM machine.” EX1038, 5:31-33. Lewis explains that “[i]f the spontaneous profile calculated by verifying means 2 matches ... then the verifying means 2 generates a ‘Positive ID’ signal on signal line 3.” EX1038, 8:13-18. Lewis further explains that “Code generator 5 transforms the user’s unique identification profile into a specific code,” and that “in ATM applications, the code generator would convert the user’s unique identification profile into a four digit numeric personal identification number (PIN) code.” EX1038, 8:38-39, 8:45-48. In Lewis, the “remote control unit 13 may remotely send information on signal line 3, which includes the ‘positive ID’ ... signal and/or the unique access number (e.g. identification number, PIN code, etc.) created from the user’s unique identification profile.” EX1038, 9:48-52. Lewis discloses that “account specific information” is sent “via infrared, microwave, or other such signal,” and “may be received and processed by the secure objective (e.g. ATM

machine ...).” EX1038, 9:44-47. Because the microwave band falls within the range of frequencies at which electromagnetic energy is radiated and received as radio waves, a POSITA would have understood microwave transmission to be a form of radio-frequency transmission. At least because Lewis states that remote control unit 13 is used “from a remote location (for example, as a key pass, or a user specific car alarm remote control key, or even highly interactive functions such as remote control use at an ATM machine),” a POSITA would have understood that Lewis’s transmissions to a transaction terminal occur over a short range. EX1038, 9:38-42. These references corroborate the advanced state of art as of the Critical Date and confirm that a POSITA would have understood that sending a code such as Maes’s authorization number, and other information in a transaction, from a user’s portable device to a transaction terminal over a short-range radio-frequency link would have been obvious according to well-known prior art techniques.

176. Establishing an RFID connection between a fob-type device and a reader was well known in the payment context before the priority date of the patents-in-suit. For example, the Berardi provisional (EX1036), filed July 10, 2001, explains that “the key fob utilizes RFID (radio frequency identification) to communicate wirelessly,” and that “[a] user will wave a transponder in front of a reader; the reader will decrypt the account information on the chip and send it to

the POS (point of sale).” EX1036, p. 3:22–24. This disclosure was included in the Berardi published application (EX1037), which claims priority to EX1036 and states that “the operation of system 100A may begin when fob 102 is presented for payment, and is interrogated by RFID reader 104,” after which “the transponder 102 may provide the transponder identification and/or account identifier to the RFID reader 104 which may further provide the information to the merchant system 130 POS device 110.” EX1037, [0032]. The Berardi application further explains that “[t]he system may further include a RFID reader configured to send a standing RFID recognition signal which may be transmitted from the RFID reader via radio frequency (or electromagnetic) propagation,” and that “[t]he fob may be placed within proximity to the RFID reader such that the RFID signal may interrogate the fob and initialize fob identification procedures.” EX1037, [0014]. The Berardi application likewise describes that “the RFID reader sends out an interrogation signal to scan for the presence of fob 102,” after which “the customer... may present the fob 102 for payment... and the fob 102 is activated by the RF interrogation signal provided.” EX1037, [0086]. Because Berardi's signal exchange necessarily precedes and enables the transponder identification and account data transfer described above, a POSITA would have understood the reader's transmission of a recognition or interrogation signal and the fob's corresponding activation and

response with its identifying information establish a connection between the reader and the fob.

177. RFID connections were also known outside the payment context. For example, Fujioka (EX1035) describes a non-contact IC card system in which “a non-contact type IC card is used as a commuter pass for train, and it is checked whether or not the commuter pass is valid based on data transmission between the IC card and a read/write apparatus disposed at a ticket gate.” EX1035, 1:9–13. Fujioka explains the connection sequence itself: “the read/write apparatus transmits a read identifier command to the IC card[; a]fter receiving the read identifier command, the IC card transmits an identification code inherent in the IC card to the read/write apparatus.” EX1035, 1:17–20. Fujioka's claim 3 similarly recites “an IC card for communicating with a read/write apparatus” having “identification code collating means, for when an identification code is sent together with a command from the read/write apparatus, collating the identification code with the identification code stored in the memory.” EX1035, 13:19–27. Because Fujioka describes operating a communication link between the read/write apparatus and the IC card, a POSITA would have understood that such a connection was established.

178. In MNC, CPU 12 in coordination with RF processor module 48 (aspects of the “*secure module*” (*supra*, [1.5.1])) are configured to perform operations for providing the selected card information and authorization number to

the POS terminal over the RF link. For example, Maes explains that CPU 12 is coupled to the RF port 50 through RF processor module 48. EX1004, 6:9-14 (“[T]he device may preferably be equipped with an RF processor module 48, operatively connected between the CPU 12 and an RF port 50, ... for generating transmission signals which are outputted from the RF port 50.”). EX1004, 6:9-14, Fig. 1; *see also id.*, 5:1-4, 6:9-14, 12:19-23.

[2] The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

179. MNC renders [2] obvious.

180. As explained at [1.3], Maes’s *biometric module* (microphone 18 and/or biometric sensor 40) is configured to read biometric information. *Supra*, [1.3].

181. Per Maes, in MNC, the biometric information is read in a local mode of operation that Maes describes as “performed to initiate a consumer transaction,” and that “is commenced by the user selecting a pre-enrolled credit card that is stored in memory 14.” EX1004, 3:53-54, 10:30-32, Figs. 1, 5.

182. Maes further explains that biometric verification governs whether the selected card information reaches the transaction terminal, 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, 12:19-23. Maes's authorization number is also only generated and made available for a transaction if the user has been biometrically verified, and the authorization number is used by the central server in the process of completing a transaction. EX1004, 12:34-39, 12:55-13:5, Fig. 6.

183. From these and related descriptions, a POSITA would thus have understood that Maes's *biometric module* reads biometric information provided by a user to complete the transaction. EX1004, 10:30-32, 12:19-23.

[3] The mobile device of claim 1, wherein the payment information is associated with a primary account number.

184. MNC renders [3] obvious.

185. As explained at [1.2], Maes's selected card information is *payment information* as claimed. *Supra*, [1.2]. The selected card information can include information regarding a pre-enrolled credit card that the user selects for the transaction. EX1004, Abstract ("selecting one of the pre-enrolled credit cards that are stored in the PDA"); 2:23-30 ("a user can store his or her credit card ... (*i.e.*, financial) information"), 4:1-11, 6:61-67, 11:51-57.

186. Maes describes enrolling such a card by "providing the service provider with the user's credit card ... information." EX1004, 6:64-65. And Maes recognizes that a payment card carries an account number, referring to "the account number provided on a credit card ..." EX1004, 6:40-41.

187. A POSITA would have understood the account number carried on the user's selected card — the number identifying the cardholder's account — to be associated with that card's "primary account number" (PAN), the standard term in the payment-card art for the account number carried on a payment card (corroborated by EX1021, 1:17-21 ("[R]emote banking generally involves the use of magnetic stripe cards, together with cheques or cash. The cards are encoded with information identifying holders of the cards. The information stored on the card is typically a primary account number (PAN)."); EX1022, 1:66-2:2 ("a Primary Account Number (PAN), [] is the embossed number on the card. The embossed number on the card is also stored on the magnetic stripe of the card"))).

[4] The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device.

188. MNC renders [4] obvious.

189. As explained at [1.5.5], in MNC, CPU 12 in coordination with RF processor module 48 (aspects of the "***secure module***" (*supra*, [1.5.1])) provide the encrypted authorization number (***encrypted key***) and the selected card information (***payment information***) via the short range RF circuitry (*e.g.* including RF port 50). *Supra*, [1.5.1], [1.5.5].

190. Maes further explains that the recipient of the PDA's RF transmission is a POS terminal, stating 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)” EX1004, 12:10-16.

191. From these and related descriptions, a POSITA would have understood that MNC’s CPU 12 in coordination with RF processor module 48 (aspects of the “*secure module*” (*supra*, [1.5.1])) are configured to provide the encrypted authorization number (*encrypted key*) and the selected card information (*payment information*) via the short range RF circuitry to a *POS device*.

[5] The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

192. MNC renders [5] obvious.

193. As an initial matter, the “stored separately” limitation in claim 5 cannot mean that the biometric authentication information and the payment information are stored in separate memories because claim 5 depends from claim 1, and [1.2] requires that both pieces of information be stored in the same “memory.”⁸ *Supra*, [1.2]. It is sufficient, therefore, that the biometric

⁸ Related U.S. Patent No. 10,706,412 similarly recites in claim 1 “a memory ... configured to store biometric authentication information and payment

authentication information and the payment information be stored separately in the same memory, such as in logically distinct regions of, or under distinct access controls, within that memory. This is consistent with the specification of the '187 Patent, which discloses a security-management unit and cryptographic block that gate access to memory using cryptographic keys (*see* EX1001, 2:32-37, 10:65-11:4, 14:55-60, 22:22-26), and describes that information contained on the RF device is “protected by sundry cryptographic methods” (*id.* at 8:38-39), indicating that different categories of sensitive data can be logically segregated within a single memory such as through distinct access-control or cryptographic regimes. The specification nowhere discloses physically distinct memory chips for the biometric and payment information.

194. In MNC, per Maes, biometric authentication information includes the user’s voice data or other biometric data, which Maes stores in memory 14. EX1004, 10:59-61 (“comparing the current biometric voice data with the user’s voice models stored in memory 14”), 5:53-62 (describing alternative forms of

information,” and recites in dependent claim 3 “wherein the biometric authentication information is stored separately from the secured payment information.” EX1023, cls. 1, 3. This further evidences that “stored separately” in the '187 Patent family does not require storage in separate memory devices.

biometric data). The payment information, *e.g.*, the user's encrypted card information, is likewise stored in memory 14. EX1004, Abstract ("a memory for storing financial and personal information of the user"), 2:60-66, 3:20-24, 5:1-4, 5:14-17, 7:1-7; 11:24-29, 12:44-47; *supra*, [1.2].

195. A POSITA would have understood that Maes's voice data or alternate biometric data (*biometric authentication information*) and its encrypted card information (*payment information*) are stored in different locations of memory and are therefore "*stored separately*" from one another as recited in claim 5. Indeed, the encrypted financial/card information and the biometric data would be stored separately in distinct locations of the memory to enable them to be accessed separately for their distinct purposes as described in Maes.

196. Maes also discloses cryptographic separation of the payment information from the biometric authentication information within memory 14. In particular, Maes discloses that "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, 5:14-17. The card information is thus stored in memory 14 in encrypted form, protected by "an encryption key unique to the PDA device 10." EX1004, 11:27-32. The biometric authentication data, such as the user's voice data and any fingerprint, palm print, handwriting, or retinal templates, is not described

as being encrypted under that same key or protected under the same regime. Maes discloses that the biometric authentication data is instead accessed through a distinct processing path via the acoustic processor module 16 or the biometric processor module 22 for the purpose of user verification. EX1004, 5:1-17, 5:53-62, 11:9-14. The payment information and the biometric authentication information are therefore stored under distinct access-control regimes within memory 14.

197. Additionally, Maes discloses that access to the payment information is gated by an additional layer of protection in the form of the digital certificate that does not gate access to the biometric authentication information. Under Maes's architecture, biometric verification alone is not sufficient to access the stored card information. The PDA device 10 also requires a valid, unexpired digital certificate stored in memory 14, which is separately decrypted by the encrypter/decrypter module 24 and validated by the digital certificate processor module 20 before the encrypter/decrypter module 24 will retrieve and decrypt the card information. EX1004, 7:42-54, 11:16-32. Biometric verification, by contrast, is performed directly against the stored voice data or biometric data without need for a valid digital certificate. EX1004, 11:9-14; Fig. 5 (steps 206-212). This access-control architecture further demonstrates how the payment and biometric information are “*stored separately*” within Maes's memory 14.

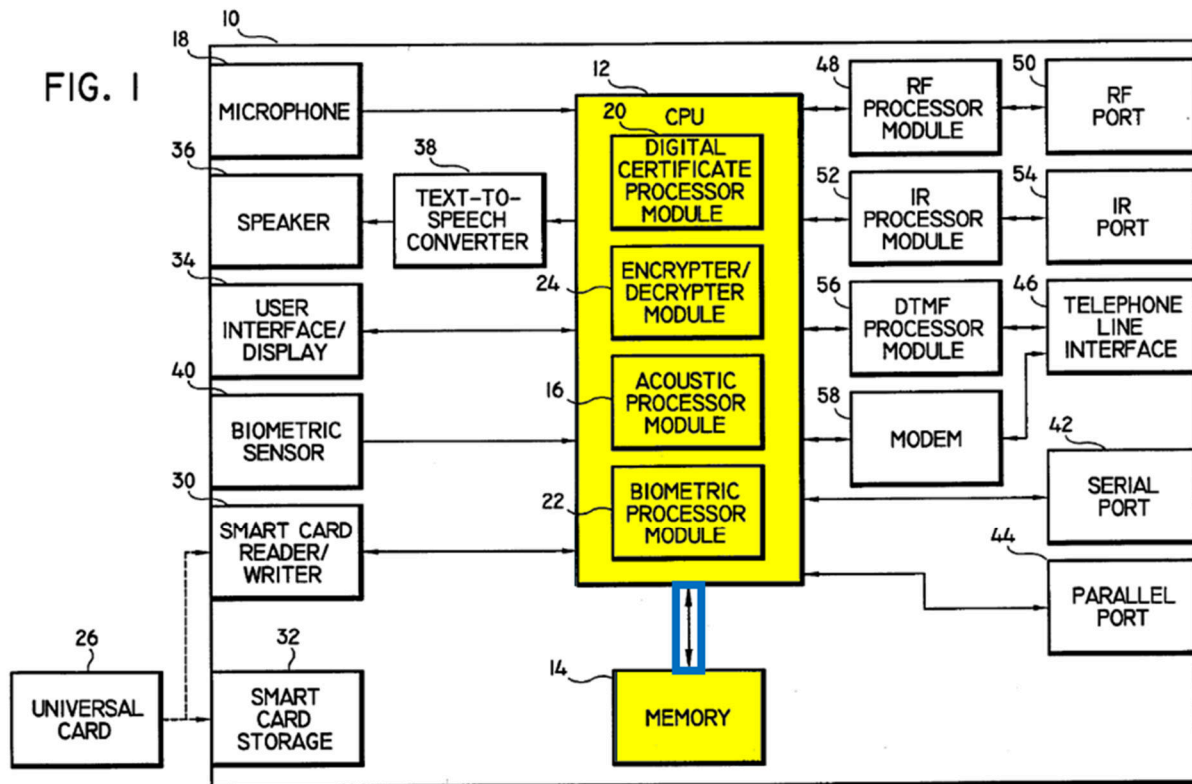
[6] The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

198. MNC renders [6] obvious.

199. In MNC, the payment information is stored in memory 14. *See* [1.2], *supra*.

200. In MNC, that memory is accessible by the CPU 12 (aspect of the “***secure module***” (*supra*, [1.5.1])). For example, Maes explains that “[t]he CPU 12 then searches the memory 14 for the desired information (step 202)” and that “the requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24.” EX1004, 10:44-45, 11:27-29.

201. Maes’s Fig. 1, reproduced below, illustrates memory 14 connected to CPU 12 and to no other device 10 component. EX1004, Fig. 1.



EX1004, Fig. 1 (highlighted).

202. Maes further describes various restrictions on access to financial or card information stored in memory 14. For example, the financial information is encrypted by the encrypter/decrypter module 24 using an encryption key unique to the PDA device 10, and is decrypted through that module before use. EX1004, 5:14-17, 11:26-29. Additionally, biometric verification is required “prior to accessing the financial and personal information stored in memory 14.” EX1004, 5:58-62. Moreover, a valid, unexpired digital certificate is independently required, and even a successfully verified user cannot access the financial information without one. EX1004, 3:63-4:2, 11:23-25. Maes then expressly prohibits the CPU

12 from retrieving and transmitting the financial information unless both the biometric verification and digital certificate checks succeed, 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.” EX1004, 12:20-25.

203. From these and related descriptions, a POSITA would have understood that MNC’s card information (*payment information*) is stored in a memory 14 (*memory*) accessible only by CPU 12 (aspect of the “*secure module*”).

[8.pre] A system, comprising:

204. MNC, per Maes, discloses a “*system*” comprising a PDA (*mobile device*), point-of-sale (POS) transaction terminal (*POS device*), and central server 60 with servers of a financial institution 70 (*central database*). *Supra*, [1.pre]; *infra*, [8.1], [8.7.1], [8.8].

[8.1] a mobile device, comprising:

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

[8.2] short range radio frequency (RF) circuitry;

206. *Supra*, [1.1].

[8.3] memory configured to store biometric authentication information and payment information;

207. *Supra*, [1.2].

[8.4] a biometric module configured to read biometric information;

208. *Supra*, [1.3].

[8.5] an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

209. *Supra*, [1.4].

[8.6.1] a secure module configured to:

210. *Supra*, [1.5.1].

[8.6.2] generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

211. *Supra*, [1.5.2].

[8.6.3] encrypt the key

212. *Supra*, [1.5.3].

[8.6.4] [encrypt] ... the payment information stored in memory; and

213. *Supra*, [1.5.4].

[8.6.5] provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

214. *Supra*, [1.5.5].

[8.7.1] a point of sale (POS) device configured to:

215. MNC renders [8.7.1] obvious.

216. For example, per Maes, the merchant's POS terminal (***POS device***) is configured to receive, process, and transmit information electronically for a transaction. *See e.g.*, EX1004, 12:5-8, 12:10-18, 13:34-38, Fig. 3.

[8.7.2] receive, from the secure module, the encrypted key and payment information; and

217. MNC renders [8.7.2] obvious.

218. Maes discloses 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, 12:10-16; *generally id.*, 12:5-29, Figs. 1, 5, 6.

219. For the reasons addressed in detail above (*supra*, §VII.D), a POSITA would have found it obvious to apply Niwa’s suggestion for electronically transferring an authorization number to Maes’s system such that Maes’s PDA would transmit not only the selected card information (payment information) but also the authorization number (key) to the POS device for use in a transaction via Maes’s short-range RF circuitry. The card information and the authorization number are encrypted, as taught in both Maes and Niwa. EX1005, 6:3-4; EX1004, 13:34-38. See [1.5.3], [1.5.4], [1.5.5], *supra*.

220. Because MNC’s PDA transmits the encrypted authorization number (*key*) and the selected card information (*payment information*) using CPU 12 and RF module 48 (aspects of the “*secure module*” (*supra*, [1.5.1])) to the POS device over link L2, a POSITA would have understood that the POS device receives, from

the secure module, the encrypted key and payment information as recited in [8.7.2]. EX1004, 12:10-16; EX1005, 6:3-4; *supra*, [1.5.1], [1.5.5], [4].

[8.7.3] transmit, to a central database, the encrypted key and payment information; and

221. MNC renders [8.7.3] obvious.

222. For example, Maes discloses that “[t]he merchant will [] transmit ... the displayed authorization number to the central server 60.” EX1004, 12:65-13:5. Additionally, “[t]he selected card information ... would be transmitted to the POS terminal ... and then transmitted in encrypted form directly to the processing financial institution together with the purchase details”; *see also id.*, Fig. 3 (depicting links L3 and L4 between the transaction terminal and the central server (service provider) and financial institution, respectively), 12:55-63 (“transmitting the selected card information to the financial institution”), 11:38-40 (“sent to the proper financial institution 70”). In MNC, the POS terminal receives the authorization number directly from the PDA over an RF link, and thus transmits the authorization number to the central server 60 (rather than a human representative of the merchant calling the service provider or financial institution with the authorization number, for example). *Supra*, [1.5.5].

223. From these and related disclosures, a POSITA would have understood that MNC’s POS device transmits the selected card information (*payment information*) and the encrypted authorization number (*encrypted key*) to a *central*

database of the central server 60 and financial institution 70. *Supra*, [1.5.5]; *infra*, [8.8].

[8.8] a central database configured to validate the key and the payment information.

224. MNC renders [8.8] obvious.

225. Maes's central server 60 together with financial institution 70 provide a "central database" as claimed. To the extent the "central database" is a single entity, consolidating the functions of Maes's central server 60 and financial institution 70 into a single back-end would have been obvious. Maes does not restrict the service provider from also being the financial institution or card issuer. See EX1004, 6:34-39, 7:19-35. Indeed, the two systems already coordinate closely in exchanging cryptographic keys and enrollment data during setup, and in working together to process transaction requests. EX1004, 6:63-7:3, 12:65-13:5, 13:47-56. In this context, it would have been obvious to a POSITA to consolidate their functions into a single back-end system as a routine design choice combining familiar elements according to known methods. A POSITA also would have been motivated to combine central server 60 and financial institution 70 in a central database to achieve well known and predictable benefits of centralization, including lower overhead costs, reduced coordination costs, and reduced latency in communicating between otherwise distant systems.

226. Further, Maes discloses that central server 60 validates the authorization number (*key*) to confirm that the user was properly verified at the PDA device 10. EX1004, 12:65-13:5 (“Since 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 [can] inform the merchant that the user was properly verified.”); *see also id.*, 12:55-13:5, Fig. 3. Financial institution 70 validates the transmitted card information (*payment information*) by decrypting it using an account-specific key and returns an authorization to the merchant if the user is verified, completing the secured transaction. EX1004, 13:47-56.

[9] The system of claim 8, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

227. *Supra*, [2].

[10] The system of claim 8, wherein the payment information is associated with a primary account number.

228. *Supra*, [3].

[11] The system of claim 8, wherein the POS device includes an RF reader.

229. MNC renders [11] obvious.

230. For example, Maes discloses that the PDA and POS device communicate over an RF link, and that the PDA transmits information for a transaction received by the PDA via RF. EX1004, 12:5-8, 12:10-15, 13:34-38, Abstract. From these disclosures, a POSITA would have understood the

merchant's terminal (**POS device**) to include an RF reader. Indeed, an RF reader would be inherent or obvious for the POS device to receive the information that Maes expressly discloses is transmitted to the POS device from the PDA via RF. EX1004, 12:5-8, 12:10-15, 13:34-38, Abstract.

[12] The system of claim 8, wherein the biometric authentication information is stored separately from the payment information.

231. *Supra*, [5].

[13] The system of claim 8, wherein the payment information is stored in a memory accessible only by the secure module.

232. *Supra*, [6].

[15.pre] A method for secure transactions using a mobile device, comprising:

233. *Supra*, [1.pre]; EX1004, 1:11-17 (“portable information and transaction processing system and method”), 14:18-21 (“perform the methods and functions of the present invention”).

234. More specifically, in MNC, the PDA device 10 performs the operations of [1.pre]-[6]. *Supra*, [1.pre]-[6].

[15.1] storing biometric authentication information and payment information in memory;

235. *Supra*, [1.2].

[15.2] reading biometric information using a biometric reader;

236. *Supra*, [1.3].

237. Maes's microphone 18 and biometric sensor 40 provide the *biometric reader*, for the reasons discussed at [1.3] (describing the *biometric module*). *Supra*, [1.3].

[15.3] determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

238. *Supra*, [1.4].

[15.4] generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

239. *Supra*, [1.5.2].

[15.5] encrypting the key

240. *Supra*, [1.5.3].

[15.6] [encrypting] ... the payment information stored in memory; and

241. *Supra*, [1.5.4].

[15.7] providing the encrypted key and payment information for use in a transaction.

242. *Supra*, [1.5.5].

[16] The method of claim 15, further comprising reading biometric information provided by a user to complete the transaction.

243. *Supra*, [2].

[17] The method of claim 15, wherein the payment information is associated with a primary account number.

244. *Supra*, [3].

[18] The method of claim 15, further comprising providing the encrypted key and payment information to a point of sale (POS) device.

245. *Supra*, [4].

[19] The method of claim 15, wherein the biometric authentication information is stored separately from the payment information.

246. *Supra*, [5].

[20] The method of claim 15, wherein the payment information is stored in a memory accessible only by a secure module.

247. *Supra*, [6].

[21] The method of claim 15, wherein the payment information is provided using a short range RF circuitry.

248. *Supra*, [1.5.5].

249. As explained at [1.5.5], in MNC, the PDA transmits the selected card information (*payment information*) to the POS terminal over the RF link (*short range RF circuitry*). *Supra*, [1.5.5], [1.1].

B. Ground 1B: Maes-Niwa-Shults Renders Obvious Claims 7 and 14

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

250. MNSC renders [7] obvious.

251. In MNSC, the PDA device 10 (mobile device) includes short range RF circuitry (see *supra*, Ground 1A at [1.1]), and that circuitry further includes an RFID circuit consistent with Shults's teachings. *Supra*, §§VII.I-J, Ground 1A at [1.1]; EX1008, [0030].

252. Therefore, a POSITA would have understood that in MNSC, the mobile device's short-range RF circuitry comprises an RFID device. *Supra*, §VII.J; EX1008, [0030].

[14] The system of claim 8, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

253. *Supra*, Ground 1B at [7].

C. Ground 2A: Maes-Bjorn Renders Obvious Claims 1-6, 8-13, and
15-21

[1.pre] A mobile device, comprising:

254. The Maes-Bjorn Combination (“MBC”) described above (*supra*, §VII.F) renders [1.pre] obvious in view of Maes’s disclosures for at least the reasons addressed above in Ground 1A. *Supra*, Ground 1A at [1.pre].

[1.1] short range radio frequency (RF) circuitry;

255. *Supra*, Ground 1A at [1.1].

[1.2] memory configured to store biometric authentication information and payment information;

256. MBC renders [1.2] obvious.

257. *As discussed, per Maes, the memory of the PDA (mobile device) is configured to store credit card information (payment information) for use in transactions. EX1004, 5:8-24, 7:1-7; supra*, Ground 1A at [1.2].

258. Further, in MBC, per Bjorn, the information stored in memory further includes a “fingerprint template” representing an authorized user’s fingerprint

scan. EX1006, 4:21-24 (“At block 320, a template is created for the user.”), 4:47-53 (“At block 335, the template is stored.”), Fig. 3; *see also* 5:31-39, 5:49-54, Fig. 4. Bjorn describes various information that can be included in the fingerprint template, each of which renders obvious the claimed “biometric authentication information,” including “a digital image of the fingerprint.” EX1006, 8:32-34; *see also* EX1006, claim 20 (“comparing the fingerprint image to the fingerprint template”).

[1.3] a biometric module configured to read biometric information;

259. *Supra*, Ground 1A at [1.3].

[1.4] an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

260. *Supra*, Ground 1A at [1.4].

261. In MBC, Bjorn corroborates the obviousness of [1.4]. For example, Bjorn describes a processor that authenticates a user by comparing data from a current scan of the user’s fingerprint to a stored template, and determining whether they match. EX1006, 4:64-5:9 & Fig. 3 (steps 345, 350), 5:65-6:10 & Fig. 4 (steps 455, 460).

[1.5.1] a secure module configured to:

262. *Supra*, Ground 1A at [1.5.1].

[1.5.2] generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

263. MBC renders [1.5.2] obvious.

264. Bjorn describes generating a cryptographic key (*key*) in response to authentication. For example, as shown in Fig. 3, Bjorn discloses key generation at step 355 in response to determining a match between the user's current fingerprint and fingerprint data of an authorized user in a stored template:

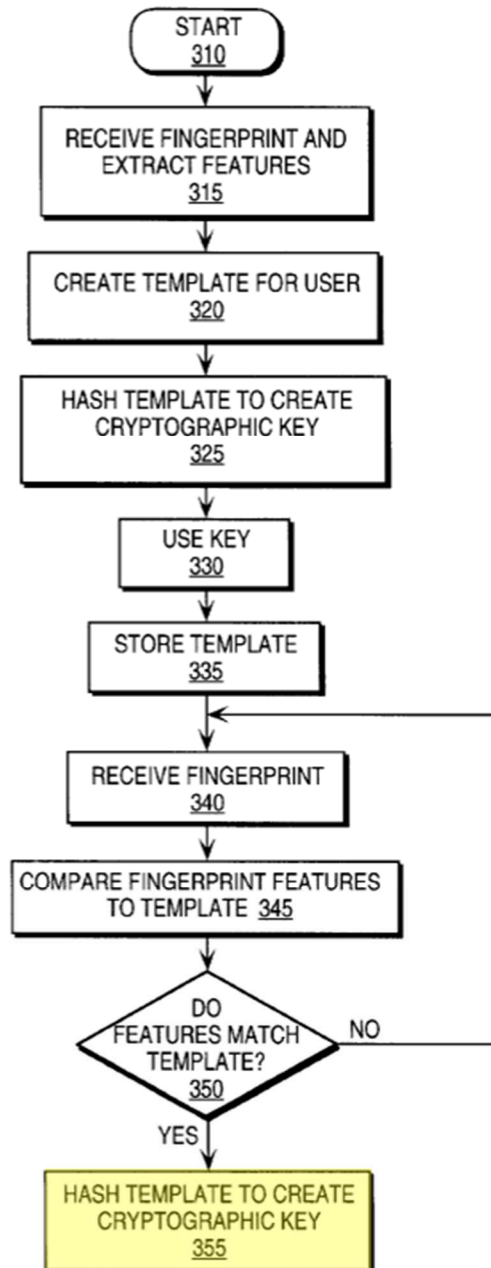


FIG. 3

EX1006, Fig. 3 (annotated)

265. See also EX1006, 4:60-5:13, 5:61-6:23 & Fig. 4; *supra*, §VII.E.

266. Bjorn does not store or otherwise retain the cryptographic key: “[t]he cryptographic key itself is not stored anywhere on the system.” EX1006, 4:47-48.

Instead, the key is produced when needed, and only in response to a successful authentication based on the fingerprint match. EX1006, 5:8-12.

267. As addressed in detail above (*supra*, §VII.F), it would have been obvious to implement Maes in accordance with Bjorn’s teachings regarding generation of a cryptographic key based on biometric information. In MBC, Bjorn’s key generation is triggered by local biometric verification consistent with Maes’s biometric verification on the PDA, and as similarly described with respect to Figs. 3 and 4 of Bjorn (e.g., blocks 340-355 and 450-470). EX1006, 5:3-12, Figs. 3-4; EX1004, 5:54-57, 11:9-13; *supra*, §VII.F. In MBC, Maes’s CPU 12—an aspect of the “secure module” (*supra*, Ground 1A at [1.5.1]) generates the Bjorn-like cryptographic key (key).

268. From these and related descriptions, a POSITA would have understood that MBC’s *secure module* generates a key when the fingerprint template (biometric information) read by the *biometric reading device* (e.g., biometric sensor 40) is determined by the *authentication module* (e.g., biometric processor module 22) to correspond to the *biometric authentication information* (e.g., fingerprint template) stored in *memory* (e.g., memory 14).

[1.5.3] encrypt the key

269. MBC renders [1.5.3] obvious.

270. In MBC, Bjorn's cryptographic key (key) is carried in an information file that accompanies the selected card information for a transaction. *Supra*, §VII.F, [1.5.2]. Per Maes, that file, which "contain[s] unique identifying information pertaining to the consumer." EX1004, 13:30-31.

271. Further, in MBC, the PDA's CPU 12 (secure module) encrypts the information file, including Bjorn's cryptographic key, using the encrypter/decrypter module 24. EX1004, 5:14-17. Per Maes, in the PDA device 10, the CPU 12's encrypter/decrypter module 24 (an aspect of MBC's "secure module" (*supra*, Ground 1A at [1.5.1])) performs encryption, with Maes explaining 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, 5:14-17, Fig. 1. Given the availability of the encrypter/decrypter module 24 to perform encryption, it would have been obvious to utilize module 24 in MBC's PDA to encrypt the information file including the cryptographic key consistent with Maes's teaching that the information file is encrypted. EX1004, 5:14-17, 13:30-31; see Ground 1A at [1.5.1], [1.5.3], *supra* §VII.F.

272. Thus, a POSITA would have understood that, because Bjorn's cryptographic key (key) is included in the encrypted information file, MBC's secure module encrypts the key. EX1004, 5:14-17, 13:30-31; *supra*, §VII.F.

[1.5.4] [encrypt] ... the payment information stored in memory; and

273. *Supra*, Ground 1A at [1.5.4].

[1.5.5] provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

274. MBC renders [1.5.5] obvious.

275. Maes discloses the PDA transmitting the selected card information (***payment information***) to a POS terminal via short-range RF circuitry for use in a secure transaction. For example, Maes explains that “[t]he selected card information[] ... would be transmitted to the POS terminal (via ... RF ...) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details.” EX1004, 13:34-38; *see also id.*, 12:5-29, Figs. 3, 5.

276. Maes further discloses that the information transmitted via RF from the PDA to the POS terminal can include an “encrypted information file” that “contain[s] unique identifying information pertaining to the consumer” for use in validating consumer in the transaction. EX1004, 13:24-38.

277. For the reasons addressed in detail above (*supra*, §VII.F), it would have obvious to incorporate a cryptographic key (key), generated in accordance with Bjorn’s techniques when the user is biometrically authenticated, in the “encrypted information” that Maes’s PDA transmits to the POS terminal via RF. *Supra*, §VII.F, IV.A. In MBC, the PDA thus transmits to the POS terminal via

short-range RF both the encrypted information file including Bjorn's (encrypted) cryptographic key (encrypted key) and the selected card information (payment information) for use in the transaction.

[2] The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

278. *Supra*, Ground 1A at [2].

[3] The mobile device of claim 1, wherein the payment information is associated with a primary account number.

279. *Supra*, Ground 1A at [3].

[4] The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device.

280. *Supra*, Ground 1A at [4].

[5] The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

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

[6] The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

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

[8.pre] A system, comprising:

283. MBC, per Maes, discloses a “***system***” comprising a PDA (***mobile device***), point-of-sale (POS) transaction terminal (***POS device***), servers of a financial institution 70 (***central database***), optionally further including central server 60. *Supra*, [1.pre]; *infra*, [8.1], [8.7.1], [8.8].

[8.1] a mobile device, comprising:

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

[8.2] short range radio frequency (RF) circuitry;

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

[8.3] memory configured to store biometric authentication information and payment information;

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

[8.4] a biometric module configured to read biometric information;

287. *Supra*, Ground 2A at [1.3].

[8.5] an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

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

[8.6.1] a secure module configured to:

289. *Supra*, Ground 2A at [1.5.1].

[8.6.2] generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

290. *Supra*, Ground 2A at [1.5.2].

[8.6.3] encrypt the key

291. *Supra*, Ground 2A at [1.5.3].

[8.6.4] [encrypt] ... the payment information stored in memory; and

292. *Supra*, Ground 2A at [1.5.4].

[8.6.5] provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

293. *Supra*, Ground 2A at [1.5.5].

[8.7.1] a point of sale (POS) device configured to:

294. *Supra*, Ground 1A at [8.7.1].

[8.7.2] receive, from the secure module, the encrypted key and payment information; and

295. MBC renders [8.7.2] obvious.

296. Per Maes, “[t]he selected card information, as well as the encrypted information file, would be transmitted to the POS terminal...” EX1004, 13:34-38. Accordingly, in MBC, per Maes, the PDA transmits the encrypted information file including the encrypted version of Bjorn’s cryptographic key (*encrypted key*) and the selected card information (*payment information*) using CPU 12 and RF module 48 (aspects of the “*secure module*” (*supra*, Ground 1A [1.5.1])) to the POS device over RF link L2. EX1004, 12:10-16, 13:19-37; *supra*, Ground 2A at [1.5.1], [1.5.5], [4]. A POSITA thus would have understood that the POS device *receives, from the secure module*, the encrypted version of Bjorn’s cryptographic key (*encrypted key*) and the selected card information (*payment information*).

[8.7.3] transmit, to a central database, the encrypted key and payment information; and

297. MBC renders [8.7.3] obvious.

298. Per Maes, “[t]he selected card information, as well as the encrypted information file, would be transmitted to the POS terminal (via the Universal Card, RF or IR) and then transmitted in encrypted form directly to the processing financial institution together with the purchase details.” EX1004, 13:34-38.

299. Maes further explains that “[t]he consumer transaction information is then sent to the proper financial institution 70 via communication link L4 (step 220).” EX1004, 11:37-40. Because Maes’s Fig. 3 (reproduced below) depicts communication link L4 between the transaction terminal 80 and the financial institutions 70, a POSITA would have understood that the transaction terminal performs that transmission, which is directed to the processing financial institution. EX1004, 11:37-40, 13:34-38, Fig. 3.

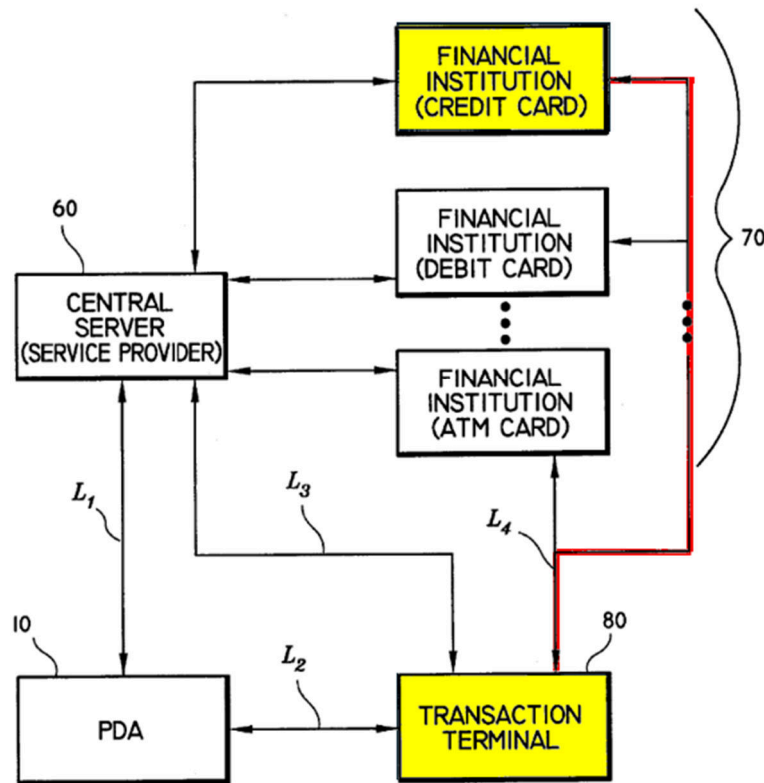


FIG. 3

EX1004, Fig. 3 (highlighted).

300. In MBC, Bjorn's cryptographic key (key) is carried in Maes's encrypted information file. Supra, §VII.F, Ground 2A at [1.5.3].

301. As explained below, MBC's processing financial institution, optionally together with central server 60, provides the *central database*. *Infra*, [8.8].

302. A POSITA would thus have understood that in MBC, the POS device transmits, to a central database, the encrypted key and payment information.

EX1004, 11:37-40, 13:34-38, Fig. 3; supra, §VII.F; infra, [8.8].

[8.8] a central database configured to validate the key and the payment information.

303. MBC renders [8.8] obvious.

304. In MBC, the processing financial institution provides a central database. EX1004, 13:34-38, Fig. 3; supra, §VII.F. Maes explains that the institution retains information provided at enrollment and applies it to information transmitted in a transaction, stating that the institution “would posses[s] the requisite key (provided by the service provider upon enrollment) to decode (i.e., decrypt) the transmitted information to verify the identity of the user.” EX1004, 13:51-55. Because the processing financial institution retains records obtained at enrollment and retrieves them to check information presented during a transaction, a POSITA would have understood that MBC’s financial institution comprises a database. EX1004, 13:51-55.

305. In MBC, the financial institution compares Bjorn’s cryptographic key (key) transmitted in Maes’s encrypted information file against the reference key regenerated from the user’s enrolled template. EX1004, 13:34-38, 13:51-55; supra, §VII.F. Bjorn explains that the cryptographic key is associated with a specific user, stating that “[t]his cryptographic key is identified with the specific fingerprint, and

thus with a specific user.” EX1006, 4:28-30. Because the comparison determines whether the transmitted key matches the reference key regenerated for that user and associated with the authorized user’s payment account, a POSITA would have understood that the comparison validates the key.

306. Maes explains that the processing financial institution “would provide an authorization number for the transaction to the merchant if the consumer was verified or, on the other hand, deny the transaction and inform the merchant if the consumer is not authorized to use the selected card.” EX1004, 13:56-60. Because the processing financial institution determines whether the consumer is authorized to use the selected card, a POSITA would have understood that the institution validates the selected card information (*payment information*). EX1004, 13:56-60.

307. A POSITA would thus have understood that in MBC, the central database validates the key and the payment information. EX1004, 13:51-55, 13:56-60; *supra*, §VII.F.

[9] The system of claim 8, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

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

[10] The system of claim 8, wherein the payment information is associated with a primary account number.

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

[11] The system of claim 8, wherein the POS device includes an RF reader.

310. *Supra*, Ground 1A at [11].

[12] The system of claim 8, wherein the biometric authentication information is stored separately from the payment information.

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

[13] The system of claim 8, wherein the payment information is stored in a memory accessible only by the secure module.

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

[15.pre] A method for secure transactions using a mobile device, comprising:

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

314. In MBC, the PDA performs the operations of [1.pre]-[6] (and corresponding operations of [15.pre]-[21]). *Supra*, Ground 2A at [1.pre]-[6].

[15.1] storing biometric authentication information and payment information in memory;

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

[15.2] reading biometric information using a biometric reader;

316. *Supra*, Ground 2A at [1.3].

317. Maes's biometric sensor 40 provides a ***biometric reader***, for the reasons discussed at [1.3] (describing the ***biometric module***). *Supra*, Ground 2A at [1.3].

[15.3] determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

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

[15.4] generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

319. *Supra*, Ground 2A at [1.5.2].

[15.5] encrypting the key

320. *Supra*, Ground 2A at [1.5.3].

[15.6] [encrypting] ... the payment information stored in memory; and

321. *Supra*, Ground 2A at [1.5.4].

[15.7] providing the encrypted key and payment information for use in a transaction.

322. *Supra*, Ground 2A at [1.5.5].

[16] The method of claim 15, further comprising reading biometric information provided by a user to complete the transaction.

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

[17] The method of claim 15, wherein the payment information is associated with a primary account number.

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

[18] The method of claim 15, further comprising providing the encrypted key and payment information to a point of sale (POS) device.

325. *Supra*, Ground 2A at [4].

[19] The method of claim 15, wherein the biometric authentication information is stored separately from the payment information.

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

[20] The method of claim 15, wherein the payment information is stored in a memory accessible only by a secure module.

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

[21] The method of claim 15, wherein the payment information is provided using a short range RF circuitry.

328. *Supra*, Ground 2A at [1.5.5].

329. As explained at [1.5.5], in MBC, the PDA transmits the selected card information (*payment information*) to the POS terminal over the RF link (*short range RF circuitry*). *Supra*, Ground 2A at [1.5.5], [1.1].

D. Ground 2B: Maes-Bjorn-Shults Renders Obvious Claims 7 and 14

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

330. Ground 1B's analysis of [7] relies only on Maes and Shults, both of which are in MBSC. *Supra*, Ground 1B at [7]; §VII.K.

331. Accordingly, MBSC renders [7] obvious for analogous reasons. *Supra*, Ground 1B at [7].

[14] The system of claim 8, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

332. *Supra*, Ground 2B at [7].

E. Ground 3A: Maes-Walker Renders Obvious Claims 1-6 and 15-21
[1.pre]

333. *Supra*, Ground 1A at [1.pre].

[1.1] short range radio frequency (RF) circuitry;

334. *Supra*, Ground 1A at [1.1].

[1.2] memory configured to store biometric authentication information and payment information;

335. *Supra*, Ground 1A at [1.2]. Walker further discloses *payment information* in the form of a credit card account number A stored in memory of a user device. EX1007, 1:20-21, 6:54-59, 8:19-20, Fig. 8 (step 803); *see also id.*, 7:49-61, Fig. 1.

[1.3] a biometric module configured to read biometric information;

336. *Supra*, Ground 1A at [1.3].

[1.4] an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

337. *Supra*, Ground 1A at [1.4].

[1.5.1] a secure module configured to:

338. *Supra*, Ground 1A at [1.5.1].

[1.5.2] generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

339. MWC renders [1.5.2] obvious.

340. As discussed above (*supra*, §VII.H), in MWC, the “selected card information” that Maes’s PDA transmits for a transaction is not the static card number itself, but rather a single-use credit card number generated according to

Walker's teachings, using a private key and a nonce associated with a credit card account that the user selected via Maes's card-selection interface. EX1004, 9:52-10:5 (local mode card selection); EX1007, 6:56-7:20 (device generating an "encrypted, single-use credit card number CCN" from the account's private key, nonce, and IV); *supra*, §VII.G. Walker teaches that this single-use number is generated by first retrieving the nonce (N) and initialization variable (IV) from memory, and then encrypting the nonce using the private key K and the IV, according to the relationship $C = EK(N, IV)$, where C is the encrypted nonce. EX1007, 8:9-19, Fig. 8 (steps 801-802), Fig. 7. The encrypted nonce C is then concatenated with the IV and the account number A (payment information) to form the transmitted single-use number: $CCN = C_IV_A$ (where $_$ denotes concatenation). EX1007, 7:12-20. Walker's single-use number directly embeds the user's credit card account number A. *Id.*

341. In MWC, generation of the single-use number (including encryption of the nonce that produces C) is conditioned on biometric authentication of the user, consistent with Maes's teaching that generation and transmission of card information and authorization numbers is conditioned on successful biometric verification. *See e.g.*, EX1004, 12:20-27 ("will prohibit the selected card information from being retrieved and transmitted to the transaction terminal 80 if the user is not biometrically verified"); 12:40-52 & 12:65-67 (conditioning

authorization number generation on biometric verification), 10:49-56 (“biometric verification must be performed before the card information can be” used), 11:15-19. To obtain analogous security improvements in MWC, a POSITA would have configured the MWC’s PDA to generate the encrypted nonce C only in response to successful biometric authentication of the user. Walker similarly describes a device that “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, 6:15-27, 11:46-52, Fig. 3B (steps 351-360).

342. In MWC, the encrypted nonce C represents a “key” for the transaction.⁹ Walker teaches that encrypted nonce C is used by the financial institution to assess whether to authorize transaction requests based on the single-use card number. EX1007, 8:41-9:10 & Figs. 9A-9B (Walker describing operations by which the issuer decrypts the encrypted nonce to recover the original nonce and determine whether the card number is “considered valid”). Absence or mismatch of the encrypted nonce C precludes authorization of the transaction. *Id.*, 7:1-3.

343. Alternately, the entire single-use credit card number including the encrypted nonce C provides the claimed “key” consistent with the Examiner’s uncontested mapping during prosecution. EX1002, 33, 37; *supra*, §VI.B.

⁹ *Supra*, Footnote **Error! Bookmark not defined..**

344. MWC's *secure module* generates the encrypted nonce (*key*) for a single-use credit card number (alternate mapping of *key*) when the *biometric information* read by the *biometric reading device* (e.g., biometric sensor 40) is determined by the *authentication module* (e.g., biometric processor module 22) to correspond to the *biometric authentication information* (e.g., voice or fingerprint data) stored in *memory* (e.g., memory 14).

[1.5.3] encrypt the key

345. MWC renders [1.5.3] obvious.

346. Per Walker, and as discussed above for [1.5.2], MWC's *secure module* encrypts the nonce, thereby forming an *encrypted key*. EX1007, 8:9-19, 9:10-20, Figs. 7-8; *supra*, Ground 3A at [1.5.2].

347. Additionally, it was well known before the Critical Date to encrypt data transmitted in a transaction request to protect against unauthorized third-parties who have access to the transmission medium (e.g., an RF link), and a POSITA would have been motivated to further encrypt the entire single-use number (alternate mapping of *key*) in MWC (including the encrypted nonce) to prevent even the single-use number from being divulged to an unauthorized party. EX1004, 13:19-38 (Maes disclosing option for encrypting unique identifying information transmitted over RF in transaction request); *see also* EX1005, 5:67-6:4

(further evidencing that encryption of data transmitted in a transaction request was known in the art).

[1.5.4] [encrypt] ... the payment information stored in memory; and

348. *Supra*, Ground 1A at [1.5.4].

[1.5.5] provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

349. MWC renders [1.5.5] obvious.

350. As discussed above in §VII.H and in connection with [1.5.2]-[1.5.3], MWC's secure module generates and transmits to a POS terminal, in response to biometric authentication of the user, a single-use card number (key) generated in accordance with Walker's teachings, where the single-use card number includes an encrypted nonce C (alternate mapping of key) and an account number A for the selected credit card (secured payment information). EX1004, 12:5-29 ("transmitting the selected card information directly from the PDA device to the ... POS transaction terminal" via RF), 13:34-38; EX1007, 7:3-8 ("single-use credit card number is transmitted to a merchant"), 8:31-36, 8:19-25; *supra*, Ground 3A at [1.5.2]-[1.5.3]; §VII.H. Walker's nonce is encrypted in the single-use number, and further it would have been obvious to encrypt the entire transmitted single-use number as discussed above. *Supra*, [1.5.3].

[2] The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

351. *Supra*, Ground 1A at [2].

[3] The mobile device of claim 1, wherein the payment information is associated with a primary account number.

352. *Supra*, Ground 1A at [3].

[4] The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device.

353. *Supra*, Ground 1A at [4].

[5] The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

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

[6] The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

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

[15.pre] A method for secure transactions using a mobile device, comprising:

356. *Supra*, Ground 3A at [1.pre].

357. In MWC, the PDA performs the operations of [1.pre]-[6] (and corresponding operations of [15.pre]-[21]). *Supra*, Ground 3A at [1.pre]-[6].

[15.1] storing biometric authentication information and payment information in memory;

358. *Supra*, Ground 3A at [1.2].

[15.2] reading biometric information using a biometric reader;

359. *Supra*, Ground 3A at [1.3].

360. Maes's biometric sensor 40 provides a *biometric reader*, for the reasons discussed at [1.3] (describing the *biometric module*). *Supra*, Ground 3A at [1.3].

[15.3] determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

361. *Supra*, Ground 3A at [1.4].

[15.4] generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

362. *Supra*, Ground 3A at [1.5.2].

[15.5] encrypting the key

363. *Supra*, Ground 3A at [1.5.3].

[15.6] [encrypting] ... the payment information stored in memory; and

364. *Supra*, Ground 3A at [1.5.4].

[15.7] providing the encrypted key and payment information for use in a transaction.

365. *Supra*, Ground 3A at [1.5.5].

[16] The method of claim 15, further comprising reading biometric information provided by a user to complete the transaction.

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

[17] The method of claim 15, wherein the payment information is associated with a primary account number.

367. *Supra*, Ground 3A at [3].

[18] The method of claim 15, further comprising providing the encrypted key and payment information to a point of sale (POS) device.

368. *Supra*, Ground 3A at [4].

[19] The method of claim 15, wherein the biometric authentication information is stored separately from the payment information.

369. *Supra*, Ground 3A at [5].

[20] The method of claim 15, wherein the payment information is stored in a memory accessible only by a secure module.

370. *Supra*, Ground 3A at [6].

[21] The method of claim 15, wherein the payment information is provided using a short range RF circuitry.

371. *Supra*, Ground 3A at [1.5.5].

372. As explained at [1.5.5], in MWC, the PDA transmits the single-use number including the encrypted nonce and payment information using ***short range RF circuitry***. *Supra*, Ground 3A at [1.5.5], [1.1].

F. Ground 3B: Maes-Walker-Shults Renders Obvious Claim 7

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

373. Ground 1B's analysis of [7] relies only on Maes and Shults, both of which are in MWSC. *Supra*, Ground 1B at [7]; §VII.L.

374. Accordingly, MWSC renders [7] obvious for analogous reasons. *Supra*, Ground 1B at [7].

IX. CONCLUSION

375. For all the reasons I have noted in the foregoing paragraphs, claims 1-21 of the '187 Patent are obvious in view of the references discussed above.

376. I currently hold the opinions 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