IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Francisco Martinez de Velasco Cortina et al.		
U.S. Patent No.:	10,235,513	Attorney Docket No.:	50095-0312IP1
Issue Date:	March 19, 2019		
Appl. Serial No.:	15/372,317		
Filing Date:	December 7, 2016		
Title:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION 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 17

V. LEGAL STANDARDS 18
- A. Terminology 18
- B. Legal Standards 18
- C. Anticipation 19
- D. Obviousness 19

VI. THE '513 PATENT 24
- A. Overview of the '513 Patent 24
- B. Prosecution History of the '513 Patent 25
  - i. The '513 Patent's Priority Date is its Filing Date 25
- C. Claim Construction 26

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES 27
- A. Overview of Wang 27
- B. Overview of Barnes 29
- C. Overview of Srey 31
- D. The Prior Art References Are Analogous Art 32
- E. Combination of Wang and Barnes 35
- F. Combination of Wang and Srey 39
- G. Overview of Bashan 41
- H. Bashan Combined with Wang-Barnes or Wang-Srey 42
- I. Overview of Mardikar 45
- J. Overview of Cooke 53
- K. Combination of Mardikar and Cooke 55
- L. Overview of Lee 57
- M. Lee Combined with Mardikar and Cooke 57

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '513 CLAIMS UNPATENTABLE 59
- A. GROUNDS 1A AND 2A: Wang in view of Barnes or Srey Renders Claims 1-9, 11-17, 19-25 Obvious 59
  - i. Claims 1 and 11 59
  - ii. Claim 19 92
  - iii. Claim 2 101
  - iv. Claim 3 101

v. Claims 4, 12, and 20 101
vi. Claims 5, 13, and 21 103
vii. Claims 6, 14, and 22 104
viii. Claims 7, 15, and 23 104
ix. Claims 8, 16, and 24 104
x. Claims 9, 17, and 25 105
B. GROUNDS 1B AND 2B: Bashan in Combination with Wang-Barnes or Wang-Srey Renders Claims 10, 18, and 26 Obvious 106
i. Claims 10, 18, and 26 106
C. GROUND 3A: Mardikar in view of Cooke Renders Obvious Claims 1-3, 5-9, 11, 13-17, 19, 21-25 107
i. Claims 1 and 11 107
ii. Claim 19 122
iii. Claim 2 126
iv. Claim 3 126
v. Claims 5, 13, and 21 126
vi. Claims 6, 14, and 22 126
vii. Claims 7, 15, and 23 128
viii. Claims 8, 16, and 24 128
ix. Claims 9, 17, and 25 129
D. GROUND 3B: Mardikar, Cooke, and Lee Render Claims 10, 18, and 26 Obvious 130
i. Claims 10, 18, and 26 130
IX. CONCLUSION 130

I. INTRODUCTION

1. I have been retained by counsel, Fish and Richardson P.C., to offer technical opinions related to US Patent No. 10,235,513 ("the '513 patent") (EX1001). I understand that Petitioners, Apple Inc. and Samsung Electronics Co., Ltd., are requesting that the Patent Trial and Appeal Board ("PTAB" or "Board") to institute an *inter partes* review ("IPR") proceeding of the '513 patent.

2. I have been asked to provide my independent analysis of the '513 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 '513 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 '513 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 (JHUISI). 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 ’513 patent (EX1001), and relevant excerpts of the prosecution history (EX1002) of the ’513 patent. Among various textbooks, documents, and publications, I have also reviewed the following prior art references:

- PCT Publication No. WO 00/52866 (“Wang” or EX1004)
- U.S. Patent No. US 8,611,919 (“Barnes” or EX1005)
- U.S. Patent No. 6,141,436 (“Srey” or EX1006)
- U.S. Patent No. 6,045,043 (“Bashan” or EX1007)
- U.S. Patent No. 8,108,318 (“Mardikar” or EX1009)
- U.S. Patent Pub. No. 2014/0025513 (“Cooke” or EX1010)

- U.S. Patent No. 8,761,665 ("Lee" or EX1011)
- U.S. Patent No. 5,144,649 ("Zicker" or EX1012)
- U.S. Patent Pub. No. 2002/0003892 ("Iwanaga" or EX1013)
- U.S. Patent No. 6,327,376 ("Harkin" or EX1014)
- Wikipedia Page for IrDA Communications, https://en.wikipedia.org/wiki/IrDA, Last accessed 9/5/16 (EX1015)
- U.S. Patent No. 5,698,836 ("Fujioka" or EX1016)
- U.S. Patent Pub. No. 20010056410 ("Ishigaki" or EX1017)

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 '513 patent at the time of the earliest possible priority date of the '513 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 '513 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 '513 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: Claims 1-9, 11-17, and 19-25 are obvious over the combination of Wang and Barnes.
- Ground 1B: Claims 10, 18, and 26 are obvious over the combination of Wang, Barnes, and Bashan.
- Ground 2A: Claims 1-9, 11-17, and 19-25 are obvious over the combination of Wang and Srey.
- Ground 2B: Claims 10, 18, and 26 are obvious over the combination of Wang, Srey, and Bashan.
- Ground 3A: Claims 1-3, 5-9, 11, 13-17, 19, and 21-25 are obvious over the combination of Mardikar and Cooke.

- Ground 3B: Claims 10, 18, and 26 are obvious over the combination of Mardikar, Cooke, and Lee.

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 1-26 ("**the Challenged Claims**") of the '513 patent in Section VIII.

IV. LEVEL OF ORDINARY SKILL IN THE ART

35. In my opinion, a person of ordinary skill in the art relating to the subject matter of the '513 Patent ("POSITA") 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, as of July 9, 2002. Additional education could substitute for professional experience, and professional experience for education.

36. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, participated in organizations, and worked closely with many such persons over the course of my career. Based on my knowledge, skill, and experience, I have an understanding of the capabilities of a POSITA. For example, from my industry experience, I am familiar with what a POSITA would have known and found predictable in the art. From teaching and

supervising my post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

V. LEGAL STANDARDS

A. Terminology

37. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless explicitly noted otherwise and unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). The '513 patent was filed December 7, 2016, and claims priority to provisional application 60/394,241, filed July 9, 2002, which I refer to as the "Critical Date" in this proceeding. It is my understanding that the '513 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 '513 patent as the point in time for claim interpretation purposes.

B. Legal Standards

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

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

C. Anticipation

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

41. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

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

D. Obviousness

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

44. I am informed by Counsel and understand that a patent claim composed of several limitations is not proved obvious merely by demonstrating that each of its limitations was independently known in the prior art. I am

informed by Counsel and understand that identifying a reason those elements would be combined can be important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. I am informed by Counsel and understand that it is improper to use hindsight in an obviousness analysis, and that a patent's claims should not be used as a "roadmap."

45. I am informed by Counsel and understand that an obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others. I have been informed by Counsel and understand that an obviousness evaluation can be based on a single reference or a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the nexus linking two or more prior art references is sometimes simple common sense. I have been informed by Counsel and understand that obviousness analysis recognizes that market demand, rather

than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

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

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

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

49. In sum, my understanding is that prior art teachings are properly combined where one of ordinary skill having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

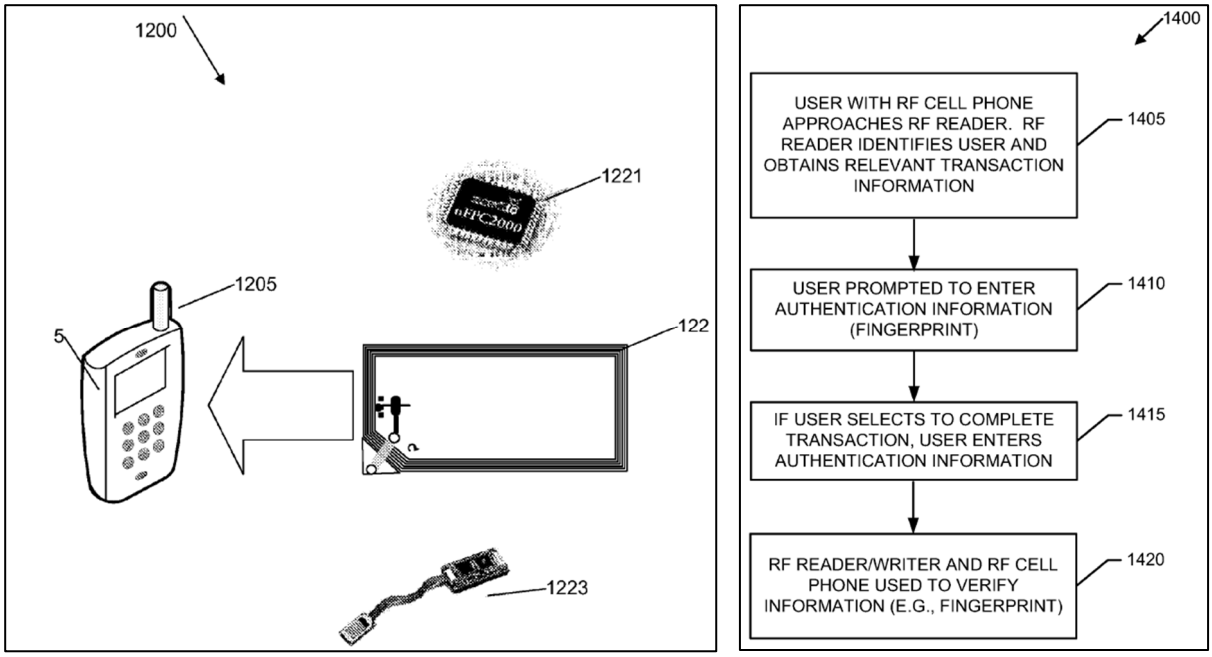
50. I have been informed by Counsel and understand that, according to 35 U.S.C. §316(e), in an *inter partes* review, "the petitioner shall have the burden of proving a proposition of unpatentability," including a proposition of obviousness, "by a preponderance of the evidence."

VI. THE ’513 PATENT

A. Overview of the ’513 Patent

51. The ’513 patent discloses a RF cellular telephone that communicates with a point of sale (POS) device. EX1001, FIG. 12 (reproduced below), 14:35-15:67. The RF cellular telephone includes an RF antenna, a chip that “carries authentication information (e.g., a fingerprint) and transaction information (e.g., credit card information),” and a fingerprint identifier/scanner. EX1001, 14:43-15:22.

52. When a user carrying the RF cellular telephone approaches an RF reader/writer at the POS, the reader identifies the user and obtains the relevant transaction information. EX1001, FIGS. 12-14, 15:24-67. The user is prompted to enter authentication information (a fingerprint), and the RF reader/writer and RF cellular telephone perform a verification that the fingerprint matches the information stored on the telephone to retrieve purchase information. EX1001, FIG. 14 (reproduced below), 15:24-67. The ’513 patent explains that the fingerprints can be imprinted on the POS device or the RF cellular telephone. EX1001, 15:24-47.



EX1001, FIG. 12 (left), FIG. 14 (right).

B. Prosecution History of the ’513 Patent

53. The ’513 patent issued from US Patent Application No. 15/372,317 (the “’317 application”), which was filed on 12/7/2016. EX1002, 476-568. After multiple office actions and an RCE, a Notice of Allowance was issued indicating that features [1.5.1]-[1.7] were the reasons for allowance. EX1002, 15. However, as explained in this Declaration, features [1.5.1]-[1.7] were well known and the Challenged Claims were obvious. *See* §§VIII.A.i.[1.5.1]-[1.7], VIII.C.i.[1.5.1]-[1.7]. Thus, the ’513 patent should not have been granted.

i. The ’513 Patent’s Priority Date is its Filing Date

54. The ’513 patent claims priority to several earlier patents and ultimately to a provisional application filed on July 9, 2002. EX1001, 2. But none of the earlier patents or the provisional application provide support for the claimed features.

55. Specifically, each of the independent claims of the ’513 patent recites a processor that is configured to perform receive, compare, and transmit operations. *See e.g.,* [1.4]-[1.8], [11.4]-[11.8], [19.5]-[19.9]. A processor or CPU is only mentioned at 20:23-36 and 21:43-63 of the specification (in addition to the claims section), but none of these sections describe a processor performing the claimed operations. The processor-related features were first recited at the time the ’317 application was filed. Because the claimed subject matter was first introduced into the application as of the filing date (12/7/2016), the earliest priority date that the ’513 patent should be accorded is 12/7/2016. EX1002, 526.

C. Claim Construction

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

57. With respect to the term “transaction information,” as recited in claims 1, 4-9, 11-17, and 19-24, I construed this term as “information used to process a transaction that includes at least credit card information or rewards card information.” Such a construction is consistent with the ’513 patent’s

specification. *See e.g.,* EX1001, 15:52-54 ("transaction information (e.g., credit card information and hotel rewards card information)).

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

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Wang[1]

59. Wang[2] is directed to a portable transaction arrangement that permits a user to conduct a charge card transaction with a charge card terminal of an electronic transaction system. EX1004, Abstract, 36:7-26 (claim 1). In particular, Wang discloses a hand-carried, portable electronic authorization device ("PEAD") 200 or portable electronic charge/approval device (PECAD) that communicates with a requesting device 202 to conduct an electronic transaction. EX1004, 10:6-23, 25:19-30. The PECAD incorporates PEAD functionality and also "permit[s]

---

[1] Overviews of the prior art references are incorporated by reference in each of the mappings that cite to the prior art references.

[2] U.S. Patent No. 6,175,922 is a U.S. patent related to Wang that was cited as one of more than a hundred cited references in an IDS. EX1002, 223-236; EX1001, 2. U.S. Patent No. 6,175,922 has overlapping disclosure with Wang, but was never applied in any rejection during prosecution.

the user to conduct transactions vis-a-vis the existing charge card infrastructures." EX1004, 25:19-35:30.

60. As shown in FIG. 2 below, the requesting device 202 sends a transaction request to PEAD 200 via data path 206, and an approval is sent back from the PEAD 200 via data path 212. EX1004, 14:5-15. Examples of the requesting device 202 and PEAD 200 include a point of sale terminal and personal digital assistant (PDA), respectively. EX1004, 20:21-25, 25:11-26:19, 37: 8-10 (claim 4).

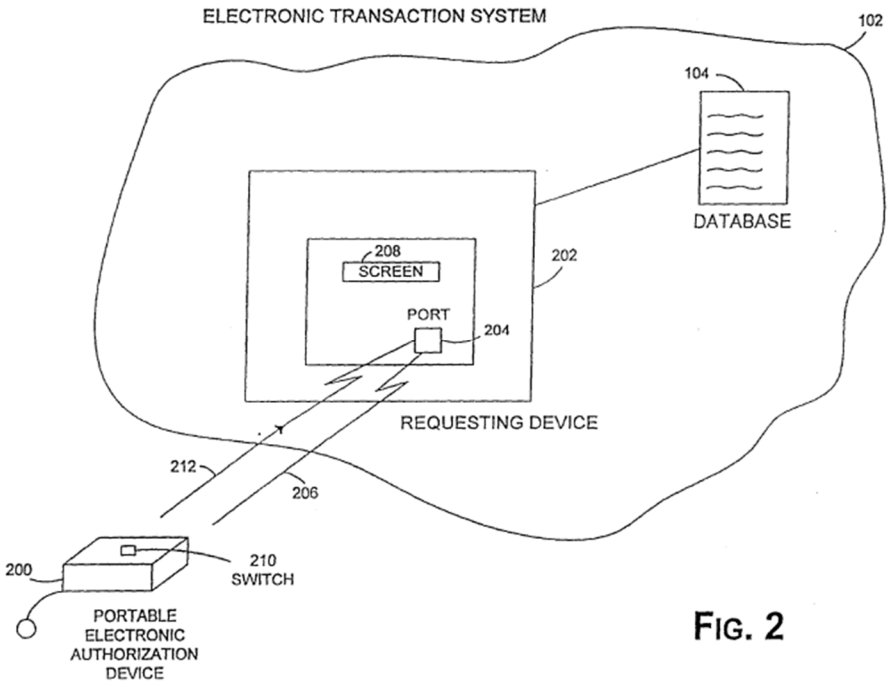


FIG. 2

EX1004, FIG. 2.

61. A user can approve the transaction. EX1004, 14:16-25. "In some cases, the transaction approval data requires the inclusion of certain pieces of identification data 302," which can include "unique biometrics or unique

identifying data such as fingerprint." EX1004, 13:16-29, 15:12-23. User identification data and user private key information is stored in memory 504, which can only be accessed by logic circuitry 502. EX1004, 18:31-19:32, FIG. 5A (reproduced below).

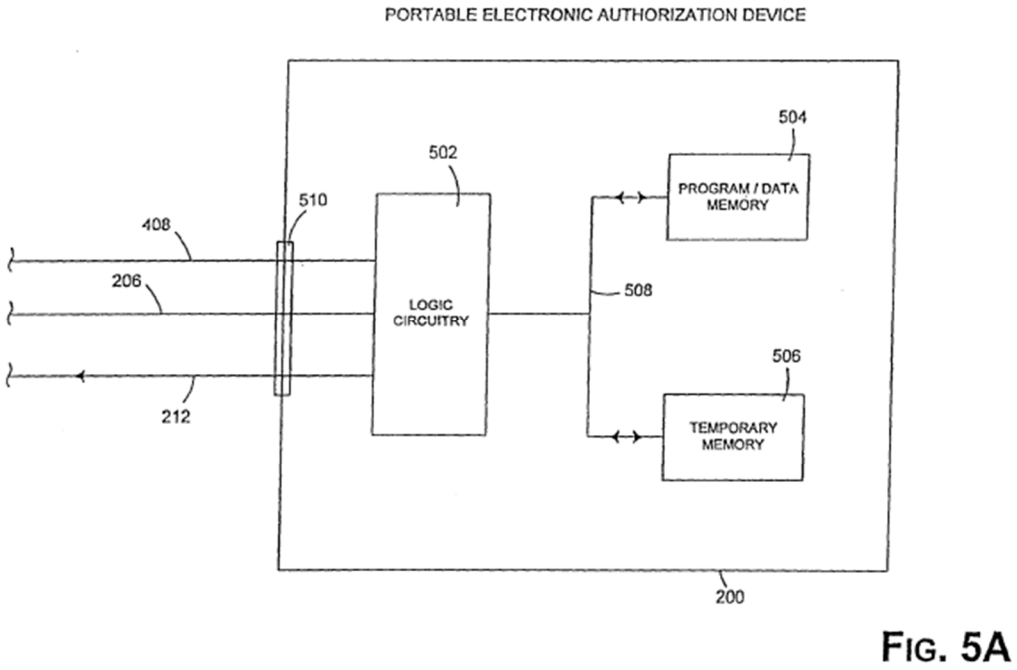


FIG. 5A

EX1004, FIG. 5A.

62. Wang teaches that before approving a transaction, a user may be required to input the user identification data, such as fingerprints, for user authentication. EX1004, 22:14-25, 13:16-22, 24:24-32, 38:5-6 (claim 12), 40:27-28 (claim 30). The transaction approval is sent only after the user authentication is complete. EX1004, 22:14-25, 24:24-32, 26:20-28.

B. Overview of Barnes

63. Barnes discloses a "multi-function communications device 101 that includes conventional mobile phone and personal digital assistant (PDA) capabilities … such as a communications module 105." EX1005, 4:27-30, FIG. 1. The device can take the form of a mobile phone or PDA. EX1005, 5:35-51. Barnes describes its device as having a cell phone profile and communicating with cell towers, 2.5G and 3G networks, GSM networks, and GPRS networks. EX1005, 7:48-50, 16:36-39. Therefore, a POSITA would have understood the Barnes's device encompasses a cellular/mobile phone.

64. Barnes's communication module "is implemented with one or more application specific integrated circuits (ASICs) and software stored in memory" and "includes hardware and software to allow" a processor (e.g., CPU 150) "to communicate with external devices and systems." EX1005, 6:1-13. The communication module enables Barnes's device to communicate with various networks including cellular networks, 2G, 2.5G, and 3G networks, GSM networks, GPRS networks, and short range networks, like Bluetooth networks and other local/personal area networks. EX1005, 6:14-9:24.

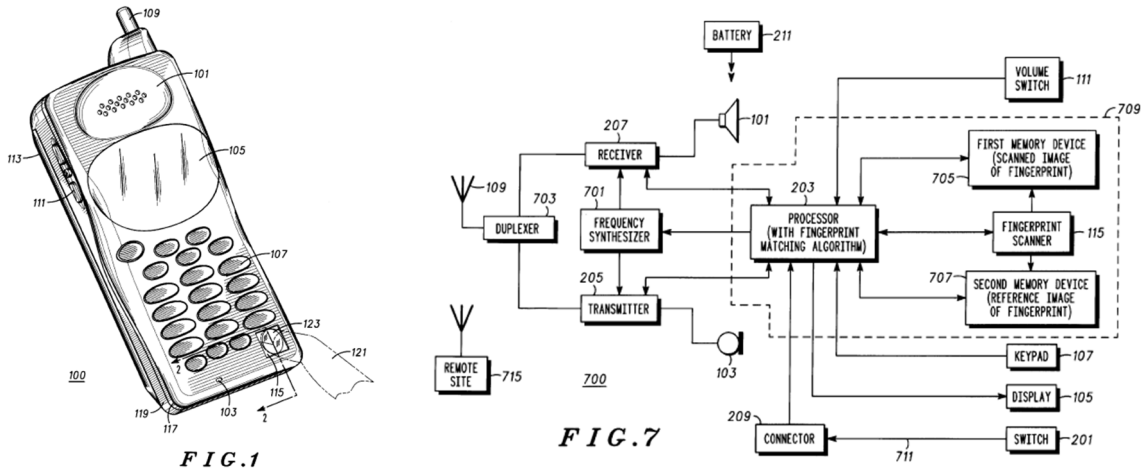
65. Barnes's device also utilizes multiple antennas respectively configured to operate with the different networks to support contemporaneous wireless communications with multiple networks. EX1005, 9:25-11:53. Thus, a POSITA would have understood the Barnes's device is configured to communicate

over short distances (e.g., using Bluetooth networks and its short range wireless local area network (LAN) module) and long distances (e.g., using a cellular network module such as its wireless wide area network (WWAN) module). EX1005, 6:14-9:24. Upon detection of a network switching condition, Barnes's device can switch from one network to another. EX1005, 9:25-10:36, 11:5-12:44, 29:4-30:33.

66. When Barnes's device is used for a commercial transaction, the user may be required to input authentication data. EX1005, 18:33-36. The device contains a module that authenticates the user with fingerprint data, e.g., by comparing fingerprint data received through a fingerprint scanner to stored user fingerprint data. EX1005, 17:33-48; 18:13-18, 21:1-14.

C. Overview of Srey

67. Srey is directed to a cellular telephone that includes an antenna 109 and "a fingerprint identification system (709) including a scanner (115) for scanning a fingerprint (123) of a finger (121) to generate an image of the fingerprint (123)." EX1006, Abstract, 2:46-64, 3:36-42, FIG. 1.



EX1006, FIG. 1 (left), FIG. 7 (right).

68. As depicted in FIG. 7 above, the fingerprint identification system 709 includes a fingerprint scanner 115 coupled to a first memory device that stores a scanned image of a fingerprint, a second memory device that stores a reference image of a fingerprint, and a processor that performs a fingerprint matching algorithm to determine if the scanned image of the fingerprint matches the stored reference image of a fingerprint. EX1006, 3:57-4:20, 4:64-5:20.

D. The Prior Art References Are Analogous Art

69. Wang, Barnes, Srey, Bashan[3], Mardikar[4], Cooke,[4] and Lee[5] are analogous art to the '513 patent at least because they: (1) are from the same field of endeavor as the purported claimed invention of the '513 patent; and/or (2) are reasonably pertinent to the problem faced by the inventors of the '513 patent. *In re Bigio*, 381 F.3d 1320, 1325, 72 USPQ2d 1209, 1212 (Fed. Cir. 2004).

70. The '513 patent describes security solutions for a radio frequency (RF) device to communicate with a RF reader/writer, e.g., a POS device. EX1001, 1:35-62, 2:5-6, Abstract, 14:35-38. The '513 patent purports to address problems such as security and user verification by implementing a user authentication protocol involving authenticating user fingerprints before authorizing a transaction. EX1001, 1:28-31, 15:24-67. The applied references are directed to the same field and/or address the same problems.

71. Wang is directed to communications between a PEAD and POS device that requires user approval and fingerprint authentication. EX1004, 13:16-15:23, 22:14-25, 24:24-32, 38:5-6 (claim 12), 40:27-28 (claim 30). 26:20-28; *see* §VII.A. Barnes requires user fingerprint authentication before its cellular device

---

[3] Reference applied in Grounds 1B and 2B.

[4] References applied in Ground 3A.

[5] Reference applied in Ground 3B.

can be used to authorize a transaction. EX1005, 7:48-50, 16:36-17:48, 18:13-36, 21:1-14; *see* §VII.B. Srey describes performing fingerprint verification to verify a user and unlock a cellular phone before use. EX1006, 2:16-17, 2:65-3:36; *see* §VII.C. Bashan is analogous art to the '513 patent at least because it relates to conducting a wireless transaction using a mobile device. EX1007, Abstract, 1:5-47; *see* §VII.G. Mardikar describes secure, biometrically-authenticated contactless payment from a personal mobile/cellular device at an NFC POS. EX1009, Abstract, 6:42-8:61, 9:35-12:55; *see* §VII.I. Cooke describes contactless payment transactions between a payment-enabled mobile device and a proximity reader incorporated with a POS terminal. EX1010, Abstract, ¶¶[0003], [0025]; *see* §VII.J. Lee describes controlling wireless RF communications between a mobile phone and an external RF reader. EX1011, Abstract, *see* §VII.L. Thus, Wang, Barnes, Srey, Mardikar, Cooke, and Lee are all analogous art to the '513 patent.

72. As explained in more detail below in §§VII.E and VII.F, a POSITA would have combined the teachings of Wang with Barnes or Srey because doing so would have merely involved combining prior art elements according to known methods to yield the predictable result of an electronic transaction system in which a portable device (cellular/mobile phone) having security features, such as fingerprint authentication, communicates with a point of sale device using short range and wide area networks.

E. Combination of Wang and Barnes

73. A POSITA would have combined Wang and Barnes such that:

1) Wang's portable device would have been implemented as or part of Barnes's cellular phone and would have included Barnes's short range wireless LAN module and WWAN (cellular) module;
2) Wang's device would have incorporated Barnes's teachings of connecting to multiple networks at the same time and switching networks upon the satisfaction of a switching condition;
3) Barnes's user authentication involving a fingerprint scanner and performing a comparison of scanned and stored user fingerprints would be part of Wang's user authentication; and
4) Retrieving payment information in response to transaction requests, as taught by Barnes, in Wang's device.

74. Wang describes conducting an electronic transaction between a portable device and a second device, such as a POS device, using a computer network (e.g., the Internet). EX1004, 1:23-35, 15:24-35. Wang teaches that the transaction communications may be performed using infrared or wireless RF technology, thereby indicating that the communications are short range communications. EX1004, 19:13-26. Specifically, infrared communications were well-known to use invisible light waves just beyond the red end of the visible

spectrum to send data between devices over a range of a few centimeters to a few meters. In fact, such communication was even developed into a standard known as the Infrared Data Association (IrDA) standard. *See generally*, EX1015. IrDA was used for communications between e.g., 5 centimeters to 2 meters. EX1015, 1-5.

75. Moreover, while Wang discloses a user authentication method utilizing biometric data such as fingerprint data, Wang does not reveal all the details of the user authentication method. EX1004, 22:14-25. A POSITA would have combined Wang and Barnes in the above-noted manner for the following reasons.

76. First, Wang's device would have been modified to incorporate hardware and software that permits Wang's device to communicate using multiple networks. For example, Wang's device would have been modified to include cellular circuitry (e.g., ASICs, antennas) and related software, as described by Barnes, so that the device can also communicate using WWAN cellular networks, such as 2G, 3G, and GSM networks. EX1005, 8:19-10:36, 6:1-14. Effectively, the combined Wang-Barnes device would operate as a cellular/mobile phone with long distance (e.g., cellular) and short distance communications capabilities, e.g., using Bluetooth technology.

77. Second, adding Barnes's long distance communication capabilities would have allowed the Wang device to conduct electronic transactions over long

and short ranges. Consequently, the user would experience enhanced convenience, accessibility, and usability. For instance, with the Wang-Barnes device, a user could pay for a transaction remotely while traveling in a car several kilometers from a vendor point of sale device or in-person a few feet away from a vendor point of sale device.

78. Third, incorporating the ability to switch between different networks, as taught by Barnes, would have allowed Wang's device to avoid a single point of failure and switch networks when a currently-connected network fails or has data transmission issues. By incorporating Barnes's network switching capabilities, Wang's device would improve reliability to maintain communications and complete a transaction. EX1005, 11:63-12:65.

79. Fourth, a POSITA looking to implement Wang's user authentication mechanism would have turned to Barnes because Barnes provides the details of fingerprint-based authentication. For instance, both Wang and Barnes disclose using biometric matching to authenticate a user. EX1004, 22:14-25, 13:16-29; EX1005, 17:38-18:18. Barnes additionally reveals that in doing so, a fingerprint is scanned and then compared with stored fingerprint data to authenticate the user. EX1005, 18:13-18. In both Wang and Barnes, such authentication can be required before completing transactions that require high security. EX1004, 22:14-25, 38:5-7, 40:27-28; EX1005, 18:1-18, 21:1-14.

80. Fifth, a POSITA looking to implement Wang's electronic transaction payment would have turned to Barnes because Barnes provides the details of providing payment information as part of the transaction. For instance, Barnes explains that a receiving mobile device provides stored payment information, such as credit card or bank account information, in response to receiving a transaction request that requests payment information stored in the receiving device. EX1005, Abstract, 3:53-4:2, 7:3-24, 21:52-22:10, 29:39-46, 30:22-33, 22:57-23:48, 49:37-67.

81. The combination of Wang and Barnes would have been predictable and had a reasonable expectation of success. Both Wang and Barnes describe their devices as being configurable to operate as a PDA. EX1004, 20:21-25; EX1005, 4:26-40. Due to the similarities of the devices, a POSITA would have predictably turned to Barnes to enhance the capabilities of the Wang device, in the manner described above. Moreover, because Wang was directed to a portable device involved in electronic transactions, it would have been predictable for a POSITA to turn to Barnes's cellular device (and communication systems) that is also directed to electronic transactions, and implement Barnes's known techniques (including e.g., network switching). For instance, as the drive for enhanced connectivity and portability using the Internet grew in the 2000s, expanding the use of Wang's device into cellular networks using known cellular hardware and software would

have been predictable and had a reasonable chance of success because incorporating cellular connectivity for portable devices was known and increasingly common in the 2000s.

82. Lastly, incorporating the details of Barnes's authentication method would also have been predictable with a reasonable chance of success because Barnes provided conventional and known implementation details for fingerprint-based user authentication, such as comparing scanned fingerprint data with stored fingerprint data.

F. Combination of Wang and Srey

83. A POSITA would have combined Wang and Srey such that:

1) Wang's portable device is implemented as or part of Srey's cellular phone including Srey's transmission/receiving capabilities for cellular network communication in addition to Wang's ability to communicate across a short range network; and
2) Wang's user authentication includes Srey's user authentication method and system architecture involving a fingerprint scanner coupled to processor and memory devices to perform a comparison of scanned and stored user fingerprints

84. A POSITA would have combined Wang and Srey in the above-noted manner for the following reasons.

85. First, Wang's device would have been modified to include cellular circuitry such as a cellular receiver and transmitter, as described in Srey, so that the device can also communicate using cellular networks. EX1006, FIGS. 5, 9; 8:25-37, 9:39-67. Effectively, the combined Wang-Srey device would have operated as a cellular phone with long range (e.g., cellular) and short range communications capabilities, e.g., using infrared or RF technology.

86. Second, modifying Wang's device into or to incorporate Srey's cellular phone capabilities would have allowed the Wang device to conduct electronic transactions over long and short ranges. Consequently, the user would experience enhanced convenience, accessibility, and usability. For instance, a user could pay for a transaction remotely while traveling in a car several kilometers from a vendor point of sale device or in-person a few feet away from a vendor point of sale device.

87. Third, a POSITA looking to implement Wang's user authentication mechanism would have turned to Srey because Srey provides the details of fingerprint-based authentication. For instance, both Wang and Srey disclose using biometric matching to authenticate a user. EX1004, 22:14-25, 13:16-29; EX1006, 5:55-6:17. Srey additionally reveals that the memory, processor, and input device (scanner) architecture to scan and compare fingerprints to authenticate the user. EX1005, 18:13-18.

88. The combination of Wang and Srey would have been predictable and had a reasonable expectation of success. Because Wang was directed to a portable device involved in electronic transactions, it would have been predictable for a POSITA to allow Srey's cellular phone to additionally communicate in a cellular communication system, which offers Internet access in a larger coverage area than short range networks. In particular, as the drive for enhanced connectivity and portability using the Internet grew in the 2000s, expanding the use of Wang's device into cellular networks using known cellular hardware and software would have been predictable and had a reasonable chance of success because incorporating cellular connectivity for portable devices was known and increasingly common in the 2000s.

89. Lastly, incorporating the details of Srey's authentication method would also have been predictable with a reasonable chance of success because Srey provided conventional and known implementation details for fingerprint-based user authentication, such as storing fingerprint data in a memory, scanning fingerprint data, and then comparing the scanned fingerprint data with the stored fingerprint data.

G. Overview of Bashan

90. Bashan relates to "a data transaction device having an on-board processor for effecting both 'contact' and 'contactless' modes of data transfer."

EX1007, 1:5-7. Bashan explains that where contactless transmission is used, "a coil antenna in the chip card is adapted to receive data from and transmit data to a reading device having a similar antenna." EX1007, 1:45-47. "Together with the coil antenna 15[,] the tuning capacitor 38 constitutes a resonant circuit whose resonant frequency is thus adjustable." EX1007, 5:17–20. In the contactless mode, a clock output CLK signal "is set to a frequency equal to f_0/N where f_0 is the input frequency of the carrier signal typically equal to 13.56 MHz." EX1007, 9:13–15.

H. Bashan Combined with Wang-Barnes or Wang-Srey

91. As explained above in §§VII.E-VII.F, the portable devices in the Wang-Barnes combination and the Wang-Srey combination are configured to operate across various communication networks, including wireless wide area networks, such as cellular networks, and short range networks, such as Bluetooth or infrared. *See* §§VII.E-VII.F; EX1005, 7:3-8:55; EX1006, FIGS. 5, 9; 8:25-37, 9:39-67. Thus, a POSITA would have understood that the portable devices in both combination systems are configured to operate at various frequencies.

92. For example, Barnes explains that the short range wireless RF LAN/PAN module can operate in the 2.4 GHz spectrum for Bluetooth communications with "signal hops among 79 frequencies at 1 MHz intervals to give a high degree of interference immunity and up to seven simultaneous

connections can established and maintained." EX1005, 7:3-24. At the same time, longer distance communications across WWANs using the same device can be conducted using, e.g., 2G, 2.5G, 3G, and GSM (380-1900 MHz) networks. EX1005, 8:25-55.

93. Similarly, Srey utilizes a frequency synthesizer 701 to manipulate the operational frequencies of its receiver 207 and transmitter 205. EX1006, FIG. 7, 9:39-67. In the Wang-Srey combination, a POSITA would have understood that the frequency synthesizer 701 would have been configured to operate in a wide spectrum of stable RF frequencies in support of the long and short range communications. Indeed, a POSITA would have understood that Wang's communication port 510's ability to support communications "using infrared technology, wireless RF technology, a magnetic read/write head, a contact-type plug for facilitating serial or parallel data transmission, or the like" would only be possible if Wang's device was configured to operate at different frequencies.

94. Relatedly, Bashan discloses a method of conducting a wireless transaction in its contactless mode using a coil antenna 16. EX1007, Abstract, 4:11-65. Bashan teaches conducting a wireless transaction in its contactless mode using a carrier frequency f_0 of 13.56 MHz, which is firmly within the radio frequency spectrum. EX1007, 9:13–15.

95. It would have been obvious to a POSITA that the short range radio frequency circuit in the Wang-Barnes device or the Wang-Srey device would have been configured to also operate in the 13.56 MHz. As explained below, doing so would have simply amounted to combining prior art elements according to known methods to yield predictable results.

96. Short range communications frequently used 13.56 MHz as the communication frequency because it offered a good balance of wireless communication distance (e.g., a few centimeters to a meter) with a desirable data speed and power transfer within an internationally approved, license-free band. Thus, using it in the Wang-Barnes device or Wang-Srey device would have been an obvious choice for a POSITA so that users would experience the same benefits.

97. Although Bashan is directed to "a card," using its teaching of conducting contactless communications at a frequency of 13.56 MHz would have been applicable to a cellular phone. Doing so would have involved modifying the operational configurations of the frequency synthesizer or modulator in Wang's communication port 510 (the short range radio frequency circuit in the Wang-Barnes device and Wang-Srey device) to permit processing (including transmission and reception) of signals at 13.56 MHz. Furthermore, using a cellular phone would still offer the benefits of contactless operation because cellular phone-based wireless transactions can be completed "without imposing the overhead incurred in

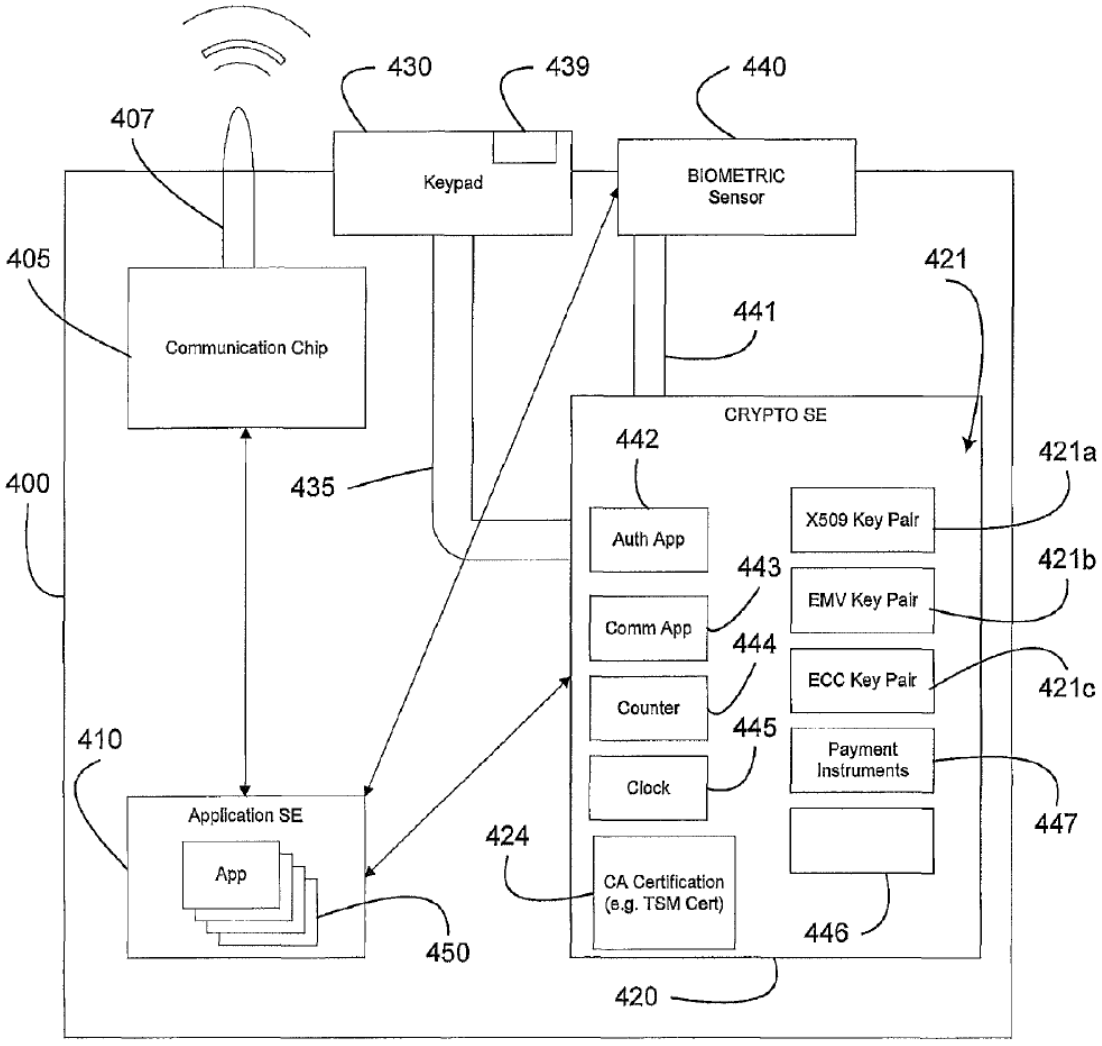
manually introducing the smart card into the slot of a card reader." EX1007, 1:23–24.

98. A POSITA would have had a reasonable expectation of success in combining Bashan with Wang-Barnes or Wang-Srey because, as noted above, Bashan's 13.56 MHz frequency was a known frequency for the type of short range card-to-reader transactions Wang's device carries out. EX1007, 9:13–15. Operating Wang's wireless RF circuit at 13.56 MHz neither alters Wang's principle of operation nor requires any redesign of Wang's transaction flow; it merely specifies the frequency of the already-disclosed wireless RF link.

I. Overview of Mardikar

99. Mardikar discloses a variety of methods for securing "financial transactions initiated from an electronic device," including methods for authenticating a user based on "biometric information" input to the device through an included biometric sensor. EX1009, Abstract, 1:15-17, 3:11-33, FIGS. 4, 5a, 5b, 6a.

100. In more detail, Mardikar's FIG. 4 (reproduced below) "shows an example embodiment of … a client device 400 … such as a mobile phone" that "may include a communication chip 405, an antenna 407, secure elements 410, 420, a keypad 430 and a biometric sensor 440." EX1009, 6:43-49.



EX1009, FIG. 4.

101. Mardikar explains that a secure element (SE) "may be, for example, a smart card … embedded inside device 400," adding that a "smart card is a small, relatively tamper-proof computer" that "may contain a CPU and some non-volatile storage" that "makes it possible for the card to keep some secrets, such as the private keys associated with any certificates it holds." *Id.*, 7:45-57.

102. FIG. 4's "Application SE" 410, and "Crypto SE" 420 "may be pre-loaded with applications and/or may be capable of downloading … applications for facilitating financial transactions over a network, key pairs, payment instruments and/or a Certifying Authority (CA) certificate." *Id.*, 7:58-63. "Splitting the App SE from the Crypto SE may enable a single Trusted Service Manager to verify and authenticate the identity of a user for each of a number of various Service Providers." *Id.*, 9:48-59.

103. In more detail, the App SE 410 may, in an exemplary embodiment, "be designated for and arranged for storing various, resident financial transaction or payment applications 450, each of which may facilitate financial transactions for a different financial Service Provider," for example, "PayPal." *Id.* 8:62-9:3. In that regard, the App SE 410 may be a "SIM card" that "securely store[s] a service-subscriber key (IMSI) used to identify a subscriber," and that is loaded with "applications 450" that are "signed by a common Trusted Service Manager (TSM) public key." *Id.*, 9:4-23.

104. The Crypto SE 420 may, in an exemplary embodiment, "be designated for and arranged for loading and storing authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 and other security-related information, including, for example, unique biometric authentication information related to a specific user." *Id.*, 9:39-

43. The Crypto SE 420 may, for example, "provide verification and authentication for multiple applications stored in the App SE 410." *Id.*, 9:43-47.

105. In that regard, a biometric authentication application 442 "may reside on the Crypto SE 420 and may evaluate" biometric data received from biometric sensor 440 "and compare the data to data from a registered user, or may register the data where the data is being collected as part of a registration or certification procedure." *Id.*, 9:60-65, 10:42-11:7; FIGS. 4, 5a, 5b.

106. Mardikar's FIGS. 5a and 5b (reproduced below) "illustrate an exemplary system 500 for registering client device 400" with a "trusted service manager 505," for example, "to unlock a payment credential or CA certificate 424 (FIG. 4) pre-loaded on the device 400." *Id.*, 10:41-47.

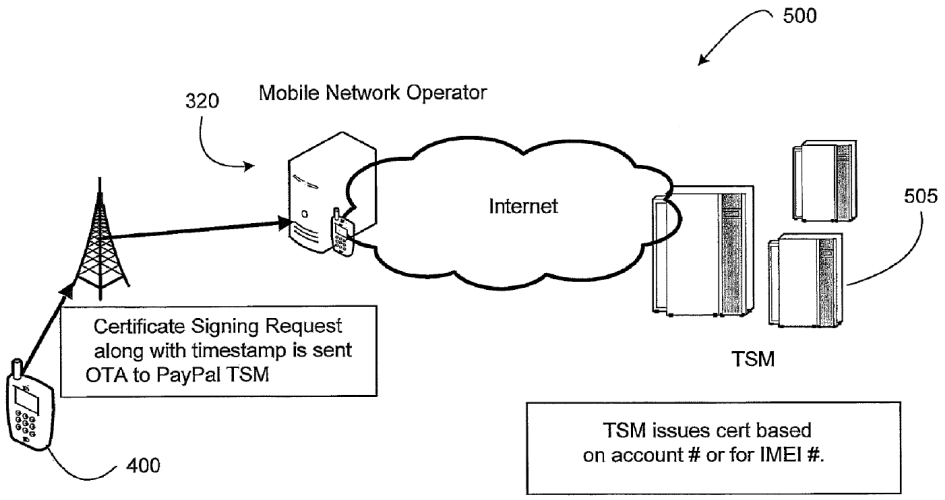


FIG. 5a

EX1009, FIG. 5a.

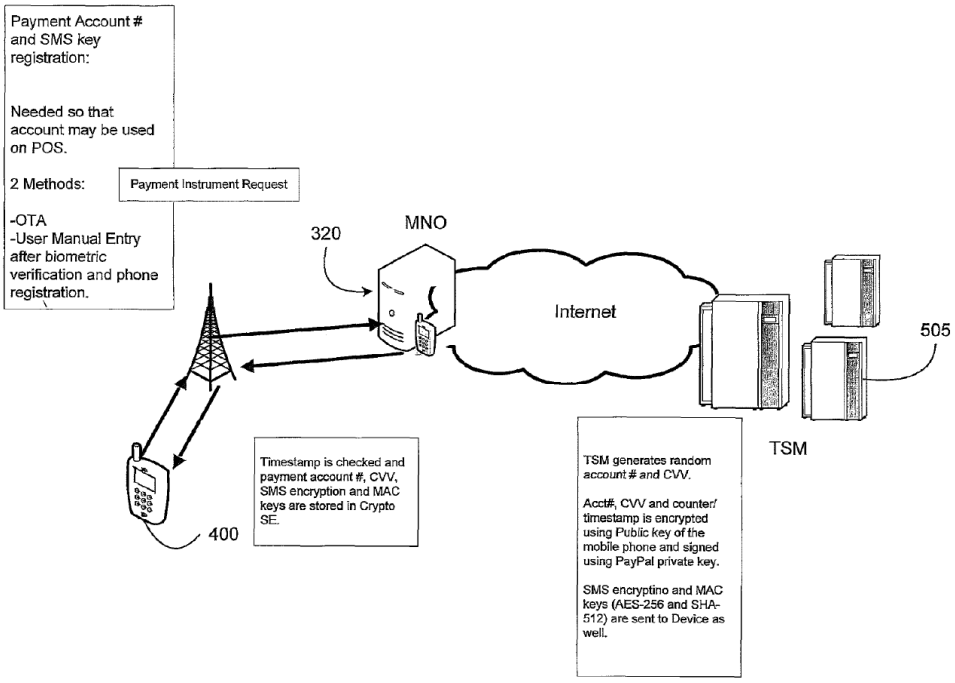


FIG. 5b

EX1009, FIG. 5b.

107. "Registration may include registering a biometric attribute, for example a thumb-print or finger-print, to unlock payment," and "[a]ll applications on the device may be registered with and deployed via the trusted service manager." *Id.*, 10:47-54. For instance, "a payment credential 424 (FIG. 4) … may be unlocked by registering the user's unique biometric profile using the biometric sensor 440 (FIG. 4) … by registering a thumb-print twice …." *Id.*, 10:54-60.

108. In this context, Mardikar further explains that "when a customer invokes pre-loaded app 450 (FIG. 4), SCEP/CRMF (Simple Certificate Enrolment Protocol/Certificate Request Message Format) is invoked," and a "user's TSM

credential or certificate 424" may be "entered and associated with the Service Provider's user account." *Id.*, 10:63-66.

109. Mardikar's FIG. 6a (reproduced below) "illustrate[s] a method 600 of conducting a near-field communication (NFC) transaction at a point of sale (POS)" that is facilitated by a Service Provider (e.g., PayPal), and that involves unlocking the user's registered payment credentials through further biometric authentication. *Id.*, 11:29-13:36, FIGS. 6a, 6b, 6c.

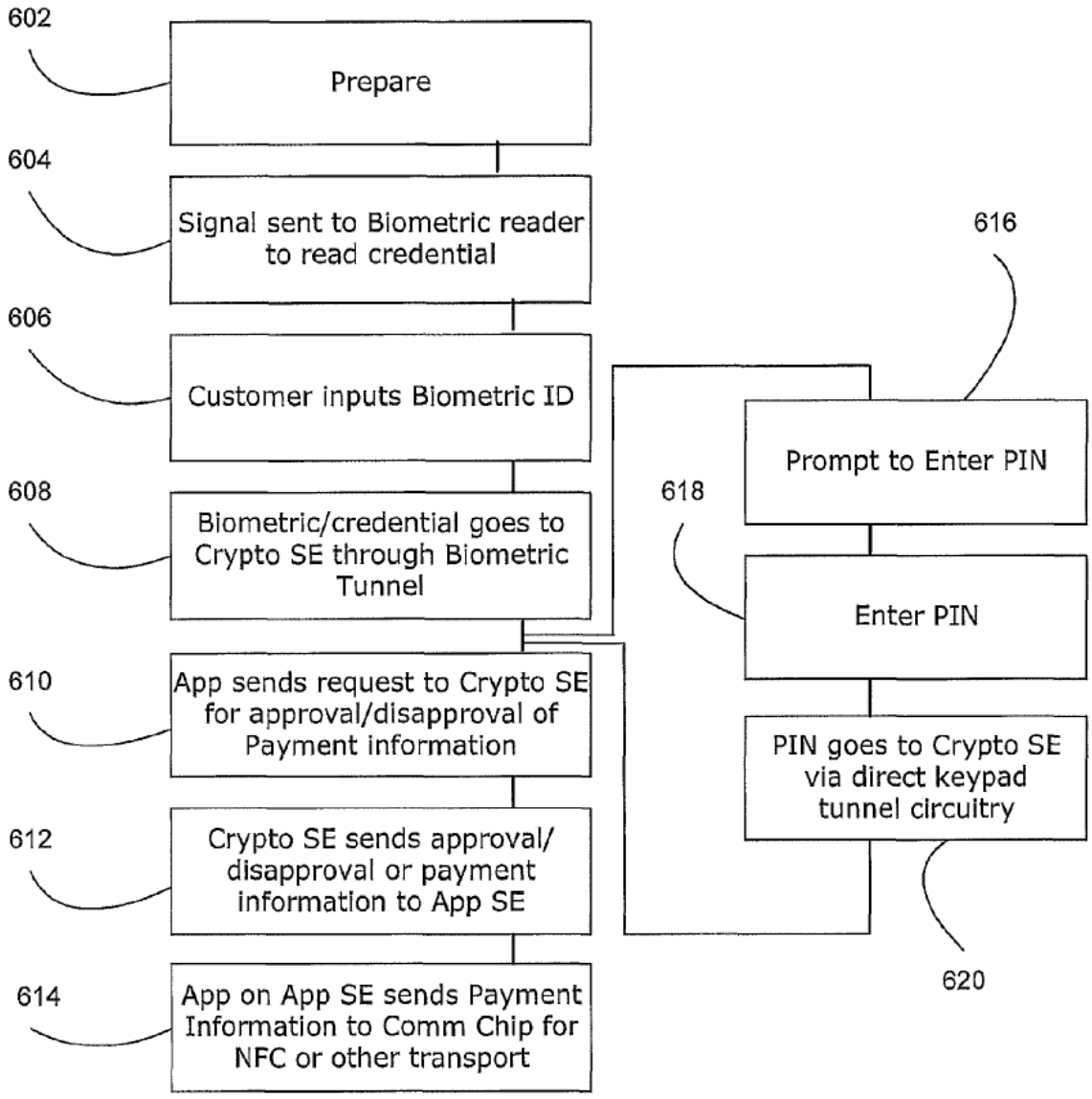


FIG. 6a

EX1009, FIG. 6a.

110. In more detail, Mardikar explains in the context of an exemplary embodiment involving a POS NFC transaction that "preparing the device for payment may prompt a payment application resident on the App SE 410 … to

check 604 the biometric sensor for biometric input," that a user may then input 606 their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor 440," and that the "input biometric ID may be directly sent or tunnelled 608 to Crypto SE 420 … for authentication/unlocking." *Id.*, 11:44-51; *see also id.*, 9:60-65 ("a biometric authentication application … may evaluate the biometric data and compare the data to data from a registered user").

111. "Once a user's biometric identity is authenticated properly, the Crypto SE 420 may send 612 an approval/disapproval message and payment or other information to the App SE," which "may then send the payment information 614 to the communication chip 405 for further transmission or transport to a reader or other communication reception device located at the POS, for example a POS NFC reader located at a merchant/vendor's place of business." *Id.*, 11:62-12:3. "In other example embodiments, the Crypto SE 420 may establish a direct, secure transmission between the Crypto SE 410 and the POS." *Id.,* 12:4-21.

112. Either way, the transmitted "[p]ayment information may include payment information, such as amount and account number, and may include a CVV." *Id.*, 12:22-30. For example, "[w]hen a payment is made at a merchant POS 650 using Visa/MC/AmEx, the last four digits of the payment instrument may be sent to the TSM (using, for example, an application provided on the App SE by the TSM)," and "[t]his information may be correlated with signature information"

that is "collected by the TSM" and "used to identify the client device and its user." *Id.*, 12:31-43.

113. Notably, Mardikar expressly indicates that "the payment information may be transmitted by alternate methods of communication as desired or necessary in a particular embodiment or circumstance …." *Id.*, 12:22-30; *see also id.*, 3:11-33, 4:27-36 ("the system is not limited to NFC applications, but may also apply to other types of applications, for example, SMS, mobile internet or other forms of communication"), 13:37-14:19 (describing a secure SMS transaction).

114. For instance, Mardikar explains that "TSM 325 may act as a payment provider system (PP), such as PayPal, and may provide payment processing for online transactions on behalf of the customer so that the customer does not expose payment information directly to the merchant." *Id.*, 6:13-29.

115. In that regard, "the customer may pre-register his account with the payment provider system, map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site." *Id.* "After the financial transaction is authorized, the TSM 325 or payment provider system completes the transaction." *Id*.

J. Overview of Cooke

116. Cooke is directed to systems and methods for conducting contactless payment transactions between a proximity payment device and a proximity reader incorporated with a point-of-sale terminal. EX1010, Abstract, ¶¶[0003]-[0004], [0014]-[0017]. Cooke explains that "the account number of the proximity payment card is automatically read from the card by radio frequency (RF) communication between the payment card and the proximity reader, which device is conventionally incorporated with a Point-of-Sale (POS) terminal." EX1010, ¶[0003].

117. Cooke teaches that a proximity payment device is not limited to a card: "mobile telephones, personal digital assistants (PDAs), tablet computers, laptop computers, and the like can be equipped with integrated circuitry having the same functionality as the RFID IC of a contactless payment card," thereby "turning such mobile devices into contactless payment devices." EX1010, ¶¶[0004], [0016], [0021], [0025], [0041], [0050].

118. Cooke discloses the POS-initiated request/response operation that governs such transactions: "the payment circuit of the proximity payment device is configured to respond to an interrogation signal from an NFC reader by transmitting payment account information such as a payment card account number (PAN) or other identifying data." EX1010, ¶[0025], FIGS. 2-3. "The RF reader transmits an interrogation signal and then listens for a response signal and/or

message from the RFID circuitry of the proximity payment device." EX1010, ¶[0025]. Cooke's readers operate in accordance with the Master Card "PayPass®" standard "for interoperability of contactless payment cards and proximity readers." EX1010, ¶¶[0003], [0025].

K. Combination of Mardikar and Cooke

119. A POSITA would have combined Mardikar and Cooke such that:

1) Mardikar's biometrically-secured mobile/cellular device would have been configured to respond to a POS-incorporated NFC reader's interrogation signal, as taught by Cooke; and
2) Mardikar's device would have returned its stored transaction information (e.g., payment instrument / account number) in response to that interrogation signal, as taught by Cooke, gated by Mardikar's on-device biometric authentication.

120. Mardikar discloses a mobile/cellular device that captures a fingerprint, compares it against a stored biometric signature on the Crypto SE, and — only upon a match — transmits a secure payment message containing the payment instrument to an NFC POS reader. EX1009, 6:42-10:24, 11:29-12:43, 15:53-16:45 (cl. 1), FIGS. 6a, 6c. Mardikar expressly contemplates operation with "Near Field Communication Point of Sale devices (NFC POS)." EX1009, 6:50-7:3. Mardikar, however, describes the transaction primarily from the perspective of the device

(prepare device, capture biometric, then tap the reader), and does not dwell on the reader-side signaling that initiates the exchange.

121. Cooke supplies that reader-side detail. Cooke expressly teaches that the proximity reader is "conventionally incorporated with a Point-of-Sale (POS) terminal" and transmits an interrogation signal, and that the payment circuit of the proximity payment device "respond[s] to an interrogation signal from an NFC reader by transmitting payment account information such as a payment card account number (PAN) or other identifying data." EX1010, ¶¶[0003], [0025], FIGS. 2-3. Cooke further teaches that the responding proximity payment device may be a payment-enabled mobile telephone. EX1010, ¶¶[0004], [0016], [0021], [0025], [0041], [0050].

122. A POSITA would have predictably combined Mardikar and Cooke for the following reasons.

123. *First*, both references are directed to NFC contactless payment in the same ecosystem (ISO 14443 / NFC / PayPass), and Cooke expressly names payment-enabled mobile telephones as the proximity payment device. EX1009, 6:50-7:3; EX1010, ¶¶[0003], [0025], [0029]. Configuring Mardikar's mobile/cellular device to answer a standard POS NFC interrogation, as taught by Cooke, would have made Mardikar's device interoperable with the widely-deployed contactless-POS infrastructure that Cooke describes.

124. *Second*, the combination is nothing more than the use of a known technique (Cooke's reader-initiated interrogation/response) to improve a similar device (Mardikar's NFC-enabled mobile/cellular device) in the same way it improves contactless payment cards — yielding the predictable result of a POS-initiated, device-response transaction.

125. *Third*, the combination would have had a reasonable expectation of success because Mardikar's device already includes the NFC communication chip 405 and antenna 407 used to receive an interrogation signal and transmit a response, and Cooke's interrogation/response operation is the conventional PayPass/ISO 14443 exchange those components are designed to perform. EX1009, 5:34-7:26; EX1010, ¶¶[0003], [0025], [0029].

L. Overview of Lee

126. Lee is directed to a mobile phone that conducts NFC communications with an external RF reader at 13.56 MHz. EX1011, 5:30-48, 6:27-50. For example, the RF antenna in the mobile phone operates at 13.56 MHz. EX1011, 6:27-50, 7:53-65.

M. Lee Combined with Mardikar and Cooke

127. As explained above in [1.2], MCC's short range radio frequency circuit includes RF (NFC) circuitry such as a communication chip 405 and antenna

407. EX1010, ¶¶[0003], [0025], [0021]; EX1009, 6:43-67. Mardikar and Cooke are silent as to which frequency its NFC circuitry operates at.

128. It was however well-known in the art that NFC communications used 13.56 MHz. For example, as noted above in §VII.L, Lee teaches that its mobile phone's RF antennas used 13.56 MHz for NFC communications. EX1011, 6:27-50, 7:53-65, 5:30-48.

129. It would have been obvious for a POSITA looking to implement the NFC communications described in the MCC system to turn to Lee's teachings to determine which frequency (13.56 MHz) to use for conducting the NFC communications performed between the mobile/cellular device and the POS device. Doing so would have simply amounted to combining prior art elements according to known methods to yield predictable results.

130. Combining the teachings of Lee with MCC would have been predictable with a reasonable expectation of success for several reasons.

131. First, using Lee's 13.56 MHz frequency would have been an obvious choice for a POSITA because 13.56 MHz was a well-known frequency used for NFC communications. For instance, 13.56 MHz was the standard frequency used for International Organization for Standardization (ISO) 14443A, a B reader, a Milfare reader and a Felica reader. EX1011, 5:30-48, 7:53-65.

132. Second, like the MCC system, Lee also describes using an RF antenna for near field communications between a mobile device and a RF reader. EX1011, Abstract, 5: 207:65. The MCC system would only have to be predictably modified to the extent of configuring its short range communication settings and components to use 13.56 MHz. Doing so would have been consistent with Mardikar's system, which is already designed to support various networks, and a routine modification well within the capabilities of a person of ordinary skill in the art. EX1009, 6:43-67.

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '513 CLAIMS UNPATENTABLE

A. GROUNDS 1A AND 2A: Wang in view of Barnes or Srey Renders Claims 1-9, 11-17, 19-25 Obvious

i. Claims 1 and 11

[1.pre] A mobile device, comprising:

[11.pre] A cellular telephone, comprising:

133. Each of the Wang-Barnes and Wang-Srey combinations renders obvious a "***cellular telephone***"/"***mobile device***" that operates as or includes a PEAD/PECAD.

134. Wang discloses a PEAD 200 that is "implemented using a general purpose portable computing device, such as any of the miniaturized portable computers or personal digital assistants (PDA's) that are currently popular. A

PDA such as the Apple Newton®, for example, may be employed to implement PEAD 200." EX1004, 20:21-25, 10:6-23. An example of a PEAD 200 is shown in FIGS. 2 and 6 below. EX1004, 8:9-26.

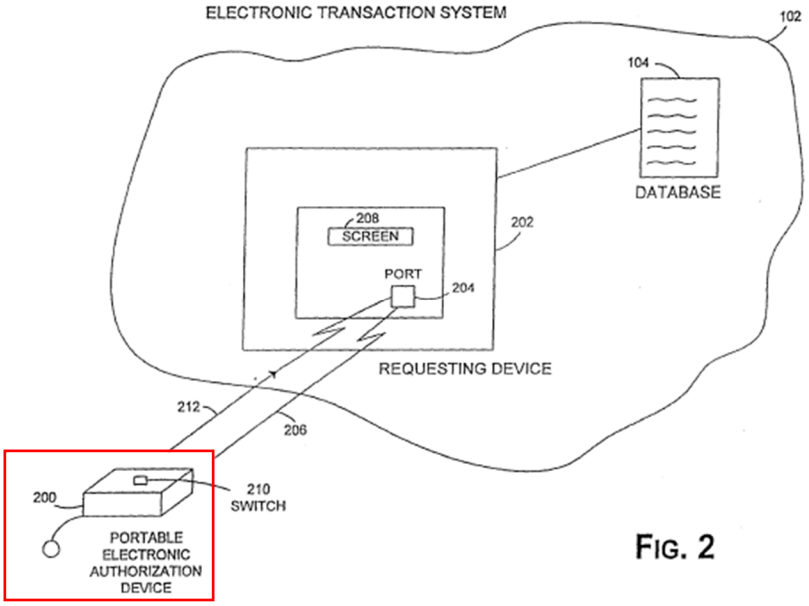


FIG. 2

EX1004, FIG. 2[6].

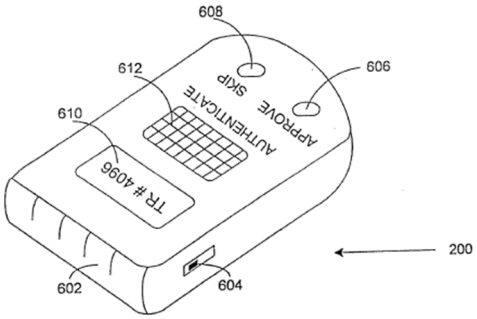


FIG. 6A

[6] Here and throughout my declaration, annotations to the figures have been added in color.

EX1004, FIG. 6A.

135. Wang's PEAD "is small enough to be comfortably carried with the user at all times." EX1004, 21:22-25. Accordingly, at least because the PEAD is a portable electronic device and because portable computers and PDAs are mobile devices, Wang discloses a "***mobile device***."

136. The PECAD incorporates PEAD functionality and also "permit[s] the user to conduct transactions vis-a-vis the existing charge card infrastructures." EX1004, 25:19-35:30. Thus, the remarks associated with the PEAD also apply to the PECAD, and the PECAD also maps onto the "***mobile device***."

137. As explained above in §§VII.B-VII.C and §§VII.E-VII.F, in the Wang-Barnes or Wang-Srey combination systems, the PEAD operates as a "***cellular telephone***" thereby enhancing its capability to communicate over a cellular network. EX1005, 4:27-30, FIG. 1, 5:35-51, 7:48-50, 16:36-39; EX1006, Abstract, 2:46-64, 3:36-42, FIG. 1. And because "***cellular telephone[s]***" are also "***mobile device[s]***," the combination of Wang with Barnes or Srey renders [1.pre]/[11.pre] obvious. EX1005, 4:27-30 ("The present invention is a multi-function communications device 101 that includes *conventional mobile phone*")[7].

[7] Here and throughout my declaration, emphasis is added to prior art quotes using italicized font.

[1.1] a biometric input device configured to receive biometric data;

[11.1] a fingerprint scanner configured to receive fingerprint data;

138. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.1]/[11.1] at least because user authentication mechanism 612 ("***biometric input device***"/"***fingerprint scanner***") is configured to receive ***"biometric data"/"fingerprint data***."

139. Referring to Wang's FIG. 6A, Wang's PEAD includes a user authentication mechanism 612 that, in some cases, requires a user "to furnish a fingerprint or a voice print, or other biometrics and/or identifying characteristics specific to the authorized user before [the] PEAD 200 can be activated and employed for approving transactions." EX1004, 22:14-25.

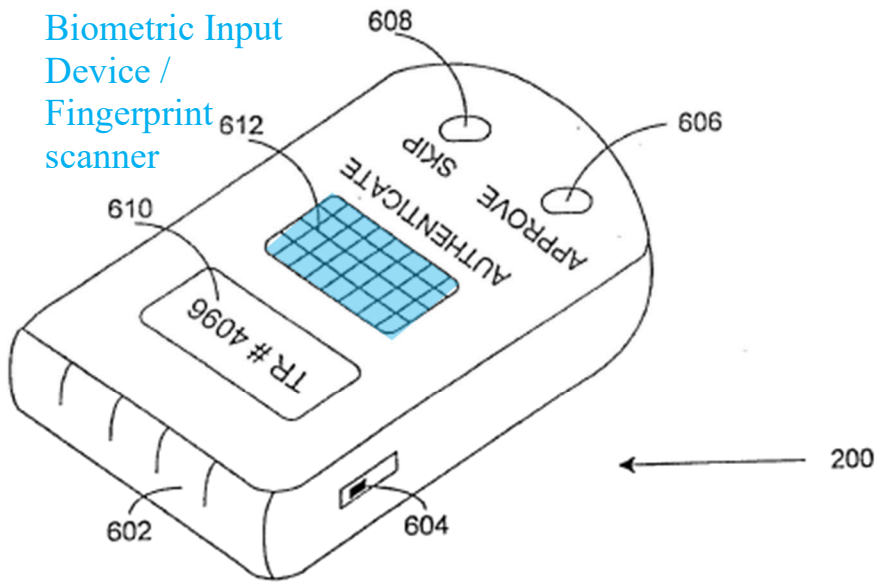


FIG. 6A

EX1004, FIG. 6A.

140. Relatedly, Wang's claims 12 and 30 recite "wherein said authentication mechanism employs fingerprint for authentication," and such an authentication mechanism is illustrated above as item 612 with the label "AUTHENTICATE." EX1004, 38:5-7, 40:27-28. Accordingly, a POSITA would have understood that Wang's authentication mechanism operates as a "***biometric input device***"/"***fingerprint scanner***" configured to receive ***"biometric data"/"fingerprint data***." Barnes and Srey corroborate this understanding.

Ground 1A

141. Barnes teaches that authentication information such as fingerprint data is stored on the cellular phone to authenticate a user. EX1005, 17:38-48, 18:42. Like Wang, user authentication may be required to permit a commercial transaction. EX1005, 18:1-6. To authenticate a user, fingerprint data is received through a fingerprint scanner and then compared to stored fingerprint data. EX1005, 18:13-18, 21:1-14. Accordingly, it would have been obvious to a POSITA that in the Wang-Barnes combination, Wang's authentication mechanism would have been a "***biometric input device***"/"***fingerprint scanner***."

Ground 2A

142. Similarly, Srey discloses the use of a fingerprint scanner 115 to obtain fingerprints which are then compared with stored fingerprints to authenticate a user. EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7. Thus, in the Wang-Srey combination, it would have been obvious to a POSITA that Wang's authentication mechanism would have been a "***biometric input device***"/"***fingerprint scanner***."

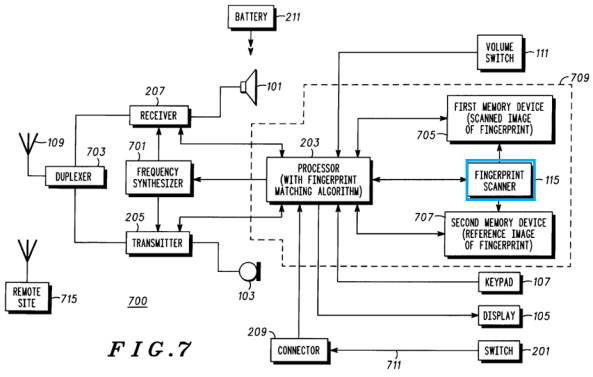


FIG. 7

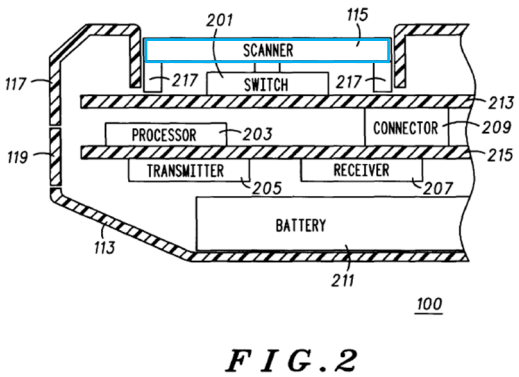


FIG. 2

EX1006, FIGS. 7, 2.

[1.2] a short range radio frequency circuit;

[11.2] a short range radio frequency circuit;

143. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.2]/[11.2] at least because Wang's PEAD includes a communication port 510 ("***short range radio frequency circuit***") that performs short range communications using wireless RF technology. EX1004, 19:13-26.

144. Wang's PEAD is used to conduct transactions with point of sale terminals, including e.g., charge card readers and ATM terminals, that are known to be used in short range transactions. EX1004, 10:6-23, 25:11-18. Accordingly, it would have been obvious to a POSITA that Wang's communication port 510 is "***a short range radio frequency circuit***," e.g., when it is communicating using wireless RF signals with charge card readers and ATM terminals located in close proximity to the PEAD.

145. Moreover, a POSITA would have understood that because infrared communications are short range, Wang's communication port is designed to operate over short range communications, e.g., a few centimeters to 2 meters. EX1004, 10:20-11:12, 19:13-26; EX1015, 1-3 (a Wikipedia page for the Infrared Data Association explaining that infrared communications are typically used for short-range communications, e.g., from between 5 centimeters to 2 meters).

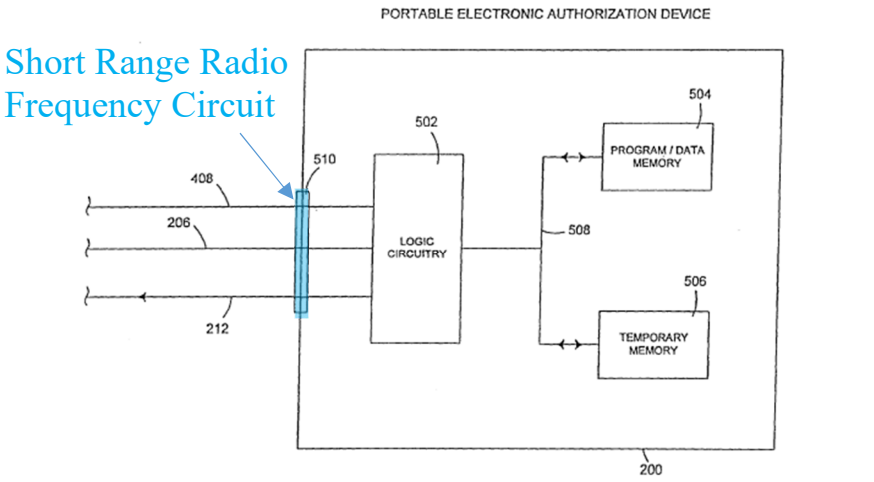


FIG. 5A

EX1004, FIG. 5A.

Additional Disclosure Relevant to Ground 1A

146. Barnes's device includes a short range wireless LAN module (e.g., a Bluetooth module) that allows the device to communicate and wirelessly exchange payment information with point of sale (POS) devices using a RF frequency, e.g., 2.4 GHz. EX1005, 7:3-25. Barnes's device can include different circuitries in the form of different antennas to communicate with different networks, respectively. EX1005, 9:25-50. Barnes also teaches that all or part of its communication module (used to communicate with external devices) "is implemented with one or more application specific integrated circuits (ASICs) and software stored in memory." EX1005, 6:1-13. Thus, Barnes teaches the use of antennas and ASICs to support LAN or short range communications. In the Wang-Barnes combination and for the reasons previously explained in §VII.E, it would have been obvious to a POSITA

that Wang's communication port 510 would have included or be implemented as Barnes's short range RF wireless LAN module and LAN circuitry to facilitate transaction communication with a POS device.

[1.3] memory configured to store biometric information for identifying an individual associated with transaction information;

[11.3] memory configured to store fingerprint information for identifying an individual associated with transaction information;

147. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.3]/[11.3] at least because Wang discloses a ***memory*** 504 configured to store user identification information ("***biometric information for identifying an individual associated with transaction information***") in the form of fingerprint information.

148. Wang teaches that "[p]rogram/data memory 504 stores, among others, the codes which operate PEAD 200 as well as the user identification data and the user's private key." EX1004, 18:31–33; *see also* FIG. 6B – flash memory 656; 22:27-35.

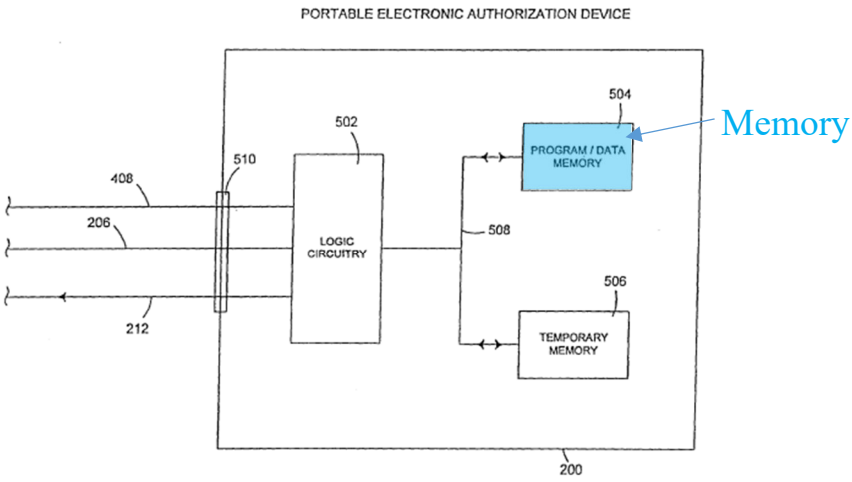


FIG. 5A

EX1004, FIG. 5A.

149. Wang's user identification data "may include any of the user's name, his birth date, his social security number, or *other unique biometrics or unique identifying data such as fingerprint, DNA coding sequence, voice print*, or the like." EX1004, 13:19–22. The identification data is for the user associated with a charge card (e.g., credit card) and a charge card transaction ("***individual associated with transaction information***") using the charge card. EX1004, Abstract ("[a] portable transaction arrangement for permitting a user to conduct a charge card transaction vis-a-vis a charge card terminal of an electronic transaction system"); 5:8-10; 25:32-35 (The charge cards themselves may represent credit cards (such as Visa or Master Cards)"). In some cases, the user must "furnish a fingerprint … or other biometrics and/or identifying characteristics" for authentication prior to approval of a transaction involving the user. EX1004, 22:14-25.

150. As explained above in [1.1], Barnes and Srey also teach storing fingerprint data to be used for comparison with received fingerprint data when authenticating a user. EX1005, 18:1-18, 21:1-14; EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7. Accordingly, each of the Wang-Barnes and Wang-Srey combinations renders [1.3]/[11.3] obvious.

[1.4] a processor coupled with the memory and the biometric input device, the processor configured to:

[11.4] a processor coupled with the memory and the fingerprint scanner, the processor configured to:

151. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.4]/[11.4] at least because Wang discloses logic circuitry 502 ("***a processor***") that is "***coupled with the memory"*** and the user authentication mechanism ("***biometric input device***"/"***fingerprint scanner***").

152. As shown in Wang's FIG. 5A below, Wang's "PEAD 200 includes logic circuitry 502, which may represent a *central processing unit such as a microprocessor or a microcontroller*, discrete logic, programmable logic, an application-specific integrated circuit (ASIC)." EX1004, 18:26-30; *see also* FIG. 6B (microcontroller 654), 22:26-23:9. "*A bus 508 couples program/data memory 504* and temporary memory 506 *with logic circuitry 502*." EX1004, 19:13-14. Thus, the Wang-Barnes and Wang-Srey devices each include "***a processor coupled with the memory***."

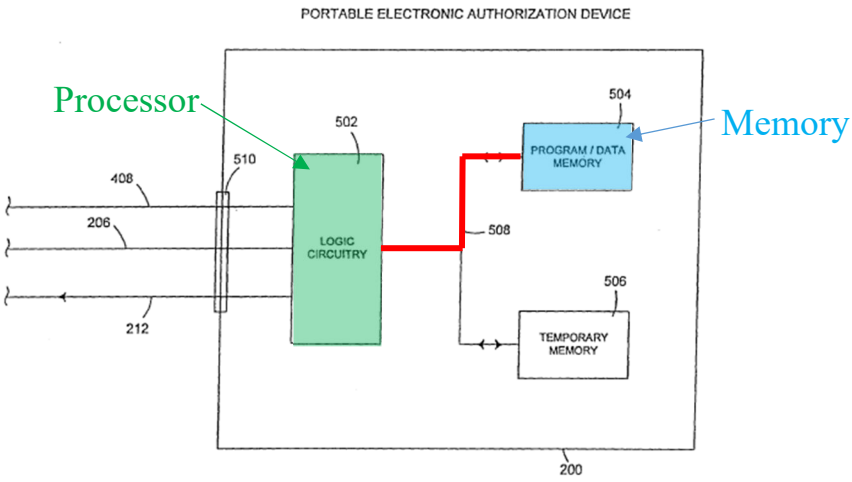


FIG. 5A

EX1004, FIG. 5A.

153. It would have been obvious to a POSITA that the logic circuitry 502 ("***processor***") is also coupled to the user authentication mechanism ("***biometric input device***"/"***fingerprint scanner***") under both grounds for several reasons.

154. First, as noted above in [1.3], the memory 504 stores user identification data such as the user's fingerprints. EX1004, 18:31–33, 13:19–22. It would have been obvious to a POSITA that a user would have scanned the user's fingerprint through the user authentication mechanism (e.g., fingerprint scanner) and the scanned fingerprint data would then be sent to memory 504 for storage. EX1004, 22:14-25; *see* [1.1]. Thus, a POSITA would have recognized that the user authentication mechanism is coupled to memory 504, which itself is coupled to the logic circuitry 502. Therefore, the authentication mechanism would have been at least indirectly coupled to the logic circuitry.

155. Second, Wang teaches that "*reading* the *user identification data* and accessing the user's private key *can only be accomplished via the encryption logic of logic circuitry 502*." EX1004, 20:5-10. And because Wang also teaches that "access to program/data memory 504 and the data therein … can only be made by logic circuitry 502," a POSITA would have understood that the logic circuitry would have been coupled to the user authentication mechanism from which user identification data is obtained or the memory 504 storing the fingerprint data. EX1004, 19:27–29.

156. Third, it would have been obvious to a POSITA that a processor would have authenticated a user's fingerprints prior to approving a transaction, as explained above in [1.3]. EX1004, 22:14-25. Indeed, using fingerprints for performing biometric authentication of a user using a processor in a cell phone was well-known. For example, Iwanaga (EX1013) discloses the use of a CPU or fingerprint processor in a cell phone to perform fingerprint authentication. EX1013, claims 12 ("wherein said fingerprint authentication device comprises a fingerprint processor configured to process the reference fingerprint image stored in said memory"), FIGS. 1A, 2, ¶¶[0054]-[0056]. Similarly, Harkin (EX1014) explains that there was "considerable interest in the use of fingerprint sensing for user identification or verification purposes. For this, a person's fingerprint is acquired by means of a fingerprint sensing device whose output is processed and

compared with stored characteristical data of one or more fingerprints to determine whether a match exists." EX1014, 1:9-15. Harkin also explains that it was known in the art to use "fingerprint sensing devices in other portable electronic equipment such as mobile phones and smart cards as a means of preventing unauthorised usage." EX1014, 1:35-46, 2:30-35, 4:8-35, 10:15-50, FIG. 7. Because the logic circuitry is the only processor shown in Wang's FIG. 5A, it would have been obvious that the logic circuitry would have been coupled to the user authentication mechanism, through which a user would have provided the user's fingerprints.

Additional Disclosure Relevant to Ground 2A

157. As shown in Srey's FIG. 7 below, Srey's fingerprint scanner 115 and second memory 707 storing a reference fingerprint image are both coupled to a processor 203. EX1006, FIG. 7, 4:64-5:10. Because the fingerprint scanner 115 is implemented as part of Wang's user authentication mechanism ("***biometric input device***") and Wang's logic circuitry would perform the same fingerprint comparison operations as Srey's processor 203, it would have been obvious to a POSITA that in the Wang-Srey device, the "***processor [is] coupled with the memory and the biometric input device***"/"***fingerprint scanner***." *See also* §VII.F.

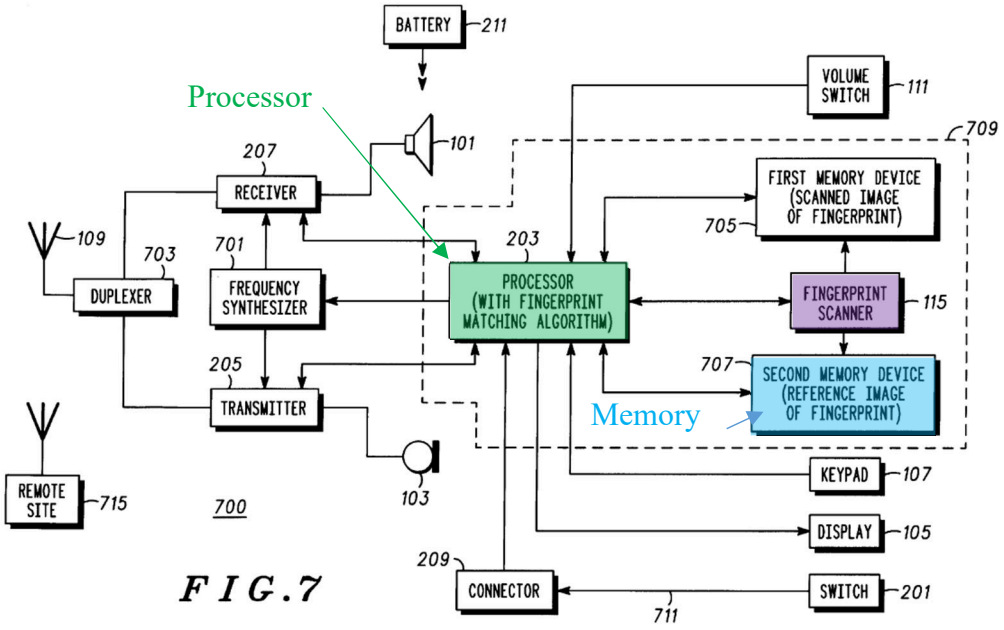


FIG. 7

EX1006, FIG. 7.

158. As explained below in [1.5.1]-[1.8]/[11.5.1]-[11.8], Wang's logic circuitry also performs the recited operations in [1.5.1]-[1.8]/[11.5.1]-[11.8].

> ***[1.5.1] receive a signal from a point of sale terminal via the short range radio frequency circuit,***
>
> ***[11.5.1] receive a signal from a point of sale terminal via the short range radio frequency circuit,***

159. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.5.1]/[11.5.1] at least because the logic circuitry in Wang's PEAD 200 "***receive[s] a signal from***" a requesting device 202 ("***a point of sale terminal***") via the communication port 510 ("***via the short range radio frequency circuit***").

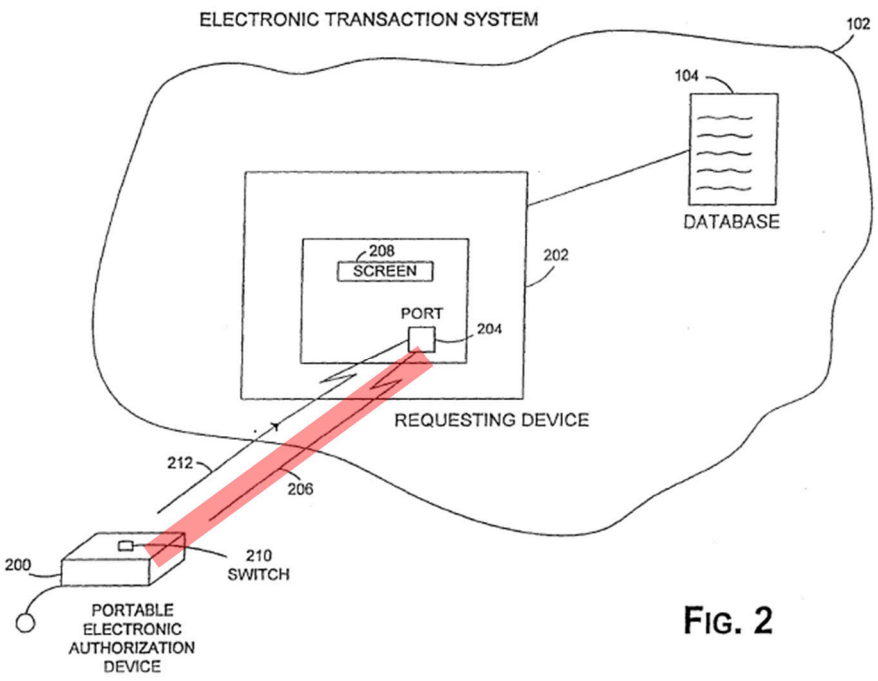


FIG. 2

EX1004, FIG. 2.

160. As shown above in Wang's FIG. 2, the PEAD 200 receives a signal 206 from a requesting device 202. EX1004, 10:13-22, 14:6-7 ("Data path 206 is provided for receiving transaction requests from the electronic transaction system"). Various types of requesting devices can be used including "for example, an ATM machine, a computer terminal in a network, an automated library check-out terminal, or *similar devices for permitting the user to transact business with the electronic transaction system*." EX1004, 10:13-16. Wang explains that point-of-sale systems are devices used to permit a user to conduct an electronic transaction with the PEAD. EX1004, 3:26-4:9; 25:11-13 ("PEAD and the PEAD-enabled point of sale terminals offer a highly secure system for approving transactions");

25:19-24 ("a portable electronic charge/approval device (PECAD), which not only offers the aforementioned PEAD functionality to permit a user *to approve a transaction vis-a-vis a PEAD-enabled point of sale terminal*"). Accordingly, it would have been obvious to a POSITA that Wang teaches "***receiv[ing] a signal from a***" requesting device that is a "***point of sale terminal***."

161. Wang also teaches that the signal 206 is received at the communication port 510. As shown in FIG. 2 above and FIG. 5A below, "[c]ommunication port 510 represents the communication gateway between PEAD 200 and the electronic transaction system," and data received through the port 510 is then provided to the logic circuitry ("***processor***"). EX1004, 19:13-26 ("Data path 206 inputs transaction requests into logic circuitry 502").

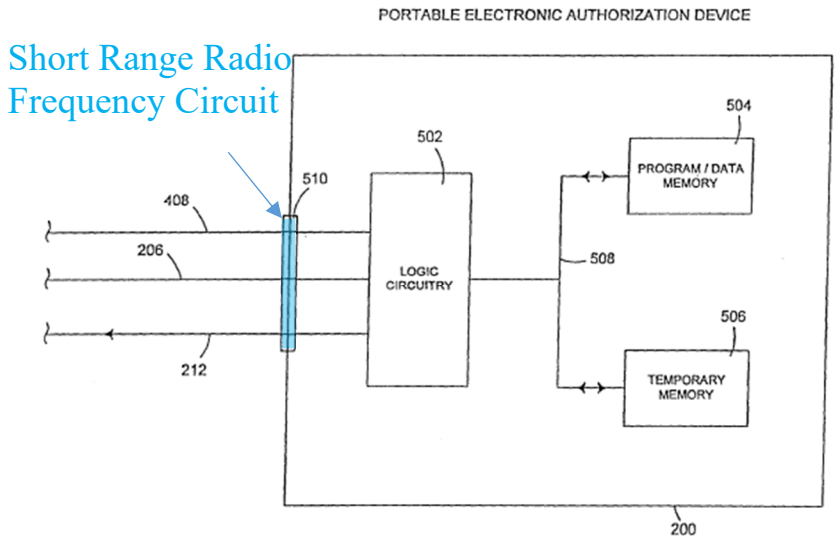


FIG. 5A

EX1004, FIG. 5A.

162. As explained above in [1.2], in the Wang-Barnes and Wang-Srey devices, the communication port 510 is a "***short range radio frequency circuit.***" Accordingly, Wang in view of Barnes or Srey renders obvious [1.5.1]/[11.5.1].

Additional Disclosure Relevant to Ground 1A

163. Barnes explicitly teaches that its device communicates with a point of sale device to conduct a transaction using its short range wireless LAN module. EX1005, 3:53-4:25, 7:3-24, 29:39-50. As explained above in [1.2], the short range wireless LAN module is the "***short range radio frequency circuit***" in the Wang-Barnes device. For this additional reason, Wang-Barnes renders [1.5.1]/[11.5.1] obvious.

[1.5.2] the signal comprising a request to access the memory and retrieve the transaction information,

[11.5.2] the signal comprising a request to access the memory and retrieve the transaction information,

164. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.5.2]/[11.5.2] at least because Wang's "***signal***" received by the PEAD includes "***a request to access the memory and retrieve the transaction information***." EX1004, 10:13-22, 14:6-7; *see* [1.5.1].

"***Request to Access the Memory***"

165. Wang teaches that when a transaction request in the "***signal***" is received from the requesting device (as explained above in [1.5.1]), a user

approves or disapproves the request. EX1004, 14:16-25. Wang explains that "[i]n some cases, *the transaction approval data requires the inclusion of certain pieces of identification data 302*. For example, a transaction embodied in the transaction request from the electronic transaction system may be appended with data representative of an 'electronic signature' prior to being encrypted and retransmitted back to the electronic transaction system." EX1004, 15:11-23, FIG. 3B. Wang also explains that transaction information, such as credit card information, is stored in the device memory, and, after user authentication, the credit card information is transmitted to the POS reader. EX1004, Abstract, 14:17-25, 15:11-24.

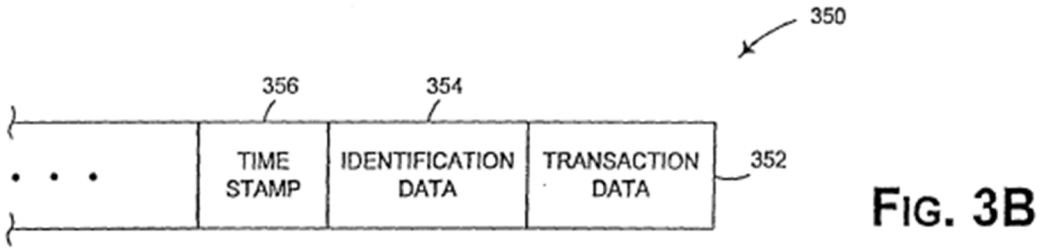


FIG. 3B

EX1004, FIG. 3B.

166. Recall from [1.3] that user identification data and a user's private key are written into the PEAD's memory. EX1004, 17:12-16 ("Advantageously, the sensitive user identification data and user's private key therein are not susceptible to access from outside once written into respective blocks 410 and 304 (which may, in one implementation, simply represent memory blocks in PEAD 200's memory)"); 18:31-33, 15:6-10; *see also* FIG. 6B – flash memory 656; 22:27-35.

167. A POSITA would have understood that for transactions that *require* "the inclusion of certain pieces of identification data 302," the received transaction request would have obviously included a "***request to access the memory***" so that identification data and/or transaction information can be accessed from the memory to respond. EX1004, 15:11-23.

168. US Patent No. 5,698,836 ("Fujioka") corroborates this POSITA understanding. Fujioka explains that a memory can be divided into a user area UA (that stores personal information and account information) and a system area SA. EX1016, 5:14-34, FIG. 2. When a first device is seeking information from a second device with this memory, the first device sends a read command to request the second device to access its memory and provide the requested information. EX1016, 6:3-20. In the same manner, Wang's request for the inclusion of certain pieces of identification data 302 in a response, would have been understood as an instruction to read the identification data from the memory of Wang's mobile device.

169. Relatedly, for highly sensitive, encrypted transactions: 1) a received transaction request is encrypted and has to be decrypted by the PEAD, and 2) an approval response may be encrypted before being transmitted to the requesting device. EX1004, FIGS. 3A-4, 15:11-18:23. For instance, Wang explains that "[f]or highly sensitive transactions, however, the transaction requests may be

encrypted and transmitted to PEAD 200 via data path 206 and input into decryption logic 402 to be decrypted." EX1004, 16:13-18. "Once decrypted, the transaction request is then displayed to the user for approval. The transaction approval data may be furnished to encryption logic 300 … to be encrypted if approved … . The encryption is preferably performed with the user's private key 304," which is stored in memory 504. EX1004, 16:20-26, 18:31-19:12, 19:22-26, 14:33-15:10, 38:11-14 (claim 14), 40:5-8 (claim 23). Access to the memory for encryption or decryption purposes is controlled by the logic circuitry 502 to prevent unauthorized access to the memory. EX1004, 19:27-20:11.

170. A POSITA would have understood that a received transaction request for a sensitive transaction would have obviously included ***a request to access memory*** locations where: 1) a decryption key is stored so that the received encrypted request can be decrypted, and 2) an encryption key is stored to encrypt a response to the transaction request. EX1004, 15:24-29, 16:7-19, 16:20-26 ("encryption is preferably performed with the user's private key 304 if a public key cryptography technique is employed, and the encrypted transaction approval data is then transmitted back to the electronic transaction system via data path 212"), 17:12-16, 18:31-33 ("memory 504 stores … user identification data and the user's private key").

"***[R]etrieve the transaction information***"

171. As a preliminary matter, it would have been obvious that Wang's PEAD would have to retrieve and return transaction information to the POS device (requesting device) in an electronic transaction system to complete a transaction. Thus, a POSITA would have understood that a signal received from the POS device would have obviously included a request to retrieve transaction information to complete the transaction. Wang's disclosure confirms the same.

172. Recall from [1.3] that Wang's transaction information encompasses credit card information to be used in a credit card transaction and that Wang's system is configured to "permit[ ] a user *to conduct a charge card transaction* vis-a-vis a charge card terminal of an electronic transaction system." EX1004, Abstract. Recall also from [1.5.1] that the transaction is conducted between Wang's PEAD 200 and a POS device (requesting device) in an electronic transaction system. EX1004, 3:26-4:9; 25:11-13, 10:13-22, 14:6-7, 25:19-24, FIG. 2. Thus, when the transaction request involves a transaction such as a "purchase from a vendor" having a POS device, it would have been obvious that the request would have requested payment information including at least credit card information. EX1004, 1:23-35, 15:12-23.

173. Wang describes an example in which a credit card-based transaction is described. For instance, Wang discloses a "portable electronic charge/approval device (PECAD)" that includes "the aforementioned PEAD functionality to permit

a user to approve a transaction vis-a-vis a PEAD-enabled point of sale terminal" and "permit[s] the user to conduct transactions vis-a-vis the existing charge card infrastructures. In particular, the complete PECAD system includes a PECAD and an associated emulation card which conforms to current charge card standards as far as its interface with existing charge card readers is concerned." EX1004, 25:19-30. "The charge cards themselves may represent credit cards (such as Visa or Master Cards), ATM cards, royalty cards, discount cards, as well as any other type of cards with which a user may employ vis-a-vis a point-of-sale terminal to obtain cash, goods, and/or services." EX1004, 25:33-26:6. "Prior to conducting a transaction, the PECAD has in its memory charge card data pertaining to one or more charge cards of the user. To perform the PEAD functionality, the memory may also include other data items discussed earlier in connection with the PEAD." EX1004, 26:7-10.

174. The charge/credit card information can be stored in a nonvolatile, tamper-proof memory that also stores the user's private key. EX1004, 28:27-35, FIG. 9. Thus, a POSITA would have understood that charge/credit card information is also stored in memory 504 (when in a PEAD, or in memory 904 when used in a PECAD).

175. Because the emulation card can be used "as if it were a charge card" and can emulate a number of charge cards, a POSITA would have understood that

a transaction request would have included a request to access and provide charge/credit card information ("***retrieve the transaction information***") to pay for the transaction. EX1004, 26:20-35; *see also* EX1005, 22:57-23:48, 30:22-33. Indeed, as evidenced by Zicker (US Patent No. 5,144,649), it was well-known as far back as 1992 to use cell phones and make credit card payments in response to messages. EX1012, 1:20-27, Abstract, 19:30-50.

176. Similarly, for transactions that require "the inclusion of certain pieces of identification data 302," an electronic signature is obtained from the memory and included as part of a transaction response. EX1004, 15:11-23, FIG. 3B. A POSITA would have understood that the electronic signature is part of the "***transaction information***" at least because it is used to complete the transaction. For example, US Patent Application Publication No. 2001/005641 (Ishigaki) explains that an electronic signature was known to be used as part of information transmitted to conduct an electronic transaction. EX1017, Abstract, ¶¶[0011]-[0013]. Accordingly, it would have been obvious to a POSITA that a transaction request (for a transaction that requires the inclusion of certain pieces of identification data 302) would have also included "***a request to … retrieve the transaction information***."

Additional Disclosure Relevant to Ground 1A

177. Barnes "facilitate[s] commercial exchanges by wirelessly exchanging payment and product information with vendors." EX1005, Abstract, 2:28-41, 3:53-4:2. Payment information, including credit card or bank information, can be provided to a POS device using the commerce module and the short range wireless RF LAN module. EX1005, Abstract, 3:53-4:2, 7:3-24, 21:52-22:10, 29:39-46, 30:22-33 ("payment information, which is also retrieved from memory of the device"). Barnes explains that data indicating the format type for a payment is provided by a vendor to the user, and the commerce module then selects a payment account and corresponding format that is acceptable to the vendor by retrieving the information from a memory. EX1005, 22:11-56. The commerce module then "formats the payment information data in a manner that is appropriate for the receiving computer system" and transmits the payment information to the desired destination. EX1005, 22:57-23:48, 30:22-33.

178. Accordingly, it would have been obvious to a POSITA that, in the Wang-Barnes combination, the request received from the requesting device would have included a request to ***retrieve***, from the memory, ***transaction information*** such as payment information (e.g., credit card information) and format information to use when responding to the transaction request.

179. Barnes also describes an example scenario in which a vendor's point of sale device sends a request to store vendor stored user information (VSUI) in the

device or a request for identification information stored on the device when the device enters the vendor's store. EX1005, 49:37-67. It would have been obvious to a POSITA that both requests would have involved a request to access the memory in the Wang-Barnes device. For these additional reasons, Wang-Barnes render [1.5.2]/[11.5.2] obvious.

[1.6] receive the biometric data from the biometric input device,

[11.6] receive the fingerprint data from the fingerprint scanner,

180. As explained above in [1.1], each of the Wang-Barnes and Wang-Srey devices "***receive[s]***" fingerprint data ("***biometric data***"/"***fingerprint data***") from the user authentication mechanism 612 ("***biometric input device***"/"***fingerprint scanner***"). EX1004, 22:14-25, 38:5-7, 40:27-28, FIG. 6A (reproduced below); EX1005, 17:38-48, 18:1-42, 21:1-14; EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7.

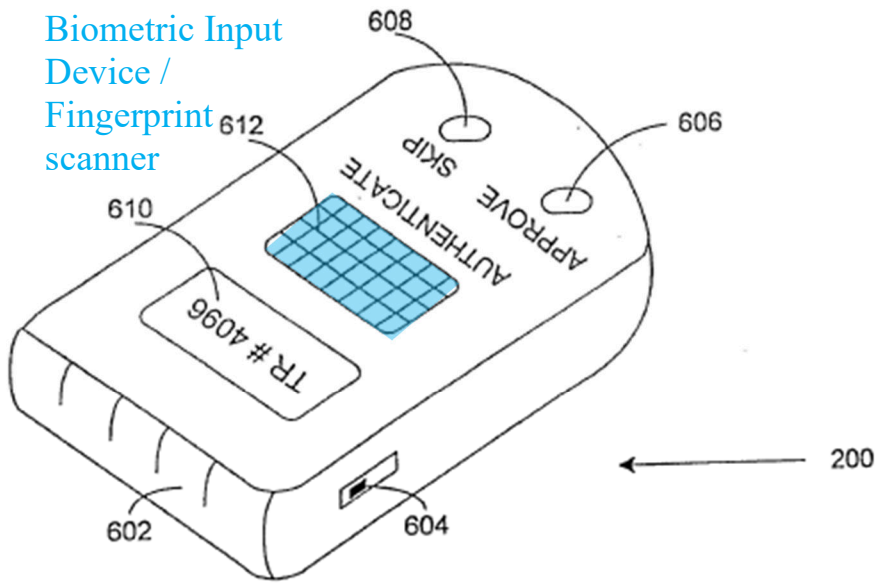


FIG. 6A

EX1004, FIG. 6A.

181. Wang also teaches that user identification data, such as fingerprints, are never exposed and are only accessible to the logic circuitry 502 ("***processor***"). EX1004, 19:27-20:11, 13:16-35, 22:18-25. And because the logic circuitry is the only processor in Wang's PEAD it would have been obvious to a POSITA that the logic circuitry 502 ("***processor***") receives the biometric/fingerprint data from the biometric input device/fingerprint scanner for comparing, as further explained in the next section.

182. Wang does not impose strict limits on when its fingerprint-based user authentication method leaving implementation of the method open to routine

design choices known to a POSITA. For instance, to the extent a switch 210 should be activated to approve a transaction, the fingerprint matching can be performed before or after activation of the switch. EX1004, 11:5-22.

[1.7] compare the received biometric data with the biometric information stored in the memory, and

[11.7] compare the received fingerprint data with the fingerprint information stored in the memory, and

183. Each of the Wang-Barnes and Wang-Srey devices "***compare[s]***" received user "***fingerprint/biometric data***" with "***fingerprint/biometric information***" stored in memory 504 ("***memory***").

184. As explained in [1.1], Wang teaches that before approving a transaction, a user may be required to input the user identification data, such as fingerprints, for user authentication. EX1004, 22:14-25, 13:16-22, 24:24-32, 38:5-6 (claim 12), 40:27-28 (claim 30). Only after the user authentication is complete is the transaction approval sent. EX1004, 22:14-25, 24:24-32, 26:20-28. Such user identification data is stored in memory 504. EX1004, 22:14-25, 34:23-25, 14:26-15:24, 18:31-33 ("Program/data memory 504 stores, among others, … the user identification data"). Recall from [1.6], that the logic circuitry ("***processor***") receives the biometric data from the biometric input device. And because only the logic circuitry 502 can access the memory 504 and user identification information, it would have been obvious that the logic circuitry ("***processor***") performs the user

authentication by comparing the received and stored fingerprints. *See also* §VIII.A.i.[1.6].

185. For the Wang-Barnes device under Ground 1A, Barnes teaches that fingerprint data is received through a fingerprint scanner and then compared to stored fingerprint data. EX1005, 18:13-18, 21:1-14.

186. For the Wang-Srey device under Ground 2A, Srey also teaches that fingerprints obtained through fingerprint scanner 115 are compared by processor 203 to stored fingerprints to authenticate a user. EX1006, 2:46-67, 3:33-4:5, 4:49-6:16, FIGS. 2, 7.

187. Accordingly, under both Wang-Barnes and Wang-Srey, a POSITA would have understood that fingerprint authentication involves the processor comparing received (via fingerprint scanner) user fingerprint data with stored fingerprint data.

> ***[1.8] transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and***
>
> ***[11.8] transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information; and***

188. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.8]/[11.8] at least because Wang's PEAD "***transmit[s] the transaction***

information" to the requesting device ("***point of sale terminal***") using the communication port 510 ("***short range radio frequency circuit***") when the "***received fingerprint/biometric data matches the stored fingerprint/biometric information.***"

189. Specifically, Wang's user authentication involving fingerprint matching, as explained above in [1.6]-[1.7]/[11.6]-[11.7], can be implemented and "employed for approving transactions." EX1004, 22:14-25. And once a user approves the transaction, an approval message is created with the user's identification data, encrypted and transmitted back to requesting device 202 via path 212." EX1004, 11:5-22, FIG. 2 (reproduced below). As shown in Wang's FIGS. 2 and 5A below, "data path 212 outputs transaction approval data from logic circuitry 502 ["***processor***")] to the electronic transaction system." EX1004, 19:13-26. An example of the transaction approval data is shown below in FIG. 3B. EX1004, 15:15-17.

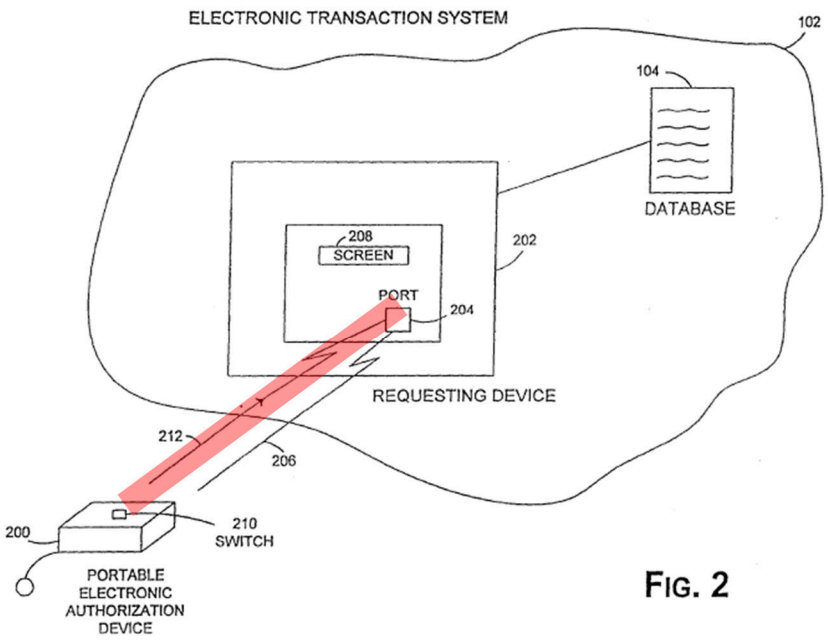


FIG. 2

EX1004, FIG. 2.

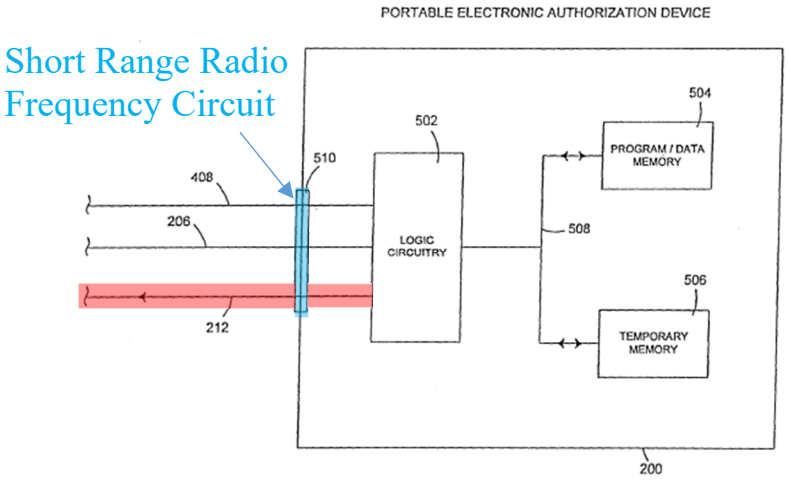
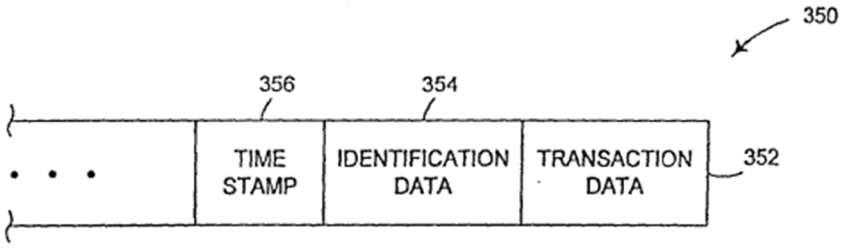


FIG. 5A

EX1004, FIG. 5A.



EX1004, FIG. 3B.

190. As explained above in [1.5.2] and shown in FIG. 3B above, the transaction information includes time stamp data, identification data, and transaction data such as credit card information, electronic signature and even the transaction ID, the merchant's name, the merchant's ID, and the time of the proposed purchase. EX1004, 15:11-23, 1:23-35, 10:13-23, FIG. 3B. For at least these reasons, Wang discloses the logic circuitry 502 ("***processor***") of the PEAD being configured to "***transmit the transaction information to the point of sale terminal using the short range radio frequency circuit***."

191. Recall also from [1.6] and [1.7] that user authentication, involving fingerprint matching, is required for highly secure transactions in Wang, and that the transaction information is sent when the received and stored fingerprints match. EX1004, 22:14-32, 13:16-22, 38:5-6 (claim 12), 40:27-28 (claim 30), 26:20-28, FIG. 6A. Accordingly, Wang also renders obvious that the transaction information is transmitted "***when the received biometric data matches the stored biometric information***."

[1.9] a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

[11.9] a mobile device[8] body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

192. Each of the Wang-Barnes and Wang-Srey combinations renders obvious [1.9]/[11.9].

193. Wang explains that the "PEAD 200 may be implemented using a general purpose portable computing device, such as any of the miniaturized portable computers or personal digital assistants (PDA's) that are currently popular." EX1004, 20:21-24. FIG. 6A depicts an example external view of the PEAD 200 in a mobile device body housing, and FIG. 5A shows that the PEAD 200 houses the biometric input device, short range radio frequency circuit, memory, and processor. EX1004, 20:18-21:35.

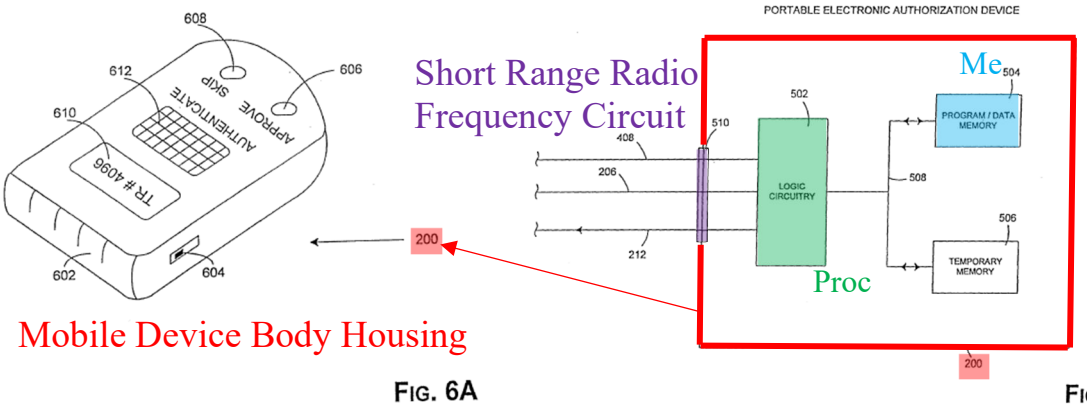


FIG. 6A FIG. 5A

[8] Feature [11.9] appears to have a typographical error and "mobile device" likely should be "cellular telephone" for consistency with [11.pre].

EX1004, FIGS. 6A, 5A.

194. As explained above, in the Wang-Barnes and Wang-Srey combinations, Wang's mobile device is implemented as or part of a cellular phone. An example of a cellular phone housing is shown in Srey's FIG. 1 below, and a POSITA would have understood that the cellular phone body would have housed the biometric input device, short range radio frequency circuit, memory, and processor.

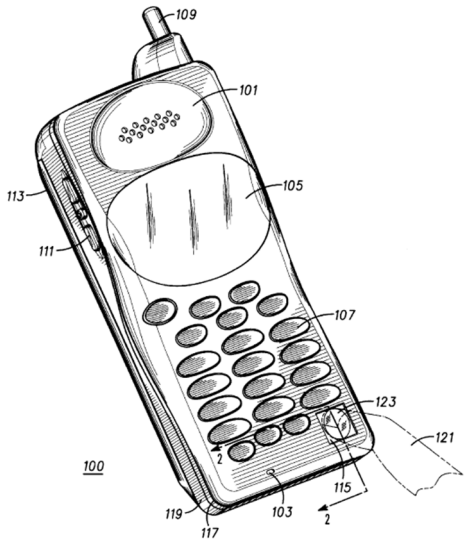


FIG. 1

EX1006, FIG. 1.

ii. Claim 19

195. Independent claim 19 differs from claims 1 and 11 in that the claimed device includes cellular circuitry (feature [19.1]) that is used to 1) receive a signal from a POS terminal (feature [19.6.1]), and 2) transmit the transaction information to a remote location, in place of a short range radio frequency circuit performing

these operations (feature [19.9]). As explained below, Wang-Barnes and Wang-Srey still render claim 19 obvious.

[19.pre] A cellular telephone, comprising:

196. *See* [1.pre]/[11.pre].

[19.1] cellular circuitry;

Ground 1A

197. As explained above in §VII.B, §VII.E, and [1.1], the Wang-Barnes device is a cellular phone. EX1005, 4:27-30, 5:35-51, 7:48-50, 16:36-39, FIG. 1. The Wang-Barnes's cellular phone can also communicate with multiple networks at the same time, including networks that a POSITA would have understood are cellular networks, such as 2G, 2.5G, 3G, and GSM networks. EX1005, 8:19-54, 9:51-12:49.

198. The Wang-Barnes's cellular phone includes ASICs and antennas to communicate with other networks, including the cellular networks noted above. EX1005, 6:1-14. 8:19-54, 9:7-50. Accordingly, it would have been obvious to a POSITA that Wang-Barnes's cellular phone includes "***cellular circuitry***" such as an ASIC and antenna.

Ground 2A

199. Wang-Srey renders obvious [19.1] at least because Srey teaches that its cellular phone includes "cellular circuitry" such as a transmitter 205 and

receiver 207 that are "mounted on the keypad printed circuit board 213" to facilitate cellular communications. EX1006, FIG. 2, FIG. 7, 4:49-5:10, 3:37-42.

[19.2] a fingerprint scanner configured to receive fingerprint data;

200. *See* [1.1].

[19.3] a short range radio frequency circuit;

201. Each of the cellular phones in the Wang-Barnes and Wang-Srey combinations include "***a short range radio frequency circuit***." *See* [1.2]. Although claim 19 recites a short range radio frequency circuit, unlike claims 1 and 11, the recited short range radio frequency circuit is not involved in any claimed operations or features of claim 19 or any of the other dependent claims. Thus, the mere presence of a short range radio frequency circuit in the Wang-Barnes's and Wang-Srey's mobile/cellular device is sufficient to satisfy [19.3].

[19.4] a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information;

202. See [1.3].

[19.5] a processor coupled with the memory and the fingerprint scanner, the processor configured to:

203. *See* [1.4].

[19.6.1] receive a signal from a point of sale terminal via the cellular circuitry,

Ground 1A

204. Barnes teaches that its device can communicate with multiple networks contemporaneously using its antennas. EX1005, 9:25-10:36. Barnes also teaches that its device can switch networks when one or more network switching conditions are present or a network is unavailable. EX1005, 11:5-12:23. Examples of when network switching conditions occur include when a network fails, has reduced bandwidth, capacity, or availability, and experiences increased noise among numerous other conditions. EX1005, 11:5-12:23. When "more than one network may be operated by the same computer system," the system determines which network the cellular phone should use for communications and switches networks accordingly. EX1005, 12:24-44. The networks can be chosen based on various factors such as available bandwidth, volume, capacity, and speed of data, communication capabilities, and more. EX1005, 11:20-31. For instance, if a short distance network, like a Bluetooth network, does not have sufficient bandwidth or capacity, communications can be carried over a cellular 3G network. EX1005, 11:33-62. Barnes describes an example of this situation when a user driving a vehicle initially communicates with a food vender's point of sale device to place an order from a far distance and then establishes a new communication link when within a predetermined distance of the vendor's restaurant to make the payment. EX1005, 29:4-30:33. Barnes explains that communication can take place "irrespective of the distance from the place of commerce exchange"

indicating that the communications encompass long distance cellular communications. EX1005, 29:39-50.

205. Consistent with this example, it would have been obvious to a POSITA that when short range communication between a POS device and the Wang-Barnes cellular phone conducted through short range wireless RF LAN module is unavailable (or any other network switching condition is satisfied), the Wang-Barnes cellular phone would switch to another network to complete the transaction described above with respect to claims 1-18. Barnes explains that a WWAN network can be used for communication between its device and a POS device. EX1005, 7:16-24. Accordingly, because the Wang-Barnes device is a cellular phone that is configured to use cellular circuitry (such as ASIC and an antenna) to communicate across a cellular network, it would have been obvious to a POSITA that the Wang-Barnes device would have switched to the cellular network and used cellular circuitry to conduct communications with the POS device. When this switch happens, it would have been obvious to a POSITA that the logic circuitry ("***processor***") in the Wang-Barnes cellular telephone "receive[s] a signal from a point of sale terminal via the cellular circuitry."

206. Barnes also discloses that its device can communicate with another device simultaneously through multiple networks, including, e.g., mobile 3G networks and wireless LAN and PANs. EX1005, 9:40-45, 11:5-20.

Communication across multiple networks can occur when a vendor or point of sale device does not know how far a user mobile/cellular device is from the point of sale device and therefore transmits a signal via the cellular circuitry to a cellular network, and to a short-distance LAN/PAN. EX1005, 16:63-17:36. In circumstances when the POS device and the Wang-Barnes cellular telephone are communicating with each other simultaneously across short range and long range (e.g., cellular) networks, it would have been obvious that the POS device would have transmitted signals simultaneously across both networks such that the Wang-Barnes cellular telephone "receive[s] a signal from a point of sale terminal via the cellular circuitry."

Ground 2A

207. Srey teaches that its receiver receives and demodulates received information. EX1006, 10:55-60, 5:57-67, FIGS. 2, 7. In the Wang-Srey cellular telephone, it would have been obvious that the receiver in the cellular circuitry would have received a signal from the requesting device 202 ("***point of sale terminal***"), as explained above in [1.5.1] and shown below in Wang's FIG. 2. Similar to the explanation above under the Ground 1A mapping of this feature, a signal from the POS terminal would have been received through the cellular circuitry instead of the short range radio frequency circuit in [1.5.1] when, e.g., short range communication between a POS device and the Wang-Srey cellular

phone conducted through short range wireless RF LAN module is unavailable (or any other network switching condition is satisfied), such that the Wang-Srey device utilizes the cellular network for POS communications.

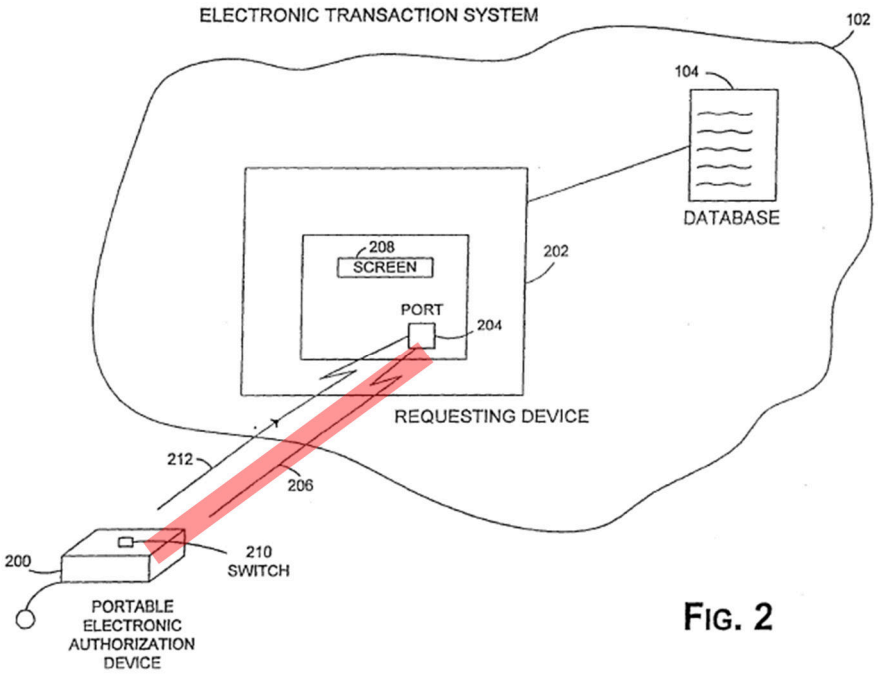


FIG. 2

EX1004, FIG. 2.

[19.6.2] the signal comprising a request to access the memory and retrieve the transaction information,

208. *See* [1.5.2].

[19.7] receive the fingerprint data from the fingerprint scanner,

209. *See* [1.6].

[19.8] compare the received fingerprint data with the fingerprint information stored in the memory, and

210. *See* [1.7].

[19.9] transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information; and

Ground 1A

211. As explained in [19.6.1], communications between the Wang-Barnes cellular telephone and the POS device would have been performed using the cellular circuitry (ASIC and antennas used to communicate with a cellular network) when the short range network communications fail or a network switch condition is satisfied. EX1005, 9:25-10:36, 11:5-12:44, 29:4-30:3, 7:16-24. In these circumstances, the logic circuitry ("***processor***") in the Wang-Barnes cellular telephone would have "***transmit[ted] the transaction information to a remote location***" associated with the POS device when the fingerprints match (instead of the short range radio frequency circuit as noted in the mapping of [1.8] above).

212. In Wang, the POS is positioned at a "remote location" from the mobile/cellular device. EX1004, FIG. 2. This is consistent with the '513 patent, which does not specify a particular distance associated with the "remote location," but provides examples such as a cellular telephone approaching a RF reader/writer (e.g., when a user of the cellular phone is in a hotel), indicating that the RF reader/writer is located away from and not physically connected to the cellular telephone and is communicating wirelessly with the same. EX1001, 15:16-22. Moreover, it would have been obvious to a POSITA that the "***transaction***

information" would have been transmitted to a remote location, such as a remote location of the POS device, when the POS device and cellular telephone are communicating over a cellular network and are not within a short range of each other, having invoked the network switch condition to communicate via the cellular network, as explained above in [19.6.1].

213. The rest of the mapping of [1.8] applies here.

Ground 2A

214. As explained in [19.6.1], communications between the Wang-Srey cellular telephone and the POS device would have been performed using the cellular circuitry (cellular transmitter) when the short range network communications fail or a network switch condition is satisfied. EX1005, 9:25-10:36, 11:5-12:44, 29:4-30:3, 7:16-24. Like in Ground 1A, it would have been obvious to a POSITA that the "***transaction information***" would have been transmitted to a remote location, such as a remote location of the POS device, when the POS device and cellular telephone are communicating over a cellular network and are not within a short range of each other, having invoked the network switch condition to communicate via the cellular network, as explained above in [19.6.1]. In these circumstances, the logic circuitry ("processor") in the Wang-Srey cellular telephone would have "***transmit[ted] the transaction information to a remote location***" associated with the POS device when the fingerprints match

(instead of the short range radio frequency circuit as noted in the mapping of [1.8] above).

215. The rest of the mapping of [1.8] applies here.

[19.10] a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

216. *See* [1.9].

iii. Claim 2

[2] The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

217. *See* [1.pre], [1.9].

iv. Claim 3

[3] The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

218. *See* [1.1].

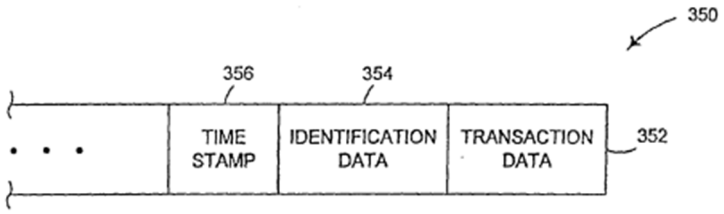
v. Claims 4, 12, and 20

[4] The mobile device of claim 1, wherein the processor is further configured to transmit the received biometric data or the stored biometric information with the transaction information.

[12] The cellular telephone of claim 11, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

[20] The cellular telephone of claim 19, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

219. Wang's FIG. 3B (reproduced below) illustrates "the format of representative transaction approval data." EX1004, 15:16-17.



EX1004, FIG. 3B.

220. Wang explains that "transaction data 352, representing a portion of or the entire transaction request received from the electronic transaction system, is appended with certain user identification data 354 and optionally a time stamp 356." EX1004, 15:17–20. Wang adds that, "[o]nce appended, transaction approval data 350 is then encrypted prior to being retransmitted back to the electronic transaction system." EX1004, 15:22–23. Wang further explains that the "user identification data … may include … unique identifying data such as fingerprint, DNA coding sequence, voice print, or the like." EX1004, 13:19–22.

221. Wang's logic circuitry 502 transmits, after encryption, the transaction approval data, in which the stored user identification data (which may include a fingerprint) is appended to the transaction data. EX1004, 13:19-22, 15:17-20, 11:5-30; §VIII.A.i.[1.2]. Therefore, a POSITA would have understood that the processor transmits the stored biometric/fingerprint information together with the transaction information.

vi. Claims 5, 13, and 21

[5] The mobile device of claim 1, wherein the transaction information is account information.

[13] The cellular telephone of claim 11, wherein the transaction information is account information.

[21] The cellular telephone of claim 19, wherein the transaction information is account information.

222. As explained in [1.3] and [1.5.2], the transaction information includes charge card information used to complete a transaction. EX1004, Abstract, 1:23-35, 15:12-23. Wang teaches that "[t]he charge cards themselves may represent credit cards (such as Visa or Master Cards), ATM cards, royalty cards, discount cards, as well as any other type of cards with which a user may employ vis-a-vis a point-of-sale terminal to obtain cash, goods, and/or services." EX1004, 25:32-26:6, 33:16-18 (explaining that a bank can issue a PEAD). Wang discloses that these cards typically store account information related to the user. EX1004, 12:12-13, 16:5-6, 3:10-16.

223. A POSITA would have understood the stored charge-card information, e.g., an ATM card or credit card information, to be account information associated with the user's credit card account or bank account to enable transaction payment. EX1004, 12:12-13, 16:5-6, 3:10-16, 33:16-18.

vii. Claims 6, 14, and 22

[6] The mobile device of claim 1, wherein the transaction information is credit card information.

[14] The cellular telephone of claim 11, wherein the transaction information is credit card information.

[22] The cellular telephone of claim 19, wherein the transaction information is credit card information.

224. *See* [5]/[13]/[21].

viii. Claims 7, 15, and 23

[7] The mobile device of claim 1, further comprising memory configured to store the transaction information.

[15] The cellular telephone of claim 11, further comprising memory configured to store the transaction information.

[23] The cellular telephone of claim 19, further comprising memory configured to store the transaction information.

225. *See* [1.5.2], [1.3].

ix. Claims 8, 16, and 24

[8] The mobile device of claim 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

[16] The cellular telephone of claim 15, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

[24] The cellular telephone of claim 23, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

226. *See* [1.5.2], [1.3].

x. Claims 9, 17, and 25

[9] The mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.

[17] The cellular telephone of claim 11, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

[25] The cellular telephone of claim 19, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

227. As explained in [1.7], in each of the Wang-Barnes and Wang-Srey devices, "the processor is configured to compare the received biometric data with the biometric information stored in the memory." Claim 9 further notes that this

comparison is "in response to receiving the request to retrieve the transaction information."

228. Recall from [1.3], [1.5.1], and [1.5.2] that in response to a transaction request in the "signal" being received from requesting device requesting transaction information (e.g., payment information) and user authentication is required to approve the transaction, Wang's user authentication mechanism 612 performs a fingerprint authentication procedure in which the user fingerprint is scanned and then compared to stored user fingerprint data in the memory. EX1004, 22:14-25, 38:5-7, 40:27-28, 14:16-25, 15:11-23, FIG. 3B. Accordingly, it would have been obvious to a POSITA that each of the Wang-Barnes and Wang-Srey devices performs the biometric data comparison "in response to receiving the request to retrieve the transaction information."

B. GROUNDS 1B AND 2B: Bashan in Combination with Wang-Barnes or Wang-Srey Renders Claims 10, 18, and 26 Obvious

i. Claims 10, 18, and 26

[10] The mobile device of claim 1, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

[18] The cellular telephone of claim 11, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

[26] The cellular telephone of claim 19, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

229. Each of Wang-Barnes-Bashan and Wang-Srey-Bashan renders [10], [18], and [26] obvious for the reasons noted above in §VII.H.

C. GROUND 3A: Mardikar in view of Cooke Renders Obvious Claims 1-3, 5-9, 11, 13-17, 19, 21-25

i. Claims 1 and 11

[1.pre] A mobile device, comprising:

[11.pre] A cellular telephone, comprising:

230. The Mardikar-Cooke Combination ("**MCC**") renders obvious a "***mobile device/cellular telephone***." Mardikar discloses a client device 400 "such as a mobile phone, [or] cellular phone." EX1009, Abstract, 6:42-50, FIG. 4.

[1.1] a biometric input device configured to receive biometric data;

[11.1] a fingerprint scanner configured to receive fingerprint data;

231. MCC renders obvious [1.1]/[11.1] at least because Mardikar discloses a biometric sensor 440 ("***biometric input device***"/"***fingerprint scanner***") that receives "***biometric/fingerprint data***."

232. Mardikar's device 400 includes a biometric sensor 440 that "may be any sensor that provides data representative of a unique, biological user attribute that may be used to identify a user, for example a finger/thumb-print sensor, retina scan or voice identifier." EX1009, 6:43-50, 7:28-32, FIG. 4 (reproduced below). A user "input[s] their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on biometric sensor 440." EX1009, 11:44-55, FIG. 6a.

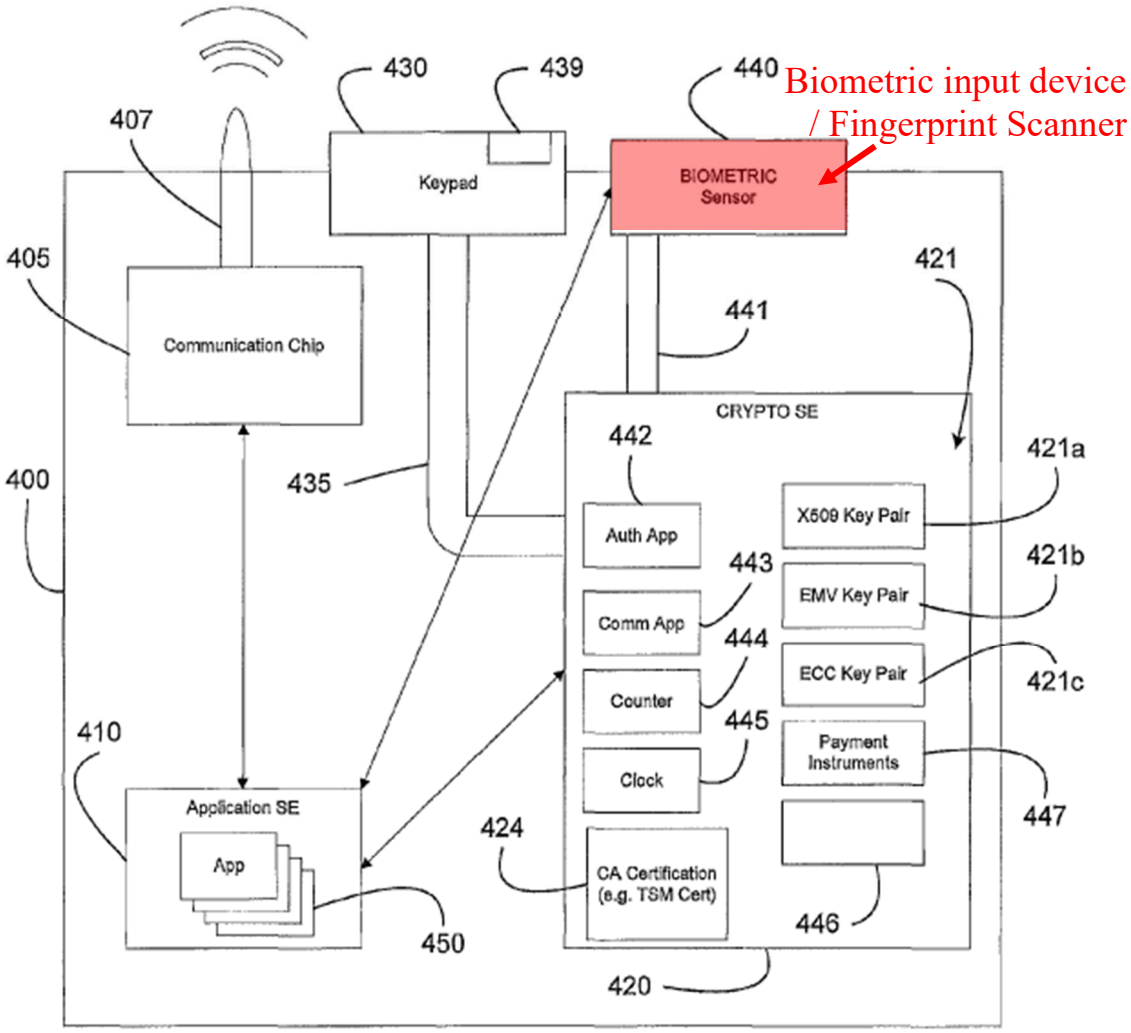


FIG. 4

EX1009, FIG. 4.

[1.2] a short range radio frequency circuit;

[11.2] a short range radio frequency circuit;

233. MCC renders obvious [1.2]/[11.2] at least because the MCC client device 400 includes RF (NFC) circuitry such as a communication chip 405 and

antenna 407 (collectively "***a short range radio frequency circuit***"). EX1009, FIG. 4.

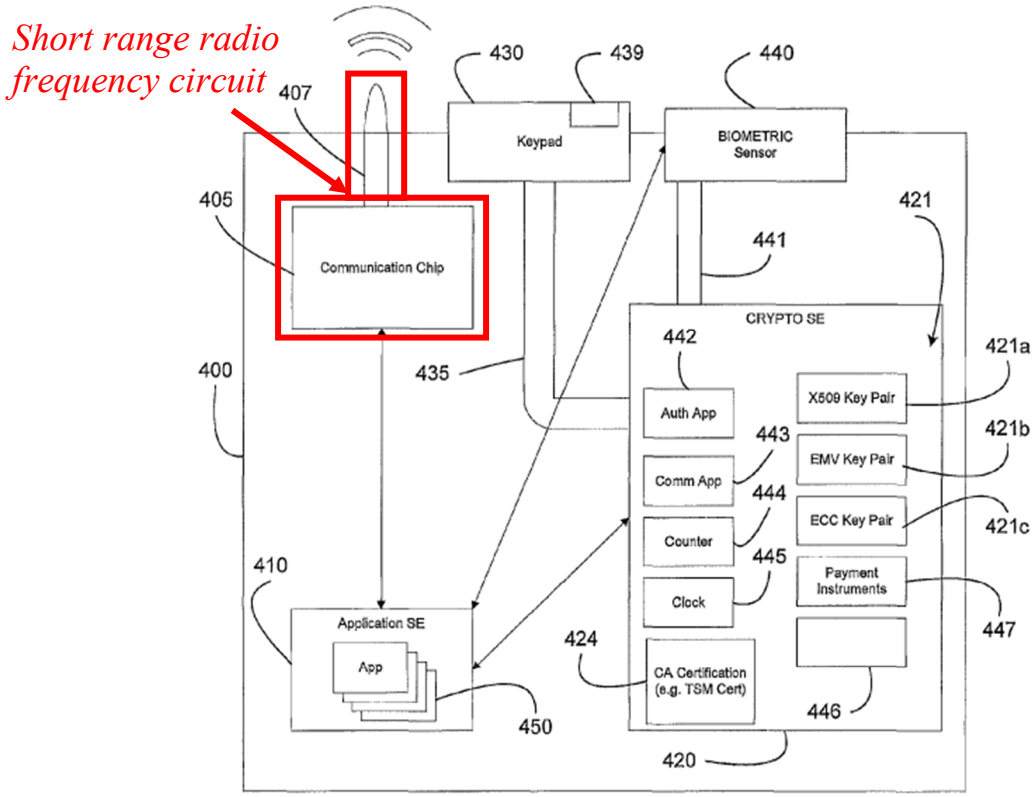


FIG. 4

EX1009, FIG. 4.

234. Mardikar explains that its communication chip 405 "support[s] one or more modes of communication, including, for example, Near Field Communication (NFC)," which is "a short-range, high frequency, wireless communication technology" used to exchange data that employ radio frequencies, such as RFIDs. EX1009, 6:43-67. Cooke also teaches that short range RF (NFC)

circuitry can be used in the proximity payment device to communicate with the POS reader. EX1010, ¶[0003] ("radio frequency (RF) communication"), ¶[0025]. Thus, a POSITA would have understood that, in MCC, the communication chip 405 and antenna 407 are used to facilitate RF communications with a POS device/reader. EX1010, ¶[0003], ¶[0025].

[1.3] memory configured to store biometric information for identifying an individual associated with transaction information;

[11.3] memory configured to store fingerprint information for identifying an individual associated with transaction information;

235. MCC renders obvious [1.3]/[11.3] at least because Mardikar's device 400 includes SE 420 with data storage ("***memory***") that stores biometric data ("***biometric/fingerprint information for identifying an individual associated with transaction information***").

236. Mardikar's SE 420 includes a data storage, and is used "for loading and storing authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 … including … unique biometric authentication information related to a specific user." EX1009, 9:36-47, 7:44-63, FIG. 4. Mardikar also discloses registering a user based on biometric attribute information such as thumbprint or fingerprint and using the authentication application 442 (also part of the Crypto SE 420) to compare biometric data with the registered biometric data (e.g., thumbprint or fingerprint). EX1009, 9:60-65,

10:41-62, 11:44-12:3. After the user's biometric identification is authenticated, a payment (credit card information) associated with the user can be made. EX1009, 9:60-65, 10:41-62, 11:44-12:3. Accordingly, it would have been obvious to a POSITA that the data storage ("***memory***") in Mardikar's Crypto SE 420 stores fingerprint data to identify the user associated with the transaction information ("***biometric/fingerprint information for identifying an individual associated with transaction information***").

[1.4] a processor coupled with the memory and the biometric input device, the processor configured to:

[11.4] a processor coupled with the memory and the fingerprint scanner, the processor configured to:

237. MCC renders obvious [1.4]/[11.4] at least because Mardikar's device 400 includes a CPU (***processor***) coupled with the Crypto SE 420 memory and the biometric sensor 440 ("***biometric input device/fingerprint scanner***").

238. As a preliminary matter, Mardikar explains that its mobile device and computer system include one or more processors that are interconnected with other system elements such as memory through "a bus or other communication mechanism," and that the processor executes the operations described in Mardikar. EX1009, 14:20-15:51 ("[l]ogic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to the processor for execution.") At least for this reason (and the reasons noted in

§VII.K), it would have been obvious to a POSITA that Mardikar, in combination with Cooke, teaches [1.4]/[11.4] and the recited operations in [1.5.1]-[1.8]/[11.5.1]-[11.8].

239. Additionally, Mardikar teaches that the SE 420 may be a smart card or smart card-like chip embedded inside device 400. EX1009, 7:45-57. "The smart card itself may contain a CPU and some non-volatile storage." EX1009, 7:45-57. Mardikar also teaches that "an authentication application 442, for example a biometric authentication application, may reside on the Crypto SE 420 and may evaluate the biometric data." EX1009, 9:60-65. "[B]iometric signature data from the biometric sensor 440 may be tunneled through a biometric tunneling circuit 441, directly to the Crypto SE 420." EX1009, 7:37-40.

240. It would have been obvious to a POSITA that: (1) a processor, such as CPU, in SE 420, would have performed the biometric data comparison/evaluation as part of the biometric authentication conducted by the authentication application 442 in SE 420; (2) the CPU in SE 420 would have been directly or indirectly coupled to the memory/storage within SE 420 e.g., to perform the biometric data comparison; and (3) the CPU and memory within SE 420 are also coupled to the biometric sensor 440, as shown in Mardikar's FIG. 4. EX1009, 7:37-40, 9:60-65, 16:31-32, FIG. 6a. Such an arrangement was known in the art as evidenced by Srey's FIG. 7 (EX1006) and discussed above in Ground 1B and Section VII.C.

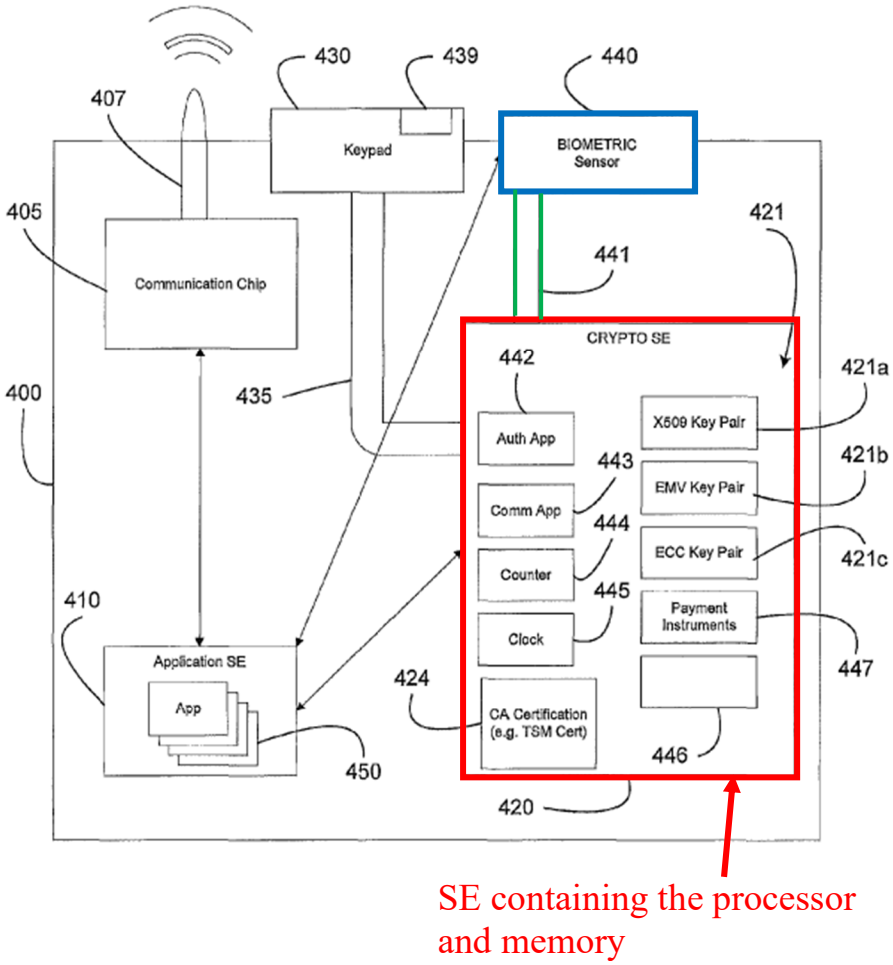


FIG. 4

EX1009, FIG. 4.

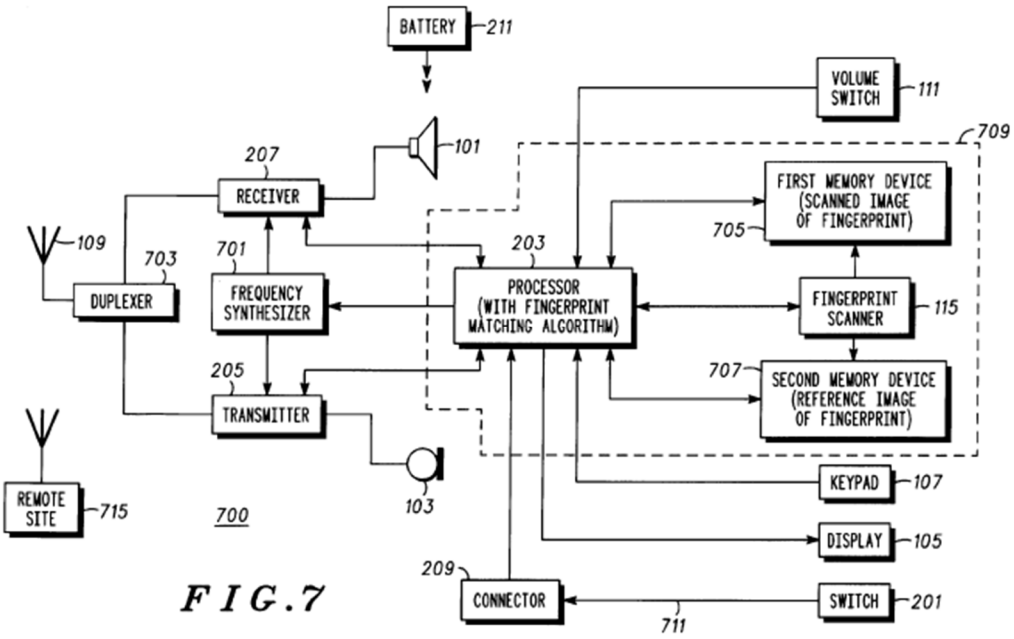


FIG. 7

EX1006, FIG. 7.

241. As explained below in [1.5.1]-[1.8]/[11.5.1]-[11.8], Mardikar's processor also performs the recited operations in [1.5.1]-[1.8]/[11.5.1]-[11.8].

> ***[1.5.1] receive a signal from a point of sale terminal via the short range radio frequency circuit,***
>
> ***[11.5.1] receive a signal from a point of sale terminal via the short range radio frequency circuit,***

242. MCC renders obvious [1.5.1] at least because the processor in MCC's SE 420 receives an interrogation signal ("***a signal from a point of sale terminal***") from a POS terminal via the RF NFC circuitry ("***via the short range radio frequency circuit***").

243. Recall from [1.2] that Mardikar's device 400 communicates with a POS device using MCC's RF NFC circuitry, including a communication chip 405

and antenna 407, that corresponds to the claimed "***short range radio frequency circuit***." EX1009, 6:43-67, FIG. 4; EX1010, ¶¶[0003], [0025]. For example, Mardikar explains that its device is "capable of near field communication (NFC) and may be capable of making secure financial transactions at an NFC point of sale (POS)." EX1009, 3:30-33.

244. Cooke teaches "the RF reader transmits an interrogation signal [to a proximity payment device such as a payment-enabled mobile telephones] and then listens for a response signal and/or message from the RFID circuitry of the proximity payment device." EX1010, ¶¶[0003], [0025], [0028], FIGS. 2-3. "[T]he payment circuit of the proximity payment device is configured to respond to [the] interrogation signal from an NFC reader by transmitting payment account information." EX1010, ¶[0025].

245. Because (1) Cooke expressly identifies payment-enabled mobile telephones as the responding proximity payment device; (2) Cooke explains that RF readers were incorporated with a POS Terminal; and (3) the payment device receives an interrogation signal from the RF reader, a POSITA would have understood that, in the combination, MCC's mobile/cellular device 400 "***receive[s] a signal from a point of sale terminal via the short range radio frequency circuit***." EX1010, ¶¶[0003], [0016], [0025]. Indeed, because MCC's device is "compatible with Near Field Communication Point of Sale devices (NFC POS)"

and includes the NFC communication chip 405 and antenna 407, a POSITA would have recognized that the interrogation signal would have been received through the MCC's NFC communication chip 405 and antenna 407. EX1009, 6:67-7:3, FIG. 4.

246. Recall also that in the MCC system, payment information is sent in response to the interrogation signal. EX1010, ¶[0025], FIGS. 2-3. The payment instruments 447 are stored in MCC's SE 420 along with other certificates and keys (e.g., crypto keys 421) needed to communicate with other devices. EX1009, 9:37-47, 10:17-40. Accordingly, it would have been obvious that the processor in SE 420 receives the interrogation signal and processes it to determine and obtain the payment information needed to respond. EX1009, 14:20-15:5.

[1.5.2] the signal comprising a request to access the memory and retrieve the transaction information,

[11.5.2] the signal comprising a request to access the memory and retrieve the transaction information,

247. MCC renders obvious [1.5.2]/[11.5.2] at least because Cooke's interrogation signal includes "***a request to access the memory and retrieve the transaction information***."

248. As noted above in [1.5.1], Cooke teaches that the NFC RF reader transmits an interrogation signal and "the payment circuit of the proximity payment device is configured to respond to an interrogation signal from an NFC

reader by transmitting payment account information such as a payment card account number (PAN) or other identifying data" that is stored on the device. EX1010, ¶¶[0003], [0025], [0028]. Relatedly, Mardikar teaches that the transaction information (e.g., payment information, account number) is stored in the Crypto SE memory and is read out and provided for transmission upon authorization. EX1009, 9:37-47 ("load[s] and stor[es] authentication data 446 (for example a PIN or biometric signature), payment instruments 447, certificates 424, crypto keys 421 and other security-related information"), 11:8-27 ("payment account number and CVV may be stored in the Crypto SE"), 12:22-30, 13:16-37, FIGS. 5b, 6a. Accordingly, it would have been obvious to a POSITA that the signal received from the RF reader in the MCC system includes "***a request to access the memory and retrieve the transaction information***." EX1010, ¶¶[0003], [0025].

[1.6] receive the biometric data from the biometric input device,

[11.6] receive the fingerprint data from the fingerprint scanner,

249. MCC renders obvious [1.6]/[11.6] at least because Mardikar's device "***receive[s]***" fingerprint data ("***biometric/fingerprint data***") from the biometric sensor 440 ("***the biometric input device***"/"***fingerprint scanner***").

250. In particular, Mardikar teaches that a user "input[s] their biometric identifying data (ID) or signature by placing or swiping a thumb or finger on

biometric sensor 440," and "[t]he input biometric ID may be directly sent or tunnelled to Crypto SE 420." EX1009, 11:44-12:3, FIG. 6a (steps 606-608). As explained in more detail below in [1.7]/[11.7], it would have been obvious that the processor in SE 420 receives the biometric/fingerprint data to perform a comparison. EX1009, 14:20-15:5.

> ***[1.7] compare the received biometric data with the biometric information stored in the memory, and***
>
> ***[11.7] compare the received fingerprint data with the fingerprint information stored in the memory, and***

251. MCC renders obvious [1.7]/[11.7] at least because Mardikar's processor "***compare[s]***" received fingerprint data ("***the received biometric/fingerprint data***") with stored biometric signature data ("***the biometric/fingerprint information stored in the memory***").

252. As explained in [1.3], Mardikar's Crypto SE 420 includes data storage that stores registered biometric attribute information such as thumbprint or fingerprint. EX1009, 9:36-47, 7:44-63, FIG. 4. After obtaining the fingerprint data ("***biometric/fingerprint data***") from the biometric sensor 440, this data is compared with the registered biometric data. EX1009, 9:60-65, 10:41-62, 11:44-12:3, 16:30-33 (cl. 1). It would have been obvious to a POSITA that for SE 420 to receive and compare registered and received biometric/fingerprint data, the

processor in SE 420 would have performed these operations. *See also* [1.4], [1.5.1]; EX1009, 14:20-15:5.

> ***[1.8] transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and***
>
> ***[11.8] transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information; and***

253. MCC renders obvious [1.8]/[11.8] at least because payment information ("***transaction information***") is transmitted to the NFC POS reader ("***point of sale terminal***") using MCC's NFC circuit ("***short range radio frequency circuit***") when the "***received biometric/fingerprint data matches the stored biometric/fingerprint information***."

254. As explained above in [1.2] and [1.5.1]-[1.5.2], in response to the interrogation signal, payment information is sent using the RF (NFC) circuitry, which in the MCC includes Mardikar's communication chip 405 and antenna 407. EX1010, ¶¶[0003], [0021], [0025], FIGS. 2, 3. Mardikar teaches that, for security reasons, the information is sent after biometric authentication by virtue of fingerprint matching is performed. In particular, Mardikar teaches "generating a secure payment information message in response to an authentication including a match of the biometric data with the stored biometric signature … the secure

payment information message includes the payment instrument; and transmitting the secure payment information message to a POS reader by … near field communication (NFC)." EX1009, 16:30-33 (cl. 1), FIG. 6a. Mardikar further teaches that, once authenticated, "the App SE 410 may then send the payment information … to the communication chip 405 for further transmission or transport to a reader … located at the POS, for example a POS NFC reader." EX1009, 11:55-12:30, FIG. 6a (steps 612-614). Because the processor in the SE 420 is performing the biometric authentication (using Auth App 442 in SE 420) and obtains payment information from payment instruments 447 (also located in SE 420), it would have been obvious to a POSITA, that the processor in MCC's SE 420 would have transmitted the transaction information to the POS NFC reader ("***to the point of sale terminal***") using communication chip 405 and antenna 407 ("***short range radio frequency circuit***") "***when the received biometric/fingerprint data matches the stored biometric/fingerprint information***." EX1009, 14:20-15:5.

[1.9] a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

[11.9] a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

255. MCC renders obvious [1.9]/[11.9] at least because Mardikar's device 400 houses the biometric sensor 440, the NFC communication chip 405/antenna

407, the secure-element memory, and the CPU. For example, Mardikar's device 400 "include[s] a communication chip 405, an antenna 407, secure elements 410, 420, a keypad 430 and a biometric sensor 440," and describes the SEs 410, 420 as containing a CPU and being "embedded inside device 400, for example inside of a cell phone." EX1009, 6:42-7:65, FIG. 4.

ii. Claim 19

[19.pre] A cellular telephone, comprising:

256. *See* [1.pre].

[19.1] cellular circuitry;

257. Mardikar's communication chip 405 "supports one or more modes of communication, including, for example, Near Field Communication (NFC), Bluetooth, infrared, GSM, UMTS and CDMA cellular phone protocols, SMS and Internet access via a mobile network or local network." EX1009, 6:43-67. Accordingly, in the context of claim 19 and its dependent claims, a POSITA would have understood that Mardikar's communication chip is also "***cellular circuitry***" that facilitates communications with mobile/cellular networks.

[19.2] a fingerprint scanner configured to receive fingerprint data;

258. *See* [1.1].

[19.3] a short range radio frequency circuit;

259. MCC's cellular phone includes "***a short range radio frequency circuit***." *See* [1.2]. Note that because the communication chip 405 can support different communications, including NFC, the communication chip 405, alone or in combination with the antenna 407, also corresponds to "***a short range radio frequency circuit***." Thus, MCC renders obvious [19.3].

[19.4] a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information;

260. *See* [1.3].

[19.5] a processor coupled with the memory and the fingerprint scanner, the processor configured to:

261. *See* [1.4].

[19.6.1] receive a signal from a point of sale terminal via the cellular circuitry,

262. As a preliminary matter, MCC renders obvious [19.6.1.] for the same or similar reasons as in [1.5.1] because Mardikar's communication chip 405 operates as the cellular circuitry and the short range radio frequency circuit.

263. In addition, Mardikar also teaches that a user can complete a transaction with a merchant/service provider having a POS device over a mobile network such as Sprint, Verizon or other mobile network service providers. EX1009, 5:34-6:12, FIG. 3. This flexibility (of using a cellular/mobile network in addition to NFC networks) is particularly helpful in the "ever changing electronic

communications environment." EX1009, 6:1-12; *see also* 4:32-36 ("It should be appreciated that although an NFC application is illustrated in this embodiment, the system is not limited to NFC applications, but may also apply to other types of applications, for example, SMS, mobile internet or other forms of communication"), 5:55-61. Cooke also explains that the NFC protocol is only used "in some payment application implementations" indicating that its disclosure is applicable beyond NFC communications. EX1010, ¶¶[0003], [0001], [0021].

264. Accordingly, it would have been obvious to a POSITA that when multiple communication networks are available for communication , the MCC cellular phone would have conducted the transaction with the POS device using a cellular network and its cellular circuitry in addition to or in place of short distance communication. *See also* §VIII.A.ii.[19.6.1]. In such an event, it would have been obvious to a POSITA that cellular circuitry would have been used for receiving an interrogation signal from a point of sale terminal and also transmitting any response back. EX1009, 1:45-2:28. Because Mardikar's communication chip is configured to support multiple modes of communication, including NFC communications and cellular communications, the cellular circuitry in the communication chip would have been configured to receive an interrogation signal. For this additional reason, MCC renders obvious [19.6.1].

[19.6.2] the signal comprising a request to access the memory and retrieve the transaction information,

265. *See* [1.5.2].

[19.7] receive the fingerprint data from the fingerprint scanner,

266. *See* [1.6].

[19.8] compare the received fingerprint data with the fingerprint information stored in the memory, and

267. *See* [1.7].

[19.9] transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information; and

268. MCC renders obvious [19.9] for at least the reasons noted above in [1.8] and [19.6.1] (explaining that cellular circuitry would have been used to transmit responsive information).

269. Moreover, Mardikar teaches that "payments and financial transactions may be made using secure SMS communication," in which the Crypto SE "generate[s], encrypt[s], and send[s] encrypted [messages] to the TSM" over the cellular channel. EX1009, 13:38-49. Mardikar further teaches that, "[w]hen fully authenticated by the PIN and/or the biometric signature, the Crypto SE 420 may send the payment information to the App SE 410 for forwarding via NFC or other communication mode." EX1009, 13:14-29. Because the secure-SMS transport carries the payment information over the cellular circuitry to a remote location (e.g., the TSM/server) after biometric authentication, MCC renders obvious

"***transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information***." EX1009, 13:14-49. The remainder of the mapping of [1.8] otherwise applies.

[19.10] a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

270. *See* [1.9].

iii. Claim 2

[2] The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

271. *See* [1.pre].

iv. Claim 3

[3] The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

272. *See* [1.1].

v. Claims 5, 13, and 21

[5] The mobile device of claim 1, wherein the transaction information is account information.

[13] The cellular telephone of claim 11, wherein the transaction information is account information.

[21] The cellular telephone of claim 19, wherein the transaction information is account information.

273. *See* [1.5.2], [1.3].

vi. Claims 6, 14, and 22

[6] The mobile device of claim 1, wherein the transaction information is credit card information.

[14] The cellular telephone of claim 11, wherein the transaction information is credit card information.

[22] The cellular telephone of claim 19, wherein the transaction information is credit card information.

274. Mardikar teaches that credit cards are used for payments and that the Service providers in its system include banks and credit card issuers. EX1009, 1:45-67, 3:53-56, 6:15-41, 13:3-15. "In an example embodiment, the Crypto SE 420 may be certified, for example by a credit processing company such as MasterCard or VISA," and Crypto SE 420 stores the security key pairs for several cards, Europay, MasterCard, VISA. EX1009, 10:5-24. A POSITA would have understood that Mardikar's system is configured in the above-noted manner, e.g., with credit card issuers as service providers and Crypto SE 420 storing security keys for credit cards, so that Mardikar's device is used to make credit card payments to complete a transaction.

275. Consistent with Mardikar, Cooke teaches that payment information, including e.g., MasterCard account number, is provided to the POS terminal in response to the interrogation signal to conduct a wireless transaction. EX1010, ¶¶[0003], [0025], [0016], [0034].

276. Accordingly, in the MCC system, when transaction information is sent to the card reader, the transaction information includes payment information such as credit card information to complete the transaction. *See also* [1.3], [1.5.2].

vii. Claims 7, 15, and 23

[7] The mobile device of claim 1, further comprising memory configured to store the transaction information.

[15] The cellular telephone of claim 11, further comprising memory configured to store the transaction information.

[23] The cellular telephone of claim 19, further comprising memory configured to store the transaction information.

277. *See* [1.5.2].

viii. Claims 8, 16, and 24

[8] The mobile device of claim 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

[16] The cellular telephone of claim 15, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

[24] The cellular telephone of claim 23, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

278. Mardikar's single Crypto SE 420 stores both the authentication data 446, such as fingerprint data ("***biometric information***") and the payment information ("***transaction information***"). *See* [1.3], [1.5.2], [7]. Thus, it would

have been obvious to a POSITA that the same memory in Crypto SE 420 stores the "***biometric information***" and the "***transaction information***."

ix. Claims 9, 17, and 25

> ***[9] The mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.***
>
> ***[17] The cellular telephone of claim 11, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.***
>
> ***[25] The cellular telephone of claim 19, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.***

279. As explained above in [1.5.1]-[1.8], a processor in SE 420 receives an interrogation signal from Cooke's NFC reader, and responds with transaction information. EX1010, ¶¶[0003], [0025]. However, for security reasons, Mardikar teaches that in preparation for a payment, biometric authentication is performed to authentication the user. EX1009, 11:44-12:30, 16:30-33 (cl. 1), FIG. 6a. Biometric authentication involves a comparison of the received fingerprint data with stored fingerprint data, as explained in [1.7]. Accordingly, it would have been obvious to a POSITA that, in the MCC system, the biometric authentication is performed in response to receiving the interrogation signal that requests retrieval of the transaction information.

D. GROUND 3B: Mardikar, Cooke, and Lee Render Claims 10, 18, and 26 Obvious

i. Claims 10, 18, and 26

[10] The mobile device of claim 1, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

[18] The cellular telephone of claim 11, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

[26] The cellular telephone of claim 19, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

280. MCC-Lee renders [10], [18], and [26] obvious for the reasons noted above in §VII.M.

IX. CONCLUSION

281. For all the reasons I have noted in the foregoing paragraphs, claims 1-26 of the ’513 Patent are obvious in view of the references discussed above.

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

APPENDIX A



Seth James Nielson's Vita

(512) 387-4310
seth@crimsonvista.com
July 2026

Academic Degrees

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

Certifications

CISSP
GCFE

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

Summary of Expertise and Experience

100+ Forensic and Incident Response Engagements: Leading specialized teams in reconstructing cyber intrusions, investigating trade secret misappropriation, and analyzing complex data artifacts on behalf of, for example, Fortune-50 organizations.
25+ years of professional experience: Working in industry as a subject-matter expert in software engineering, cybersecurity, and computer networks with breadth and depth in architectures, programming languages, protocols, cryptography, and evaluation.
12 Years of Academic Leadership and Research: Currently serving as Adjunct Associate Professor at the University of Texas at Austin; formerly Director of Advanced Research Projects and Research Scientist at Johns Hopkins University Information Security Institute.
10 Years as a Qualified Testifying Expert: Recognized expert in technical matters of patent infringement, validity, copyright, DMCA, industry standards, digital forensics and cybersecurity incidents.

Summary of Core Competencies

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

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

Current Appointments

CEO	Crimson Vista, Inc.
Adjunct Assistant Professor	University of Texas at Austin

Professional Service

International Cryptographic Module Conference, 2018-2026 Program Committee

Professional Advising

2019-2024	Advisory Board	Syccure, Inc.

Non-profit and Community Engagement

2026-	Member	FBI's Infragard
2025	Corporate Contribution	The Digital Harbor Foundation
2021-2025	Founding Director	The Crypto Done Right Foundation
2019-2021	Cyberlab Advisory Board	The SEED School of Maryland

Grants and Research Awards

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

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

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

Patents

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

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

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

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

issued March 18, 2014 (Co-inventor)

Academic Awards

Brown Fellowship
John and Eileen Tietze Fellowship

University Research Funding

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

Publications

Books

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

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

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

Refereed Publications

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

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

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

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

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

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

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

Testimony Before Government Bodies

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

Invited Talks, Panels, and Technical Training

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Theses

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

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

Technical Reports

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

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

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

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

White Papers and Trade Publications

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

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

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

Undergraduate Advising

Independent Research and Capstones (University of Texas Austin)

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

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

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

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

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

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

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

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

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

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

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

Gonzalo Tamariz-Martel Sánchez (June 2022).

Graduate Advising

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In the News

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

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

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-2025)
Network Security and Privacy (2020-2021)

Johns Hopkins University

Advanced Network Security (2017 - 2019)
Network Security (2014 – 2019)

Rice University

Data Structures and Algorithms (Spring 2008)

Selected Projects

Machine Learning and AI

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

Software Research and Development

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

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

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

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

Intrusion and Incident Response

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

Applied Cryptography

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

Security Operations, Compliance, Oversight

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

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

IoT Devices and IoT Security

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

Network Security

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

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

Malware and Viruses

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

Privacy

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

Miscellaneous Security Technologies

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

Software Engineering and Software Analysis

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

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

Employment History (Last Title Only)

CEO, Crimson Vista, Inc. (2016-).
Adjunct Assistant Professor, University of Texas at Austin (2020-).
Founder and Partner, Source Code Discovery, LLC. (2019-2021).
Director of Advanced Research Projects, Johns Hopkins University (2016-2019).
Adjunct Associate Research Scientist, Johns Hopkins University (2014-2019).
Principal, Harbor Labs, LLC. (2011-2015).
Senior Security Analyst, Independent Security Evaluators (2005-2011).
Summer Intern, Google Inc. (2005).
Software Engineer II, Metrowerks (2001-2003).

Expert Testimony

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

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

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

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

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

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

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

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

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

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

Deposition: 1 deposition February 2026

In support of Unified's Request for Ex Parte Reexamination of 11,503,105
Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security, content delivery networks
Reports: 1 declaration, February 2026

On behalf of Vizio in Software Freedom Conservancy v Vizio (30-2021-01226723-CU-BC-CJC)
Counsel: Quinn Emanuel
Venue: Superior Court of the State of California, County of Orange
Subject Matter: Open source use in industry, nature and contents of artifacts, build issues
Deposition: 1 deposition December 2025

On behalf of Nielsen Consumer Inc in Nielsen Holdings Limited v Nielsen Consumer Inc. (2025-0651-NAC)
Counsel: Ropes and Gray
Venue: Court of Chancery of the State of Delaware
Subject Matter: Cybersecurity issues in data sharing agreement
Reports: 1 report July 2025
Deposition: 1 deposition July 2025
Trial: July 2025

On behalf of Samsung in Secure Wifi v Samsung (2:24-CV-00047-JRG)
Counsel: Blank Rome
Venue: Eastern District of Texas, Marshall Division
Subject Matter: Source code analysis of Wifi modules
Reports: 1 report July 2025
Deposition: 1 deposition July 2025

On behalf of Axonics in Alfred E. Mann Foundation for Scientific Research v Axonics
Counsel: Tensegrity
Venue: JAMS Arbitration
Subject Matter: Software completeness, correctness, comparison
Reports: 1 report April 2025, 1 report May 2025, 1 report June 2025
Deposition: 1 deposition June 2025, 1 deposition November 2025

In support of Unified's Request for Ex Parte Reexamination of 8,782,283
Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, May 2024

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

On behalf of USAA in PacID v. USAA
Counsel: Fish and Richardson
Venue: ITC

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

On behalf of the State of Texas in State of Texas v. Google
Counsel: Norton Rose Fulbright
Venue: District Court of Victoria County Texas
Subject Matter: Biometric Data Storage
Reports: 1 report, February 2025

In support of Unified's Request for Ex Parte Reexamination of 7,249,262
Counsel: Unified Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, February 2024

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

On behalf of LG Electronics in TOT Power Control v LG Electronics; C.A No. 21-1304-MN
Counsel: DLA Piper
Venue: District of Delaware
Subject Matter: Outer loop power control, source code
Reports: 1 report September 2024
Deposition 1 deposition November 2024

On behalf of Dexcom in Dexcom v Abbott Diabetes Care; C.A. No. 22-605-KAJ
Counsel: Quinn Emanuel
Venue: District of Delaware
Subject Matter: Glucose alerts source code
Reports: 1 report September 2024

On behalf of Axonics in In the Matter of Certain Video Processing Devices and Components Thereof; Investigation No. 337-TA-1396
Counsel: Tensegrity
Venue: ITC
Subject Matter: Medical implant wireless transmission source code
Reports: 2 reports September 2024
Deposition: 1 deposition October 2024
Trial: December 2024

On behalf of Apple in Carbyne v. Apple; Civil Action No. 1:23-cv-00324
Counsel: Ropes and Gray
Venue: West District of Texas, Austin Division
Subject Matter: Authentication, Secure Storage, Secure Processing, Access
Reports: 1 report August 2024, 1 report September 2024
Deposition: 1 deposition October 2024
Trial: Evidentiary hearing November 2024

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

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

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

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

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

Counsel:	Quinn Emanuel
Venue:	Norther 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:	Vennable
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:	Flachsbart & 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 Delware)
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 Afilias in Afilias 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