

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

TELCOM VENTURES LLC,

Patent Owner.

Case No. IPR2025-01236

U.S. Patent 11,770,756

DECLARATION OF CHUCK EASTTOM

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Qualifications.....	2
III.	Materials Considered	5
IV.	Scope of Opinions.....	6
V.	Related Matters	8
VI.	Legal Standards	10
	A. Claim Construction.....	11
	B. Obviousness.....	12
	C. Motivations to Combine.....	14
VII.	Level of Ordinary Skill in the Art	16
VIII.	Claim Construction.....	18
	A. “Physiological State”.....	18
IX.	Technology Background.....	19
	A. Near Field Communications (“NFC”)	19
X.	U.S. Patent No. 11,770,756 (“’756 Patent”) (Ex. 1001)	21
	A. Priority Date	21
	B. ’756 Patent Overview	22
	C. The ’756 Patent’s Prosecution History	23
XI.	Asserted References.....	24
	A. <i>Carlson</i> (Ex. 1005).....	24
	B. <i>Holloway</i> (Ex. 1032)	26
	C. <i>Jazayeri</i> (Ex. 1007)	27
	D. <i>ISO-14443</i> (Ex. 1016)	29
	E. <i>Sherman</i> (Ex. 1014).....	29
	F. <i>Murakami</i> (Ex. 1009).....	29
XII.	The Challenged Claims of the ’756 Patent Would Not Have Been Obvious.....	30
	A. Petitioner’s Grounds 1–6 Fail Because the Challenged Claims Would Not Have Been Obvious Over the Asserted References.....	30

1.	Carlson in View of Jazayeri Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed” (Grounds 1-3).	33
2.	Carlson in View of Murakami Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed” (Grounds 4-6).	41
3.	Carlson’s request for PPAI does not teach and would not have rendered obvious “requesting . . . from a second device an authorization to enable a function for conducting a financial transaction by the device” (Grounds 1-6).	44
XIII.	Summary and Other Remarks	56

Table of Exhibits

Exhibit No.	Description
2001	Interim Processes for PTAB Workload Management, Acting Director Memorandum (March 26, 2025) (https://www.uspto.gov/sites/default/files/documents/InterimProcesses-PTABWorkloadMgmt-20250326.pdf)
2002	Order Granting Joint Stipulation to Dismiss With Prejudice Counts I, II, V, and VIII of Telcom Ventures' Complaint
2003	Third Amended Docket Control Order
2004	Standing Order for Civil Cases Before Judge Rita F. Lin
2005	Telcom Ventures' Proposed Case Schedule for the Apple Litigation
2007	<i>Curriculum Vitae</i> of Dr. Chuck Easttom
2008	Chiradeep BasuMallick, "What is NFC (Near Field Communication)? Definition, Working, and Examples" (Sept. 29, 2022), https://www.spiceworks.com/tech/networking/articles/what-is-near-field-communication/
2009	Liu et al., "Near-Field Communications: A Comprehensive Survey," IEEE (June 2025)
2010	"The Creation of the NFC Forum and its Vision" (2011) https://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/NFCChips/nfcforum.html
2011	McHugh & Yarmey, "Near Field Communication: Introduction and Implication," ERIC (2012)
2012	Coskun et al., "The Survey on Near Field Communication," Sensors (June 5, 2015)

I. INTRODUCTION

1. My name is Dr. Chuck Easttom, and I have been retained as a technical expert by counsel for Patent Owner Telcom Ventures LLC (“Telcom Ventures” or “Patent Owner”) to investigate and opine as to the validity of U.S. Patent No. 11,770,756 (the “’756 patent”) in view of the Petition for *Inter Partes* Review (the “Petition”, Paper 1) by Petitioner Apple Inc. (“Petitioner” or “Apple”).

2. This declaration is based on information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study and thus may expand or modify my opinions as my investigation and study continues. I may also supplement my opinions in response to any additional information that becomes available to me, any matters raised by Petitioner and/or opinions rendered by Petitioner’s experts, or in light of any relevant orders from the Board.

3. My opinions are based on my years of education, research, and experience, as well as my investigation and study of relevant materials.

4. I am being compensated at the rate of \$550 per hour for my work in this case, including time spent testifying. I am also being reimbursed for reasonable fees and expenses, including hotel and travel expenses, incurred as a result of my work in this case. Neither I nor my company have received any additional compensation for my work in this *inter partes* review. My compensation is not tied in any way to

the substance of my testimony or the outcome of this proceeding. I have no other financial interest in this inter partes review or to the parties. I am available to offer these opinions at deposition and at trial if called upon to do so.

II. QUALIFICATIONS

5. I have summarized in this section my educational background, work experience, and other relevant qualifications. A true and correct copy of my curriculum vitae is attached as Ex. 2007 to Patent Owner's Preliminary Response, which includes a list of all other cases in which, during the previous four years, I have testified at trial or by deposition.

6. I have over thirty years of experience in the computer science industry including extensive experience with computer security, mobile devices, and related topics. I have authored forty-five computer science books, including books on mobile devices and on cryptography. I also have authored over eighty research papers and am an inventor with twenty-seven computer science patents.

7. I hold a Doctor of Science (D.Sc.) degree in Cyber Security from Capitol Technology University (Dissertation Topic: "A Comparative Study of Lattice Based Algorithms for Post Quantum Computing"). I also hold a Doctor of Philosophy (Ph.D.) in Technology focused on nanotechnology (Dissertation Topic: "The Effects of Complexity on Carbon Nanotube Failures") from Capitol Technology University. I also have a Doctor of Philosophy (Ph.D.) in Computer

Science from the University of Portsmouth (Dissertation Topic: “A Systematic Framework for Network Forensics Using Graph Theory”). I also hold four Master’s degrees—one in Applied Computer Science, one in Education, one in Defense and Strategic Studies, and one in Systems Engineering.

8. I am currently an Adjunct Lecturer for Georgetown University teaching graduate courses in requirements engineering, artificial intelligence, cybersecurity, and cryptography. I am also an adjunct for Vanderbilt University teaching graduate computer science courses in quantum computing, digital forensics, algorithms, and cybersecurity. I also developed a graduate course in digital forensics for the University of Dallas and taught that course from 2019 to 2022.

9. I am a Senior Member and Distinguished Speaker for the Association of Computing Machinery (“ACM”) and a Senior Member and Distinguished Visitor of the Institute for Electrical and Electronics Engineering (“IEEE”). The IEEE is the world’s largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards for a wide range of engineering disciplines, including software development. I am also a Distinguished Visitor of the IEEE. I have been involved in IEEE standards creation for several years.

10. I have extensive experience with smart cards, Near Field Communications (“NFC”), the ISO/IEC 7810 standard for identification cards, the ISO/IEC 7816 standard for electronic cards for identification, the ISO/IEC 14443

standard for contactless integrated circuit cards, the EMV standard, and related standards and technologies.

11. I have worked with smart cards as an authentication method since the Department of Defense began using the Common Access Card in the early 2000s. Near Field Communications were covered in networking courses that I took as part of my second Master's degree and in some of the networking certifications I hold. I have also worked with NFC since at least 2005. Specific certifications I hold that are relevant to NFC and/or mobile devices include:

- Associate of Systems Engineering (ASEP) from INCOSE (International Council on Systems Engineering) 275062
- CompTIA Network + Certified COMP10163630
- CompTIA Network Infrastructure Professional – CNIP COMP10163630
- EC Council Certified Security Administrator (ECSA) ECC947248
- EC Council Certified Encryption Specialist (ECES)
- CISSP – ISSAP – Certified Information Systems Architecture Professional #387731
- CISSP – ISSEP Information Systems Security Engineering Professional #387731
- Oxygen Phone Forensics Certified
- CompTIA Security+ COMP001021522764
- SC-300 - Microsoft Identity and Access Administrator

12. Specific publications that I have authored or participated in related to NFC, chip design, and/or mobile devices include the following:

- Easttom, C. (2005). Introduction to Computer Security. New York City, New York: Pearson Press.
- Easttom, C. & Dulaney, E. (2015). CompTIA Security+ Study Guide: SY0-401. Hoboken, New Jersey: Sybex Press.
- Easttom, C. & Roberts, R. (2018). Networking Fundamentals, 3rd Edition. Goodheart-Wilcox Publishing.
- Easttom, C. (2020). Modern Cryptography: Applied Mathematics for Encryption and Information Security 2nd Edition. New York City, New York: Springer Press.
- Easttom, C. (2021). An In-Depth Guide to Mobile Device Forensics. CRC Press.
- Easttom, C., Mei, N. (2019). Mitigating Implanted Medical Device Cybersecurity Risks. IEEE 10th Annual Computing and Communication Conference UEMCON.
- Easttom, C., Sanders, W. (2019). On the Efficacy of Using Android Debugging Bridge for Android Device Forensics. IEEE 10th Annual Computing and Communication Conference UEMCON.

13. I am qualified to render the opinions set forth herein. Under my definition of a POSITA, or Mr. Lipoff's definition, set forth below, I am and was as of the priority date of the '756 Patent, at least one of ordinary skill in the art.

III. MATERIALS CONSIDERED

14. I have reviewed the '756 Patent, including the challenged claims, prosecution history, and relevant patent family. The '756 Patent was marked as Exhibit 1001, and its prosecution history was marked as Exhibit 1002.

15. I also reviewed the Petition, and each of Exhibits 1001-1041 attached to the Petition. I also reviewed Apple’s Exhibit 1042 that was attached to Petitioner’s Updated Exhibit List.

16. In forming my opinions, I have considered the materials listed above and any other documents cited in this declaration. I have also relied on my own education, knowledge, and experience in the relevant art.

17. I have also considered the understanding of a person of ordinary skill around the time of the invention of the ’756 Patent.

IV. SCOPE OF OPINIONS

18. I set forth my opinions throughout this declaration.

19. I understand that Petitioner argues that:

Ground	Claims	Proposed Ground of Unpatentability
1	1-3, 5-8, and 10	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> ¹ in view of <i>Holloway</i> ² and <i>Jazayeri</i> ³
2	4, 9, and 11-17	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Holloway</i> , <i>Jazayeri</i> , and <i>ISO-14443</i> ⁴

¹ U.S. Patent No. 8,229,852 (“*Carlson*,” Ex. 1005).

² WIPO International Patent Application Publication No. WO 02/49322 (“*Holloway*,” Ex. 1032).

³ U.S. Patent Application Publication No. 2008/0155268 (“*Jazayeri*,” Ex. 1007).

⁴ ISO/IEC 14443 (“*ISO-14443*,” Ex. 1016).

Ground	Claims	Proposed Ground of Unpatentability
3	18	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Holloway</i> , <i>Jazayeri</i> , <i>ISO-14443</i> , and <i>Sherman</i> ⁵
4	1-3, 5-8, and 10	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> ⁶ in view of <i>Murakami</i> ⁷
5	4, 9, and 11-17	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>ISO-14443</i> , and <i>Murakami</i>
6	18	Obvious under pre-AIA 35 U.S.C. § 103 over <i>Carlson</i> in view of <i>Jazayeri</i> , <i>ISO-14443</i> , <i>Sherman</i> , and <i>Murakami</i>

20. All six grounds rely on *Carlson* as a primary reference, and Petitioner's expert, Mr. Lipoff, suggests that a person of ordinary skill would have been motivated to combine *Carlson* with up to five different secondary references to meet the language of the claims.

21. I disagree. It is my opinion that the Challenged Claims (claims 1-18) of the '756 Patent would not have been obvious in view of the asserted references, alone or in combination, for the reasons discussed herein.

⁵ U.S. Patent Application Publication No. 2007/0232358 ("*Sherman*," Ex. 1014).

⁶ U.S. Patent No. 8,229,852 ("*Carlson*," Ex. 1005).

⁷ WIPO International Application Publication No. WO 01/95246 ("*Murakami*," Ex. 1009).

V. RELATED MATTERS

22. Patent Owner is asserting the '756 Patent against Petitioner in the Northern District of California, styled *Telcom Ventures LLC v. Apple Inc.*, Case No. 5:25-cv-05041 (filed October 4, 2024).

23. I understand that Patent Owner asserted a total of eight patents against Petitioner in that action: U.S. Patent Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,924,743, 11,937,172, and 12,028,793. I understand that Patent Owner has dismissed four of the asserted patents from the litigation, including the '756 Patent.

24. I understand that Petitioner filed IPR petitions against all eight patents originally asserted by Patent Owner. These are:

- IPR2025-01232, regarding U.S. Patent No. 9,462,411
- IPR2025-01233, regarding U.S. Patent No. 9,832,708
- IPR2025-01234, regarding U.S. Patent No. 10,219,199
- IPR2025-01235, regarding U.S. Patent No. 10,674,432
- IPR2025-01236, regarding U.S. Patent No. 11,770,756 (the Petition)
- IPR2025-01237, regarding U.S. Patent No. 11,924,743
- IPR2025-01238, regarding U.S. Patent No. 11,937,172
- IPR2025-01239, regarding U.S. Patent No. 12,028,793

25. I also understand Patent Owner asserted the '756 Patent against Samsung Electronics Co., Ltd. ("Samsung") in the Eastern District of Texas, styled *Telcom Ventures LC v. Samsung Electronics Co., Ltd. et al*, Case No. 2:24-cv-00691-JRG (filed August 21, 2024).

26. I understand Patent Owner asserted the same eight patents against Samsung in that action. I understand that Patent Owner informed Samsung that it was withdrawing its infringement allegations for two patents in the Samsung Litigation (but not the '756 Patent), but Samsung responded the same day by filing declaratory judgment claims of invalidity on all eight of the patents. Accordingly, the validity of all eight patents remains at issue in the Samsung action.

27. I understand that a jury trial for the suit between Patent Owner and Samsung is expected to begin on June 1, 2026. Ex. 2003.

28. I understand that Samsung filed IPR petitions against all eight patents originally asserted by Patent Owner. These are:

- IPR2025-00957, regarding U.S. Patent No. 11,937,172
- IPR2025-00972, regarding U.S. Patent No. 10,219,199
- IPR2025-00973, regarding U.S. Patent No. 9,462,411
- IPR2025-00974, regarding U.S. Patent No. 10,674,432
- IPR2025-00975, regarding U.S. Patent No. 9,832,708
- IPR2025-00976, regarding U.S. Patent No. 11,924,743

- IPR2025-00977, regarding U.S. Patent No. 11,770,756
- IPR2025-00978, regarding U.S. Patent No. 12,028,793

29. I understand that institution was denied in all eight of those IPRs.

30. I understand Google LLC (“Google”) has filed IPR petitions against seven of the eight patents asserted by Patent Owner in the above litigations. These are:

- IPR2025-01349, regarding U.S. Patent No. 11,924,743
- IPR2025-01389, regarding U.S. Patent No. 11,937,172
- IPR2025-01401, regarding U.S. Patent No. 12,028,793
- IPR2025-01408, regarding U.S. Patent No. 9,832,708
- IPR2025-01409, regarding U.S. Patent No. 11,770,756
- IPR2025-01419, regarding U.S. Patent No. 10,219,199
- IPR2025-01421, regarding U.S. Patent No. 10,674,432

31. As of the signing of this declaration, I have been retained to provide an opinion in all eight IPRs filed by Petitioner against the patents asserted by Patent Owner. I have also been retained to provide an opinion in each of the IPRs filed by Samsung and Google.

VI. LEGAL STANDARDS

32. For purposes of this Declaration, I use the legal principles below as a guide in formulating my opinions. I am not an attorney, and I am not offering any

opinions regarding legal matters; however, I have been informed by Telcom Venture's counsel of the legal principles relevant to the issues herein and have the following understanding.

33. In an *inter partes* review proceeding, I understand that a party seeking to invalidate a claim must prove invalidity by a preponderance of the evidence, which I understand to mean evidence that convinces you that it is more likely than not that the particular proposition is true. I understand that the preponderance of the evidence standard applies to all aspects of an allegation of anticipation or obviousness, including the prior art status of the relevant reference(s).

A. Claim Construction

34. I understand the first step in determining whether or not a patent claim is valid is to properly construe the claims. I understand that the words of a claim are generally given their ordinary and customary (sometimes referred to as their plain and ordinary) meaning as understood by a person of ordinary skill in the art at the time of the invention. I also understand that, as a general matter, a claim should not be limited to a preferred embodiment, but that in certain cases, the scope of the right to exclude may be limited by a narrow disclosure or by positions taken, such as by statements made during patent prosecution. I also understand the claims must be supported by the specification. Also, to the extent that a patent claims priority to an earlier filed application, the claims must be supported by the disclosure in that

application. For terms that have not been construed, I understand that they should be afforded their plain and ordinary meaning to one of ordinary skill in the art.

35. I understand that the plain and ordinary meaning of a claim term is the meaning a person of ordinary skill in the art would have understood at the time of the effective date in view of the specification and the prosecution history.

B. Obviousness

36. I understand that a claimed invention is not patentable under 35 U.S.C. § 103 if the differences between the invention 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 person having ordinary skill in the art to which the subject matter pertains. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and objective indicia of non-obviousness to the extent they exist.

37. I understand that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the art at the time of the invention. A person of ordinary skill in the art is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. The person of ordinary skill is not an automaton and may be able to fit together the teachings of multiple patents employing ordinary

creativity and the common sense that familiar items may have obvious uses in another context or beyond their primary purposes.

38. I understand that if a reference or proposed combination of references does not disclose or suggest all of the elements of a claim, the combination cannot render the claim obvious. I also understand that in order to combine prior art references to show obviousness, a person of ordinary skill in the art, without knowledge of the claimed invention, or without the use of hindsight, must have been motivated to combine the prior art by some suggestion or teaching in the prior art, the knowledge of one of skill in the art, or the nature of the problem to be solved.

39. I understand that an invention would have been obvious if a designer of ordinary skill in the art, facing the wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it may have been obvious to a person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would have recognized that it would improve similar devices in the same way, using the technique may have been obvious. I understand, however, that routine experimentation does not necessarily preclude patentability.

40. I understand that obviousness of a patent claim cannot properly be established through hindsight, and that elements from different prior art references, or different embodiments of a single prior art reference, cannot be selected to create the claimed invention using the invention itself as a roadmap. I understand that the claimed invention as a whole must be compared to the prior art as a whole, and courts must avoid aggregating pieces of prior art through hindsight that would not have been combined absent the inventors' insight.

C. Motivations to Combine

41. I understand that in order to show obviousness based on a single reference or a combination of references, a particular motivation to modify the reference or combine the teachings in the references, and a reasonable expectation of success must be shown.

42. I understand that the art must evidence a motivation to combine or modify the independently known elements to arrive at the claimed invention and an explanation as to how or why the references would be combined to arrive at the claimed invention to solve the particular problem. I understand that a challenger must show that there was a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does in an obviousness determination. I also understand that it is not

enough to prove obviousness merely by a showing that the references were capable of combination without a suggestion of the desirability of the modification.

43. I understand that there is no single way to define the line between true inventiveness on the one hand (which is patentable) and the application of common sense and ordinary skill to solve a problem on the other hand (which is not patentable). For example, market forces or other design incentives may be what produced a change, rather than true inventiveness. I may consider whether the change was merely the predictable result of using prior art elements according to their known functions, or whether it was the result of true inventiveness. I may also consider whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent. I may consider whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent. I may consider whether the innovation applies a known technique that had been used to improve a similar devices or method in a similar way. I may also consider whether the claimed invention would have been obvious to try, meaning that the claimed innovation was one of a relatively small number of possible approaches to the problem with a reasonable expectation of success by those skilled in the art.

44. I also understand, however, that I must be careful not to determine obviousness using the benefit of hindsight; many true inventions might seem

obvious after the fact. I should put myself in the position of a person of ordinary skill in the field at the time the claimed invention was made and I should not consider what is known today or what is learned from the teaching of the patent.

45. Finally, I understand that any obviousness rationale for modifying or combining prior art must include a showing that a person of ordinary skill would have had a reasonable expectation of success. I further understand that whether a proposed modification or combination of the prior art has a reasonable expectation of success is determined at the time the invention was made.

VII. LEVEL OF ORDINARY SKILL IN THE ART

46. I understand that patent claims are to be interpreted from the viewpoint of one of ordinary skill in the relevant art. To determine the level of skill that would be “ordinary,” I understand that a person of skill (“POSITA”) must generally have the capability of understanding the general principles that are applicable to the pertinent art.

47. In my opinion, a POSITA would have had at least a bachelor’s degree in electrical engineering, computer engineering, or a related field, with about two years of experience in wireless communications. More work or practical experience may qualify one not having the requisite education as a person with ordinary skill in the art, while a higher level of education could offset less experience. I was at least

a person of ordinary skill in the art as of the effective filing dates of the Asserted Patents under this definition.

48. I have reviewed Mr. Lipoff's Declaration (Ex. 1003). I understand that Mr. Lipoff contends that a POSITA would have had "a bachelor's degree in computer science, electrical engineering, computer engineering or equivalent from an accredited academic program with a year of work experience with mobile payment systems or wireless communication systems." Ex. 1003, ¶51. Mr. Lipoff also contends that a POSITA "would have been knowledgeable regarding the field of mobile communication devices using mobile payment systems and wireless communication systems, including short-range communication technologies" and that "[a] POSITA would have possessed a working knowledge of short-range communication technologies in portable wireless devices." *Id.* I disagree that "a working knowledge of short-range communication technologies" is necessary. Nonetheless, I was at least a person of ordinary skill in the art as of the effective filing dates of the Asserted Patents under Mr. Lipoff's definition. Thus, I met the requirements of a POSITA under either my definition or Mr. Lipoff's definition as of the priority date of the '756 Patent. Furthermore, whether I apply Mr. Lipoff's definition of a POSITA or my own my opinions herein would not change.

VIII. CLAIM CONSTRUCTION

49. I understand that unless claim terms are provided an express construction, the terms must be given their plain and ordinary meaning.

A. “Physiological State”

50. I understand that Petitioner contends that “physiological state” requires a construction. *See* Petition at 4-6; Ex. 1003, ¶¶45-50. Specifically, Mr. Lipoff suggests that a fingerprint is not a “physiological state.” Ex. 1003, ¶49.⁸ I disagree.

51. Nonetheless, a construction is not necessary to resolve the proposed grounds. Mr. Lipoff has proposed two sets of grounds under different interpretations of “physiological state.” Under the first set of grounds, Mr. Lipoff relies on fingerprint-based biometric authentication to satisfy the “physiological state” limitation. Ex. 1003, ¶50. Under the second set of grounds, Mr. Lipoff relies on “a datapoint representing a snapshot of the parameter in time.” *Id.* In my opinion, the Challenged Claims are not taught or suggested by the prior art under either construction. Because the grounds fail regardless of the physiological state that Mr. Lipoff relies on, it is my opinion that a construction is not necessary for the

⁸ Mr. Lipoff also suggests that facial geometry is not a “physiological state,” but facial geometry is not relevant to the Petition or the grounds therein. I focus on the “fingerprint” part of his construction.

purposes of institution. I reserve the right to address the construction of “physiological state” if this case is instituted.

IX. TECHNOLOGY BACKGROUND

52. Below, I provide a brief overview of the history of contactless smart cards, or proximity cards, and the use of the same technologies in devices.

A. Near Field Communications (“NFC”)

53. Near Field Communication (“NFC”) is a broad term for short-range wireless communication technology that allows devices to exchange data when they are brought very close together. It is an extension of Radio Frequency Identification (“RFID”) technology, designed for secure, quick, and convenient data transfer.

54. NFC-capable devices can communicate with other NFC-capable devices in either active or passive mode. In active mode, both devices generate their own radio frequency field to transmit data. Ex. 2008 at 4. In passive mode, one device generates the radio frequency field while the other responds without a power source. *Id.*

55. A paper by Liu et al. provides a history of NFC, stretching back to the first understanding of the wave theory of light. Ex. 2009 at 4. That paper includes an overview of NFC history which is shown here:

TABLE I: Timeline of NFC Milestones

1678		•	Huygens presented his “Wave Theory of Light”.
1801		•	Young presented the double-slit diffraction experiment.
1815		•	Fresnel presented a series of memoirs about his understanding of diffraction.
1821		•	Fraunhofer constructed the first diffraction grating.
1887		•	Hertz demonstrated the existence of radio waves.
1891		•	Lord Rayleigh calculated the Rayleigh distance $\frac{A^2}{2\lambda}$.
1947		•	Cutler <i>et al.</i> reformulated the Rayleigh distance as $\frac{2A^2}{\lambda}$.
1956		•	Polk calculated the Fresnel distance.
1983		•	The first patent on RFID-based NFC was granted.
1984		•	Winters formulated the initial theory of MIMO.
1994		•	The first patent on MIMO was granted.
1996		•	Foschini laid down crucial theoretical foundations for MIMO.
1999		•	Driessen and Foschini utilized a spherical wave-based model to characterize LoS MIMO.
2003		•	Jiang <i>et al.</i> proposed to use spherical wave-based models to describe short-range MIMO.
2010		•	Marzetta proposed the concept of massive MIMO.
2015		•	Channel measurement results on massive MIMO necessitated the use of a spherical wave-based channel model.
2016		•	Prather proposed the concept of holographic MIMO.
2017		•	Hu <i>et al.</i> re-showed the potential of large intelligent surfaces in enhancing wireless transmissions.
2018		•	Amiri <i>et al.</i> proposed the concept of ELAA.
2023		•	The first tutorial review of NFC was presented.

56. Despite the long history of the physics and technology supporting NFC, NFC itself is relatively new. For example, the NFC Forum was created in 2004 to ensure maximum compatibility across all implementations of NFC technology. Ex. 2010 at 1. But the NFC Forum was not even founded until many years after the first standards related to smart cards were published. As late as 2012, *see* Ex. 2011 at 1, and even 2015, some sources still referred to NFC as an “emerging technology.” Ex. 2012 at 1.

57. Within the umbrella of NFC, there are numerous individual standards that are more specific. One such standard is ISO/IEC 14443. The ISO/IEC 14443

standard has four parts. Part 1 defines the physical properties of the card (e.g., size, durability, environmental tolerance). Part 2 specifies how the card is powered by the RF field of the reader and how modulation/coding are done for transmitting and receiving signals. Part 3 describes card initialization and how multiple cards in the field are identified and selected (anti-collision protocol). Part 4 defines higher-level data exchange protocols, including how commands and responses are structured.

58. The specificity of individual NFC standards means that any such standard is self-sufficient. In other words, a POSITA consulting one of these standards, such as ISO/IEC 144443, would have a complete solution for near field communications and would not need to look to other standards or technologies.

X. U.S. PATENT NO. 11,770,756 (“’756 Patent”) (Ex. 1001)

A. Priority Date

59. Through a series of continuation applications, the ’756 Patent claims the benefit of U.S. Patent Application No. 12/264,711—later issued as U.S. Patent No. 9,462,411, which has a filing date of November 4, 2008. Ex. 1001.

60. I understand that Mr. Lipoff does not challenge this priority date for purposes of the Petition. For the purposes of Patent Owner’s Preliminary Response, I have assumed that each of the challenged claims is entitled to at least a priority date of November 4, 2008. Ex. 1003, ¶32.

B. '756 Patent Overview

61. The '756 Patent describes mobile wireless devices and methods of using a mobile wireless device to perform financial transactions, but only when certain conditions or criteria are met, such as the satisfaction of a proximity condition and a value of a parameter, e.g., a physiological parameter, satisfying a criterion. Ex. 1001, 1:25-30; 6:13-23. The specification recognizes that devices in the art were rigidly configured to perform a predetermined number of functions. *Id.*, 1:39-44. The '756 Patent addresses this rigidity problem by providing devices and methods that “may be used to enable adaptively one or more modes/functions of a device” based upon the satisfaction of certain criteria. *Id.*, 1:49-54. The specification explains that the invention advantageously allows “a mobile wireless device [to] act as a ‘wallet’ (over and above other functions) only when it is time to pay for an item and not act as a wallet when there is no need to do so.” *Id.*, 1:44-57.

62. The '756 Patent also describes estimating “a value of at least one other parameter that may be associated with the wireless communications device . . . and/or an entity (living or otherwise) that is associated with and/or is proximate to the wireless communications device.” *Id.*, 6:15-19. Such parameters include “velocity, acceleration, ToD, ToM, ToY, humidity, temperature, height, level of brightness, level of darkness, a blood pressure, a heart rate, a blood content, a physiological state, a psychological state, etc.” *Id.*, 6:20-23. These parameters can

be estimated using “sensors that may, according to some embodiments, be device-based and/or network assisted/based means and/or sensors.” *Id.*, 6:28-30. The disclosed wireless communications devices may be “configured to selectively enable the first communications mode/function” responsive to a value of such a parameter. *Id.*, 6:40-44.

C. The ’756 Patent’s Prosecution History

63. I have reviewed the prosecution history of the ’756 Patent.

64. U.S. Patent Application No. 17/653,748 was filed March 7, 2022 and issued as U.S. Patent No. 11,770,756 on September 26, 2023.

65. In a non-final rejection, the Examiner rejected the claims as unpatentable under § 103 over U.S. Patent Application Publication No. 2009/0058637 in view of U.S. Patent Application Publication No. 2003/0172028 and for double patenting over claims 1, 7, and 17 of U.S. Patent No. 11,304,118. Ex. 1002 at 104, 106. Applicants then amended the independent claims to include “responsive to the value that is determined . . . enabling . . . a number of functions . . . and disabling a function” and filed a terminal disclaimer to traverse the rejections. *Id.* at 135–37. The Examiner allowed the claims of the ’756 Patent following this amendment and filing of the terminal disclaimer. The Examiner stated in the Notice of Allowance that the closest prior art of record, U.S. Patent Application Publication No. 2009/0058637, alone or in combination failed to teach

or suggest “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device.” *Id.* at 207.

XI. ASSERTED REFERENCES

A. *Carlson* (Ex. 1005)

66. U.S. Patent No. 8,229,852 to Carlson is titled “Secure Mobile Payment System.” *Carlson* is directed to portable wireless devices that are used to conduct contactless payment transactions in a secure manner. *Carlson*, 1:16-20.

67. *Carlson* explains that “[d]ue to the wireless nature of the contactless reader, it is possible that the contactless reader may be used for surreptitious interrogation of the portable wireless device by intercepting the portable wireless device’s communication.” *Carlson*, 1:64-2:1. *Carlson* further explains that “it is conceivable that a contactless reader may be developed or modified to enhance its power and sensitivity and thereby increase its ability to interrogate with and intercept signals from the portable wireless device from a greater distance than specified in standards used for contactless readers.” *Carlson*, 2:1-6.

68. *Carlson* describes “[t]heft of sensitive information, such as an account number, using wireless interrogation or interception of communications from portable wireless device” as a “major concern for consumers and businesses alike.”

Carlson, 2:7-10. *Carlson* notes that wireless interrogation can “occur at virtually any time and place,” and “[o]nce the victim of the wireless interrogation discovers that they had sensitive information stolen, it is often too late to discover where the theft took place.” *Carlson*, 2:10-16. As a result, “[t]he victim must then deal with the consequences and hassle of correcting the unauthorized access and possible uses of the information.” *Carlson*, 2:16-18.

69. *Carlson* describes other “safeguards for protecting purchase from fraudulent attacks,” including employing encryption technologies to encrypt the payment account number and other data associated with account transactions. *Carlson*, 2:19-23. *Carlson* explains that many merchants avoid implementing or upgrading to the latest encryption technology “[d]ue to the cost, time, and risk of potential business interruption (e.g., loss of sales).” *Carlson*, 2:27-35.

70. *Carlson*’s solution describes the use of “pseudo account identifiers” or “PPAI.” *Carlson*, 2:62-63. . According to *Carlson*, “[p]seudo primary account identifiers may include identifiers that are similar in format to a consumer’s real account identifier.” *Carlson*, 5:30-32. “These account identifiers may include account numbers or any other alphanumeric sequence.” *Carlson*, 2:66-3:1. *Carlson* also describes the pseudo account identifier as “bogus, fake, decoy, substitute, or the like.” *Carlson*, 5:42-43. “

71. *Carlson* describes “a method for conducting a transaction that includes receiving a pseudo account identifier that corresponds to a consumer’s account identifier.” *Carlson*, 3:3-6. In some embodiments of *Carlson*, “the pseudo primary account identifier may not be requested at all, but rather is pushed to the portable wireless device at any time, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” *Carlson*, 7:4-7, 12:67-13:3. *Carlson* also explains that “the pseudo primary account identifier may not be requested by the portable wireless device at all” and “[t]he portable wireless device may generate the pseudo primary account identifier.” *Carlson*, 7:15-19.

B. *Holloway* (Ex. 1032)

72. International Patent Application Publication No. WO 02/49322 to Holloway is directed to a mobile telephone that “includes a device (15) for checking the identity of a user in connection with various transactions.” *Holloway*, Abstract. *Holloway* describes “fingerprint scanning means, voice or password recognition means (e.g. using a microphone of the telephone), photograph display means (e.g. using a display (12) of the telephone) or retina recognition means.” *Id.*

73. *Holloway* proposes using a “means for checking the identity of a user of the unit” to solve the problem of identity verification. *Holloway*, 2:1-5. *Holloway* explains that “the means for telephonic communication includes a display, a microphone and a keypad and said means for checking identity is arranged to show

a photograph of the user on said display, and/or means for recognizing the voice of the user and/or a password spoken by the user when the user speaks into said microphone, and/or incorporates means for identifying a PIN number entered by a user on said keypad.” *Holloway*, 2:14-18.

C. *Jazayeri* (Ex. 1007)

74. U.S. Patent Application Publication No. 2008/0155268 to Jazayeri is directed to “[a]n architecture . . . that controls access to secure data via biometric verification.” *Jazayeri*, Abstract. *Jazayeri* discloses a “memory module that communicates with biometric data to establish a heightened level of security for controlling access to data stored in the non-volatile memory.” *Id.* “Specifically, biometric data is input and communicated to the security processor, then compared against the existing biometric templates stored in the non-volatile memory. If the data matches, verification is sent to the external processor and the user is granted access to the secure assets.” *Id.*

75. *Jazayeri* requires a security processor. *Jazayeri*, ¶[0006] (“As the security processor controls access to the entire non-volatile memory space and monitors all traffic to and from the non-volatile memory components, the security processor is able to manage access to the secure assets stored in the non-volatile memory.”); *see also Jazayeri*, ¶¶[0024], [0025], [0027], [0028], [0030], Figs. 1, 2. *Jazayeri* explains that “[o]nly the security processor 104 accesses the security

software from the nonvolatile memory 102 and performs security functions based on the specific security software being executed.” *Jazayeri*, ¶[0027].

76. Figure 3 of *Jazayeri* illustrates a block diagram of *Jazayeri*’s security processor.

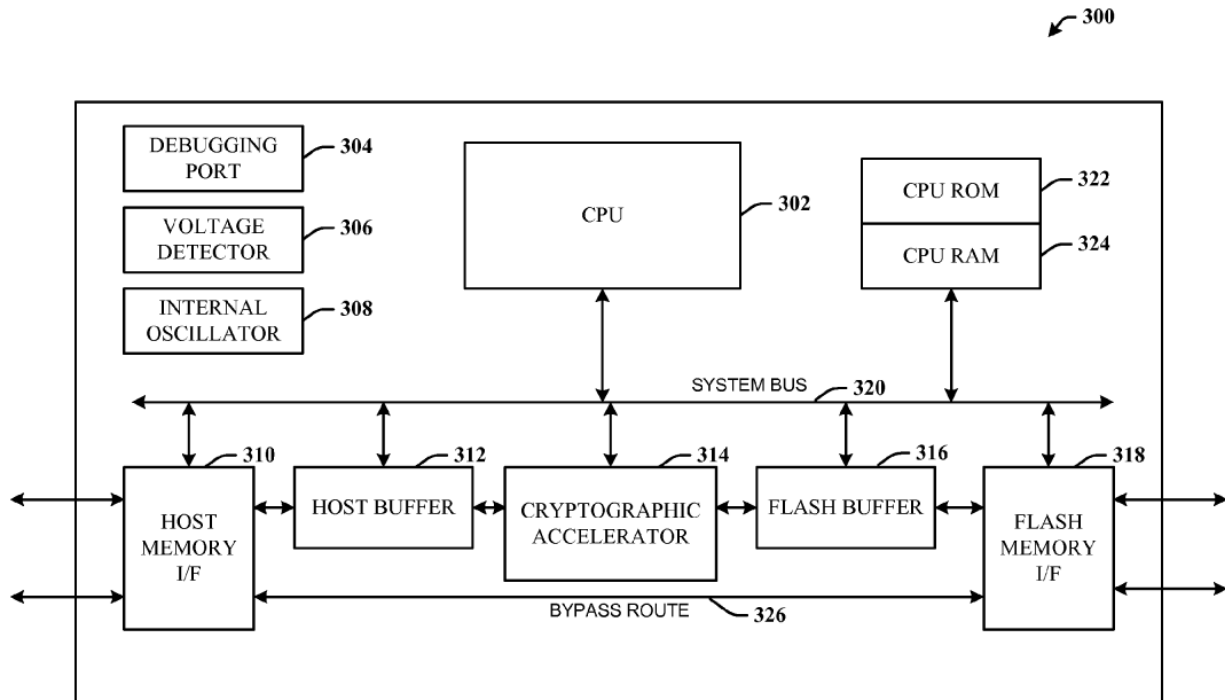


FIG. 3

Jazayeri, Fig. 3.

77. *Jazayeri*’s security processor comprises sophisticated hardware. *Jazayeri* explains that “[a] cryptographic accelerator 314... performs all the cryptographic algorithms, symmetric and a-symmetric needed by the system.” *Jazayeri*, ¶[0033].

D. *ISO-14443* (Ex. 1016)

78. The ISO/IEC 14443 standard has four parts. Part 1 defines the physical properties of the card (e.g., size, durability, environmental tolerance). Part 2 specifies how the card is powered by the RF field of the reader and how modulation/coding are done for transmitting and receiving signals. Part 3 describes card initialization and how multiple cards in the field are identified and selected (anti-collision protocol). Part 4 defines higher-level data exchange protocols, including how commands and responses are structured.

79. *ISO-14443* “is one of a series of International Standards describing the parameters for identification cards as defined in ISO/IEC 7810 and the use of such cards for international interchange.” *ISO-14443*, 4.

E. *Sherman* (Ex. 1014)

80. United States Patent Application Publication No. 2007/0232358 to Sherman was filed on April 2, 2007, and published on October 4, 2007. *Sherman* is directed to an “apparatus for and method of Bluetooth and WiMAX coexistence.” *Sherman*, Abstract. *Sherman* explains that WiMAX is “a long range system that uses licensed spectrum to deliver a point-to-point connection to the Internet from an ISP to an end user.” *Sherman*, ¶[0009].

F. *Murakami* (Ex. 1009)

81. International Patent Application Publication No. WO 01/95246 to Murakami is directed toward “a method and device for biometric authentication

using a signal transmitter (20), a signal receiver (22), a memory module, and a processing module.” *Murakami*, Abstract. Specifically, *Murakami* “employ[s] histological and physiological biometric markers that are substantially unique to an individual in order to permit an individual to activate a device, participate in a transaction, or identify him or herself.” *Murakami*, 1:10-13.

XII. THE CHALLENGED CLAIMS OF THE ’756 PATENT WOULD NOT HAVE BEEN OBVIOUS

A. Petitioner’s Grounds 1–6 Fail Because the Challenged Claims Would Not Have Been Obvious Over the Asserted References.

82. The following paragraphs address examples of why the challenged claims would not have been obvious in view of *Carlson* in combination with *Holloway* and *Jazayeri* or in combination with *Murakami*.

83. While I address certain limitations and combinations to demonstrate that each of the challenged claims is not unpatentable, I reserve the right to supplement this declaration to include additional information and opinions related to any and all challenged claims and claim elements and the asserted Grounds and prior art references.

84. Claim element 1[b] and 6[b] require “determining by the device a value of the parameter that is sensed.” Claims 2 through 5 depend directly or indirectly from claim 1, and thus also include this limitation. Claims 7 through 10 depend directly or indirectly from claim 6, and thus also include this limitation. Similarly,

claim element 11[b] requires “determining by the wireless device a value of the parameter that is sensed and determining by the wireless device whether or not the value that is sensed satisfies a threshold criterion,” and claim element 14[b] requires “determining a value that is associated with the parameter that is sensed and determining whether or not the value satisfies a threshold criterion.” Claims 12 and 13 depend from claim 11, and thus also include this limitation. Claims 15 through 18 depend from claim 14, and thus also include this limitation. All dependent claims depend from independent claim 1, 6, 11, or 14.

85. In Ground 1, Mr. Lipoff opines that a combination of *Carlson*, *Holloway*, and *Jazayeri* teach claim element 1[b]. Ex. 1003, ¶103. Mr. Lipoff merely incorporates his analysis of claim element 1[b] into his discussion of claim element 6[b]. Ex. 1003, ¶126. Mr. Lipoff also incorporates his analysis of claim element 1[b] into his discussion of claim elements 11[b] and 14[b]. In Grounds 4–6, Mr. Lipoff claims to “apply a narrower interpretation” for physiological state and instead suggests that a POSITA would have combined *Carlson* with *Murakami* instead of *Holloway* and *Jazayeri*. I disagree with Petitioner’s assertions.

86. Claim elements 3[a] and 8[a] and claim elements 11[d] and 14[d]⁹ require “requesting . . . from a second device an authorization to enable a function for conducting a financial transaction by the device.” Claims 4 and 5 depend from dependent claim 3, and thus also include this limitation. Claims 9 and 10 depend from dependent claim 8, and thus also include this limitation. Claims 12 and 13 depend from independent claim 11, and thus also include this limitation. Claims 15 through 18 depend from independent claim 14, and thus also include this limitation.

87. In Grounds 1-3, Mr. Lipoff relies on a combination of *Carlson*, *Holloway*, and *Jazayeri* to teach the “authorization” limitations of claims 3, 8, 11, and 14. In Ground 1, Mr. Lipoff opines that the *Carlson-Holloway-Jazayeri* combination teaches claim element 3[a] of dependent claim 3. Ex. 1003, ¶¶119-120. Mr. Lipoff merely incorporates his analysis of claim element 3[a] into his discussion of claim element 8[a] of dependent claim 8. Ex. 1003, ¶133. In Ground 2, addressing

⁹ Claim elements 3[a] and 8[a] are from dependent claims 3 and 8. Claim elements 11[d] and 14[d] are from independent claims 11 and 14. Because Mr. Lipoff provided his analysis with respect to “requesting . . . from a second device an authorization to enable a function for conducting a financial transaction by the device” with respect to dependent claim 3[a], I likewise discuss dependent claim 3[a] instead of an independent claim.

claim elements 11[d] and 14[d] from independent claims 11 and 14, Mr. Lipoff again merely incorporates his discussion of 3[a] from Ground 1 into his discussion of claim elements 11[d] and 14[d]. Ex. 1003, ¶¶167, 179. In Grounds 4–6, Mr. Lipoff claims to “apply a narrower interpretation” for physiological state and instead suggests that a POSITA would have combined *Carlson* with *Murakami* instead of *Holloway* and *Jazayeri*. I disagree with respect to all Grounds.

1. Carlson in View of Jazayeri Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed” (Grounds 1-3).

88. Claim limitations 1[b], 6[b], and 11[b] state “determining . . . a value of the parameter that is sensed.” Claim limitation 14[b] similarly states “determining a value that is associated with the parameter that is sensed.” Mr. Lipoff states that “*Carlson-Holloway-Jazayeri* teaches Claim 1(b).” Ex. 1003, ¶103; *see also id.* at ¶127 (addressing limitation 6[b] and stating “*See supra* Claim 1(b)”), ¶165 (addressing limitation 11[b] and stating “*See supra* Claims 1(b)-1(c)”), ¶177 (addressing limitation ¶14[b] and stating “*See supra* Claims 1(b)-1(c)”).¹⁰ I disagree.

¹⁰ Claim limitation 1[c] states “responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device.” Mr. Lipoff’s analysis of claim limitation 1[c] addresses “satisfying a

89. Mr. Lipoff states that “[l]ike *Carlson* and *Holloway*, *Jazayeri* discloses providing access to secure data on a device using biometric data such as ‘iris data, face data, ***fingerprint data***, Deoxyribonucleic acid (DNA), or any other human physical characteristic for identification and authentication purposes.” Ex. 1003, ¶104 (citing *Jazayeri*, ¶[0029]). Mr. Lipoff does not identify any disclosures in *Carlson* or *Holloway* that disclose or render obvious limitation 1[b], nor does Mr. Lipoff identify how *Carlson* and *Holloway* allegedly similarly disclose “providing access to secure data on a device using biometric data.” Based only on this disclosure in *Jazayeri*, Mr. Lipoff concludes that a POSITA would have been motivated to “unlock” the *Carlson-Holloway* device “pursuant to the biometric authentication process described by *Jazayeri*.” Ex. 1003, ¶106. For the reasons explained below, I disagree.

threshold criterion” (Ex. 1003, ¶113), which is also required in claim limitations 11[b] and 14[b]. Given the difference in claim language, Mr. Lipoff’s analysis and incorporation of 1[c] is not relevant to the analysis of whether *Carlson-Holloway-Jazayeri* teaches the “determining by the device a value of the parameter that is sensed” requirement in 11[b] and 14[b]. If this petition is instituted, I reserve the right to address Mr. Lipoff’s analysis of limitation 1[c].

***A POSITA Would Not Have Had a Reasonable Expectation of
Success in Modifying Carlson with Jazayeri***

90. I first note that Mr. Lipoff greatly underestimates the difficulties a POSITA would have in combining *Carlson* and *Jazayeri*, based on the system architecture of *Jazayeri*. Specifically, *Jazayeri* depends on a security processor (Figure 1, Figure 2, ¶¶[0005]-[0006], [0023]-[0025], [0027]) and a cryptographic accelerator (Figure 3, ¶[0034]). *Jazayeri* ¶[0027] confirms the essential nature of the security processor as it states: “[o]nly the security processor 104 accesses the security software from the nonvolatile memory 102 and performs security functions based on the specific security software being executed.” *Jazayeri*, ¶[0027]. The security processor is further depicted in *Jazayeri* Figure 3, which provides a block diagram of a security processor of the memory module:

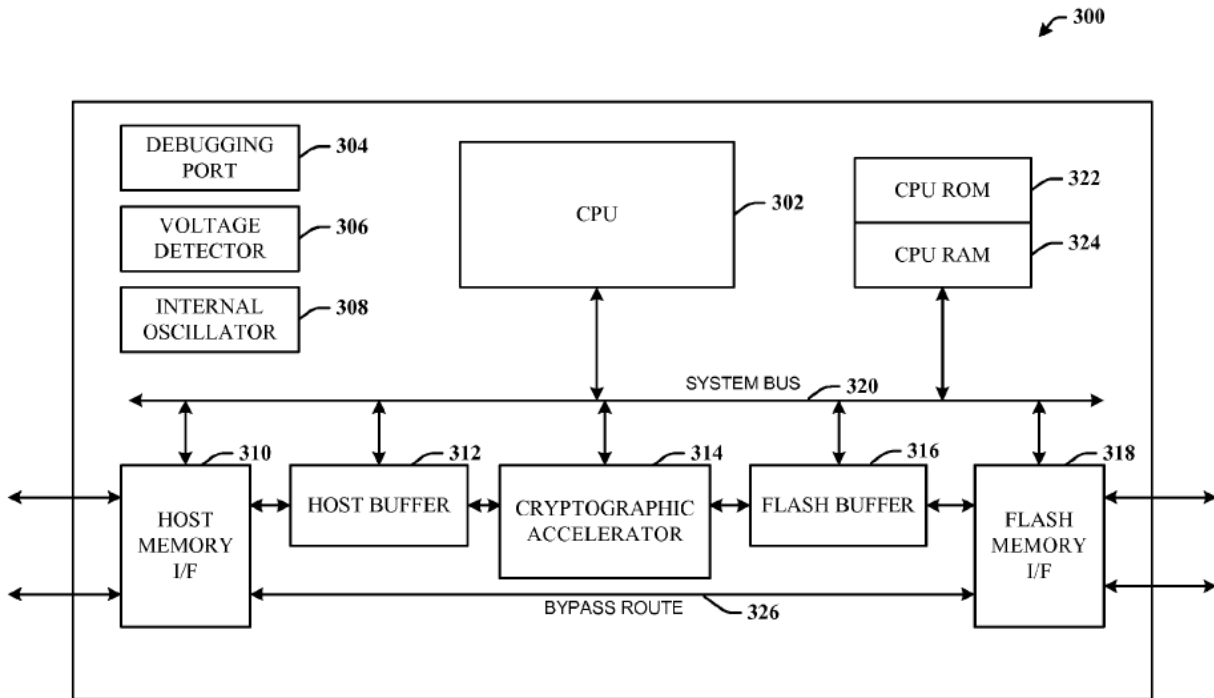


FIG. 3

Jazayeri, Fig. 3.

91. With respect to a POSITA, Mr. Lipoff states that “[i]n my experience working in this field, most people of ordinary skill in the art as of the earliest possible priority date of November 4, 2008, would have had a bachelor’s degree in computer science, electrical engineering, computer engineering or equivalent from an accredited academic program with a year of work experience with mobile payment systems or wireless communication systems. A POSITA would also have possessed a working knowledge of short range communication technologies in portable wireless devices.” Ex. 1003, ¶51. Nothing in Mr. Lipoff’s definition of a POSITA includes the requirement that a POSITA have knowledge of security processor

design or cryptography. As such, a POSITA, as defined by Mr. Lipoff or even a POSITA under the definition I propose, would not have been able to combine *Jazayeri* with any other prior art based at least on its complex architecture, which includes the security processor.

92. Mr. Lipoff erroneously interprets *Jazayeri* and states that *Jazayeri* relies on “common hardware elements,” stating “[f]or example, *Jazayeri*’s memory module 202, integrated into a mobile device (*Jazayeri*, ¶[0031]), includes common hardware elements, including a security processor 204, non-volatile memory 206, and volatile memory 208. *Id.*, ¶[0028], Fig. 2. These elements are no more than common hardware elements housed within the secure memory module 202, where ‘access control rights of the nonvolatile memory can be set so that the security processor alone has access’ to the contents of the memory.” Ex. 1003, ¶111. Mr. Lipoff is inaccurate in his summary of *Jazayeri*. *Jazayeri* requires a sophisticated security processor, specially designed for *Jazayeri*’s disclosed system and purposes. In fact, it is the “security processor 204 [that] will capture the user’s biometric data via the biometric sensor 214 the compare the biometric data against biometric templates stored in the non-volatile memory 206 for verification.” *Jazayeri*, ¶[0030]. Without this processor, *Jazayeri* has no mechanism for performing the disclosed verification process.

93. Specifically, *Jazayeri* provides specific details about its custom security processor. *Jazayeri* specifically highlights that its security processor is specially designed for processing biometric data and it is this security processor that passes verification data to another external processor. That is, the security processor is necessary for any biometric authentication process disclosed in *Jazayeri*.

The security processor provides for concurrent processing of security protocols, provides a secure execution environment within the memory module to evaluate and store biometric data, communicates either directly or indirectly with the biometric data sensors to fetch the biometric data, and analyzes the biometric data to control access to data or applications stored in the non-volatile memory. Specifically, biometric data is input and communicated to the security processor. The biometric data is then compared against the biometric data stored in the non-volatile memory. If the data matches, verification is sent to the external processor, and the user or system is granted access.

Jazayeri, ¶[0005].

94. More details are disclosed in *Jazayeri*, which confirms to the POSITA that the security processor is an essential part of *Jazayeri* and not a common hardware element:

In more detail, FIG. 3 illustrates the components of a security processor 300. The security processor 300 includes a central processing unit (CPU) 302 or any other type of low power application processor. The

CPU 302 within the security processor 300 can manage the flash memory storage (not shown) and provide a secure environment to implement authentication algorithms and security software. The security processor 300 also includes a Joint Test Action Group (JTAG) port 304 for debugging the system with a mechanism to prevent tampering, a voltage detector 306 that indicates the voltage level of the security processor 300 and stops the memory module from functioning when voltage levels are outside of the acceptable range in order to prevent side channel attacks, and an internal oscillator 308 that provides a clock for the security processor 300. This clock may be exported in its present form or it may be divided to provide the clock signal for other components such as a separate NFC RF chip or a fingerprint sensor. However, other mechanisms (not shown) can be provided that help prevent tampering. For example, temperature detecting, metal overlay (to hide signals), and scrambling of signals are additional methods that can be utilized in the security processor 300. A host memory interface (I/F) 310 handles all the flash memory transactions with a host processor (not shown). Specifically the host memory I/F 310 manages signaling, thus complying with the interface definitions of the flash memory. The host memory I/F 310 also manages interpretation or differentiating between a secure and non-secure request, and monitors requests to the non-volatile memory to enforce access rights and permissions.

Jazayeri, ¶[0033]; *see also id.* at ¶¶[0034]-[0036], [0039], [0043]-[0044].

95. *Jazayeri* did not intend its security processor to be “common hardware elements,” as alleged by Mr. Lipoff. Instead, as disclosed in the detailed description

Telcom Ventures Exhibit No. 2006

Apple Inc. v. Telcom Ventures LLC

IPR2025-01236, U.S. Patent No. 11,770,756

Page 43 of 61

and shown in the block diagram, *Jazayeri* disclosed a custom security processor to provide “a secure environment to implement authentication algorithms and security software.” *Jazayeri* ¶[0033]. As a result, it is my opinion that the POSITA would not have been able to combine *Jazayeri* with *Carlson*, and would not have had a reasonable expectation of success in doing so.

A POSITA Would Not Have Been Motivated to Combine Carlson with Jazayeri

96. Furthermore, there is no motivation to modify *Carlson*’s system, modified by the biometric authentication process of *Jazayeri*. Mr. Lipoff proposes combining *Carlson* and *Holloway* with *Jazayeri* to “unlock[] a device with biometric authentication.” Ex. 1003, ¶107. I disagree.

97. A POSITA would have readily understood that using biometrics of *Jazayeri* to unlock a device is contrary to the teachings of *Carlson*. *Carlson* is solely concerned with the lack of security in any short-range wireless communication concerning sensitive financial information. *Carlson*, 2:10-18. *Carlson* proposes the use of a “pseudo primary account identifier” (PPAI) to overcome the deficiencies of all other security measures. *Carlson* 2:63-66, 3:3-22, 4:26-38, 5:19-29. In *Carlson*’s view, biometrics would not improve the security of the account number once it is in transmission, which is the goal of *Carlson*. Thus, a POSITA would not have been motivated to combine the secure authentication process of *Jazayeri* with *Carlson* at

the point of unlocking the device. Indeed, additional security would have undercut the usability of *Carlson*, further undercutting the motivation provided by Mr. Lipoff.

2. *Carlson in View of Murakami Would Not Have Rendered Obvious “determining” “a value of the parameter that is sensed” (Grounds 4-6).*

98. Claim limitations 1[b], 6[b], and 11[b] state “determining . . . a value of the parameter that is sensed.” Claim limitation 14[b] similarly states “determining a value that is associated with the parameter that is sensed.” In Grounds 4–6, Mr. Lipoff replaces *Holloway*’s biometric sensor and *Jazayeri*’s authentication process with “*Murakami*’s biometric sensor and authentication process.” Ex. 1003, ¶214.¹¹ I disagree that a POSITA would have been motivated to implement *Murakami*’s biometric sensor and authentication process to unlock *Carlson*’s device.

¹¹ Mr. Lipoff relies on *Jazayeri* in Grounds 5 and 6 only “for the purpose of alternatively mapping an additional biometric authentication step prior to conducting the financial transaction or establishing a wireless link for Claims 4, 9, 11, 14, and 17-18.” Nowhere does Mr. Lipoff describe “an additional biometric authentication step” or “establishing a wireless link” for any limitation of claims 11 or 14. Indeed, Mr. Lipoff never mentions “an additional biometric authentication step” in this declaration. *See generally* Ex. 1003. Mr. Lipoff therefore does not rely on *Jazayeri* for at least claim limitations 1[b], 6[b], 11[b], and 14[b] in Grounds 4-6.

99. Mr. Lipoff states that “*Carlson* modified to unlock its device pursuant to the biometric authentication process described by *Murakami* teaches the claimed limitation of a parameter comprising a heart rate and/or a physiological state.” Ex. 1003, ¶218. Mr. Lipoff relies on *Murakami*’s sensor “used to measure a heartbeat waveform, a dynamic variable determined by measuring a user’s heartbeat.” Ex. 1003, ¶217 (citing *Murakami*, 32:30-33:6). Specifically, Mr. Lipoff relies on an embodiment wherein a waveform is measured, and “25 features are extracted out of a waveform to create a list of 25 parameters, each parameter requesting a different unique feature for a particular person’s heartbeat waveform.” *Murakami*, 23:20-22. *Murakami* teaches “tak[ing] more than one reading of the biometric for purposes of individualization.” *Murakami*, 32:31-33:1. “In one preferred embodiment 30 heartbeats were taken and monitored to do the individualization for each person being identified. In another preferred embodiment, a hundred heartbeats were used. In capturing a good sample, it is preferred to take as many samples as is possible.” *Murakami*, 33:1-4. *Murakami* even acknowledges that “taking a large number of sample waveforms takes time and using an extended period of time to individualize the waveform may be impractical.” *Murakami*, 33:4-6. As a result, a POSITA would have understood that *Murakami*’s biometric sensor provides updated security but at the expense of a significant amount of the user’s time. A POSITA would not have

been motivated to implement *Murakami*'s biometric sensor for functionalities, such as those disclosed in *Carlson*, which require little or no delay.

100. Specifically, a POSITA would not be motivated to implement *Murakami*'s biometric sensor for unlocking a consumer's wireless device because a consumer would not use a lock that takes 30–100 heartbeats to use. For example, such delay would be extremely disadvantageous in an emergency situation, where quick access to the device's functions are preferred. Indeed, *Murakami* expressly discloses that “[w]hen the signal is not valid, the biometrically activated switch will remain off or the device will remain disabled.” *Murakami*, 20:9-10.

101. Further, Mr. Lipoff identifies no disclosures in *Murakami* that resolve the issues a POSITA would have had combining *Carlson* and *Jazayeri*. Mr. Lipoff again alleges that *Carlson* “discloses a fingerprint authentication to unlock a wireless device and subsequent PIN authentication prior to performing transactions.” Ex. 1003, ¶219. Again, as discussed above, this misstates *Carlson*, which discusses, in its Background section, the use of PIN authentication as an inadequate security measure which “still does not resolve the situation where the sensitive information is intercepted while the user is making a legitimate purchase and has thus already entered the PIN.” *Carlson*, 2:46-48. This does not establish that a POSITA would have been motivated to combine *Carlson*'s device with the authentication or authorization disclosures of *Jazayeri* or the exceedingly complicated, time

consuming, and untemplated authentication procedures of *Murakami* such that *Carlson*'s device "determin[es]" "a value of the parameter that is sensed" and unlocks the device.

102. For at least these reasons, a POSITA would not have been motivated to use *Murakami*'s biometric sensor to unlock *Carlson*'s device. As such, Grounds 4-6 fail to disclose or render obvious "determining" "a value of the parameter that is sensed" of independent claims 1[b] 6[b], 11[b], and 14[b], and thus all dependent claims as well.

3. *Carlson's request for PPAI does not teach and would not have rendered obvious "requesting . . . from a second device an authorization to enable a function for conducting a financial transaction by the device" (Grounds 1-6).*

103. Dependent claim limitations 3[a] and 8[a] and independent claim limitations 11[d] and 14[d] state "requesting by the device from a second device an authorization to enable a function for conducting a financial transaction by the device." Claims 4, 5, 9, 10, 12, 13, 15, 16, 17, and 18 also include this limitation.

104. To meet this limitation, Mr. Lipoff states that "[b]ecause the financial transaction requires requesting and receiving the PPAI before the process may proceed for that particular transaction or a particular limited set of transactions, the PPAI is an authorization to perform that particular transaction or a particular limited set of transactions in *Carlson's* system." Ex. 1003, ¶120; *see also id.* at ¶133

(incorporating by reference analysis of limitation 3[a] for 8[a]), ¶167 (incorporating by reference analysis of limitation 3[a] for 11[d]), ¶179 (incorporating by reference analysis of limitation 3[a] for 14[d]) ¶¶212-213 (setting forth Mr. Lipoff’s opinion regarding grounds 4-6 utilizing *Murakami* and incorporating by reference all arguments and evidence from Grounds 1-3). Mr. Lipoff relies exclusively on *Carlson*’s request for PPAI as an alleged authorization for a particular transaction or particular limited set of transactions.¹² I disagree that *Carlson*’s PPAI is an authorization to perform a particular transaction or particular set of transactions for the following several reasons.¹³

105. *First*, the PPAI in *Carlson* is not “an authorization” to perform a transaction, as Mr. Lipoff alleges, nor would the disclosure of the request for PPAI have rendered this limitation obvious to a POSITA. *Carlson*’s request for PPAI is not a request for any type of authorization of a transaction as it is simply a request

¹² I understand Mr. Lipoff interprets the “authorization” of claims 3[a], 8[a], 11[d], and 14[d] to be an authorization for a particular transaction or particular set of transactions. Ex. 1003, ¶¶119-120 (Grounds 1-3); *see also* Ex. 1003, ¶212 (incorporating analysis of *Carlson* into Grounds 4-6).

¹³ Mr. Lipoff does not rely on *Holloway* or *Jazayeri* in Grounds 1-3 nor *Murakami* in grounds 4-6 for this part of the limitation.

for an identifier that is used as a proxy for the consumer's account identifier during a transaction. In fact, *Carlson* never describes or even suggests that the PPAI is an authorization to perform a transaction.

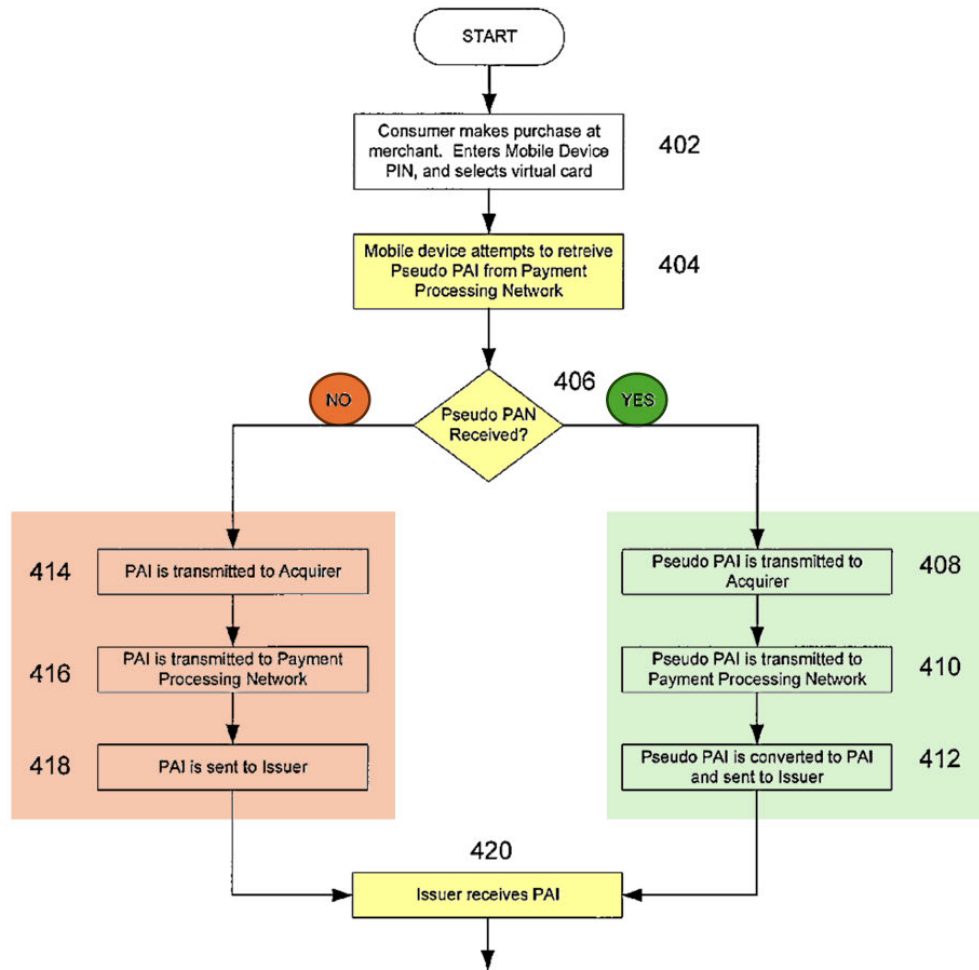
106. Instead, *Carlson* explains that the PPAI is used in a financial transaction instead of the user's real account identifier to protect the user from "[t]heft of sensitive information . . . using wireless interrogation or interception of communications from portable wireless device." *Carlson*, 2:7-10. According to *Carlson*, "[p]seudo primary account identifiers may include identifiers that are similar in format to a consumer's real account identifier." *Carlson*, 5:30-32. "These account identifiers may include account numbers or any other alphanumeric sequence." *Carlson*, 2:66-3:1. *Carlson* also describes the PPAI as "bogus, fake, decoy, substitute, or the like." *Carlson*, 5:42-43. Just like a real account number that can be denied by a merchant, the PPAI can likewise be denied when used during a particular transaction. As a result, the PPAI is not and cannot be "an authorization" to perform a transaction, as Mr. Lipoff alleges.

107. Mr. Lipoff relies on one embodiment in *Carlson* where the wireless device requests PPAI from the payment processing network. Ex. 1003, ¶119. Accordingly, Mr. Lipoff alleges that because *Carlson*'s financial transaction "***requires*** requesting and receiving the PPAI before the process may proceed" (*id.* (emphasis added)), then the PPAI is an authorization for a particular transaction. But

Mr. Lipoff is wrong. The mere fact that this embodiment discloses *requesting* the PPAI does not transform the PPAI into an authorization.

108. The purpose of requesting a PPAI in *Carlson* is so that *Carlson's* wireless device and the payment processing network can both associate the same PPAI with a user's real account information. *See Carlson*, 3:3-6 (“[T]he present invention provides a method for conducting a transaction that includes receiving a pseudo account identifier that corresponds to a consumer's account identifier.”), 6:48-50 (“The payment processing network can further store the pseudo primary account identifier's relationship to the primary account identifier.”), 7:21-24 (in embodiment where the wireless device generates the PPAI instead of receiving the PPAI, confirming that “[t]he payment processing network can send an acknowledgement to the portable wireless device indicating that the pseudo primary account identifier has been received.”). The user's authorized real account information is already on *Carlson's* wireless device at the time of requesting a PPAI. *Carlson*, 12:25-37 (“The user then may select which virtual card they wish to use to conduct the transaction 214. A virtual card corresponds to an account that the user has with an issuer and may be identified by the issuer through the use of a primary account identifier. . . . In this exemplary embodiment, the portable wireless device 202 may then request a pseudo primary account identifier that corresponds with a primary account identifier from the payment processing network 210.”). Indeed, a

financial transaction will proceed in *Carlson* regardless of whether a PPAI is received in response to a request for PPAI. For example, if a PPAI is not received in response to *Carlson*'s request for PPAI, the particular transaction will still proceed using, for example, the primary account identifier—because a PPAI is not a necessary part of any particular financial transaction. In *Carlson*'s Figure 4, if the PPAI is not received in response to the request for PPAI, the transaction continues with the user's real account identifier (orange, below), instead of proceeding with a received PPAI (green, below). *Carlson*, 14:24-33 (“If the portable wireless device fails to retrieve a pseudo primary account identifier at step 406 the process continues on to step 414 where the transaction proceeds using the primary account identifier.”).



Carlson, Fig. 4 (cropped and annotated).

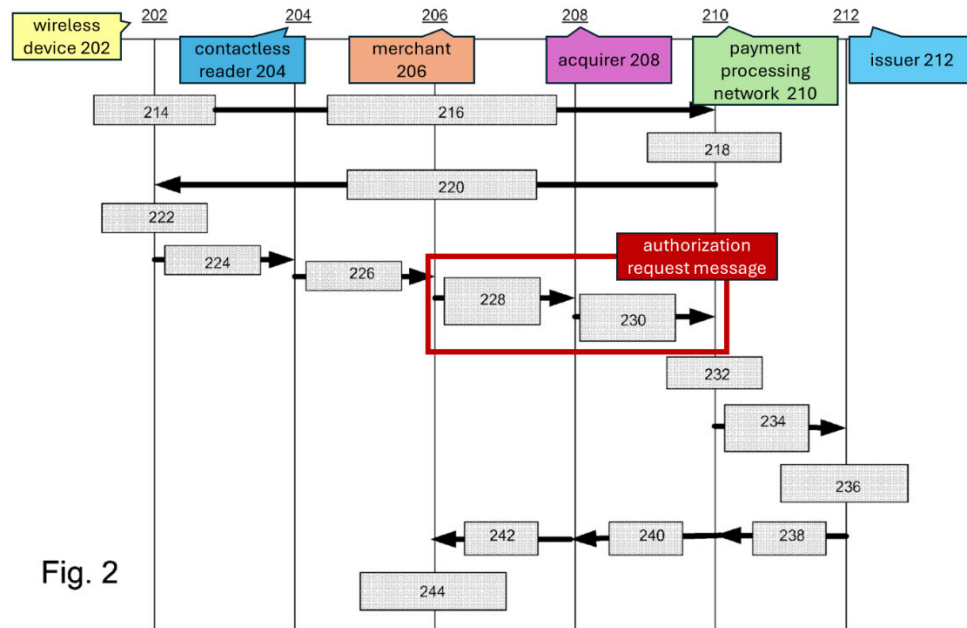
109. Additionally, *Carlson* is clear that the PPAI “*may not be requested at all.*” *Carlson*, 7:4 (emphasis added). This further undercuts Mr. Lipoff’s position that the request for PPAI is required for a particular transaction because there is no embodiment that *requires* a response to a request for PPAI. For example, the PPAI may be “pushed to the portable wireless device at any time, such as when the device is turned on, when the device is idle, periodically, or through any other such criteria.” *Carlson*, 7:4-7, 12:67-13:3. As another example, *Carlson* discloses that “[t]he

portable wireless device may generate the pseudo primary account identifier.” *Carlson*, 7:15-19. In embodiments where the PPAI is pushed or generated, the PPAI cannot act as an authorization for a particular transaction because the PPAI is unrelated to any particular transaction.

110. *Second*, *Carlson* itself undercuts Mr. Lipoff’s theory that PPAI is an authorization because *Carlson* discloses a different message, an “authorization request message,” as a function for requesting an authorization of a transaction and, thus, the authorization of a transaction is dependent on the “authorization request message” and not the call-and-response of an optional request for PPAI. As a result, a transaction authorization is agnostic to whether the PPAI is received, or if the PPAI request is even made. *Carlson* discloses, “[a]fter receiving the pseudo primary account identifier from the contactless device, the merchant may then use that identifier, as well as additional information to form an authorization request message.” *Carlson*, 8:10-13. “An authorization request message can include a request for authorization to conduct an electronic payment transaction or some other type of activity.” *Carlson*, 8:13-15. “The payment processing network may then process the authorization message and return a response that indicates if the transaction is authorized or not.” *Carlson*, Abstract. As a result, it is the “authorization request message” sent by the merchant, not the request for PPAI sent by *Carlson*’s device, that drives authorization in the *Carlson* system.

111. Even if Mr. Lipoff had identified *Carlson*'s "authorization request message" instead of *Carlson*'s request for PPAI as the claimed "authorization," the mapping would still fail. The claims require "requesting *by the device*" or "requesting *by the wireless device*." Ex. 1001, cls. 3, 8, 11 (emphasis added); *see also id.* cl. 14 (claiming "[a] wireless device that is configured to perform operations comprising" the request for authorization). Because *Carlson*'s "authorization request message" is sent by the merchant, the "authorization request message" cannot be the claimed "request[]" for "authorizaiton." *Carlson* explains that the "authorization request message" is sent by the merchant—not by *Carlson*'s device—over a different network than the one used by *Carlson*'s device to request a PPAI. According to *Carlson*, "[t]he pseudo primary account identifier can then be included in an authorization request message 228 that is sent to an acquirer 208" by the **merchant 206**. *Carlson*, 13:18-20. *Carlson* explains that "messages that are sent between the merchant 206, the acquirer 208, and the payment processing network 210, are typically sent over a restricted access network that is separate from the communications channel used to request the [PPAI]." *Carlson*, 13:23-27. Indeed, *Carlson* teaches that having the merchant send the "authorization request message" is an advantage: "[S]ince a [PPAI] is sent over a different communication network than the network that is used to conduct the authorization for the transaction, the merchant never receives the actual account identifier." *Carlson*, 15:50-53; *see also*

Carlson, 11:17-34, Fig. 1 (explaining the need for two separate networks). *Carlson* warns of “fraudulent merchants” who may try to steal real account identifiers. *Carlson*, 15:53-56.



Carlson, Fig. 2 (annotated).

112. Having the “authorization request message” sent by the merchant instead of by *Carlson*’s device is also consistent with *Carlson*’s Figure 4, which shows an authorization step (purple, below) separate from *Carlson*’s device requesting and potentially receiving the PPAI (yellow, below).¹⁴

¹⁴ Notably, Mr. Lipoff excerpts Figure 4 in his declaration and excludes the authorization step in purple below. Ex. 1003, ¶122; *but see* Ex. 1003, ¶154 (annotating Figure 4 and highlighting the authorization step).

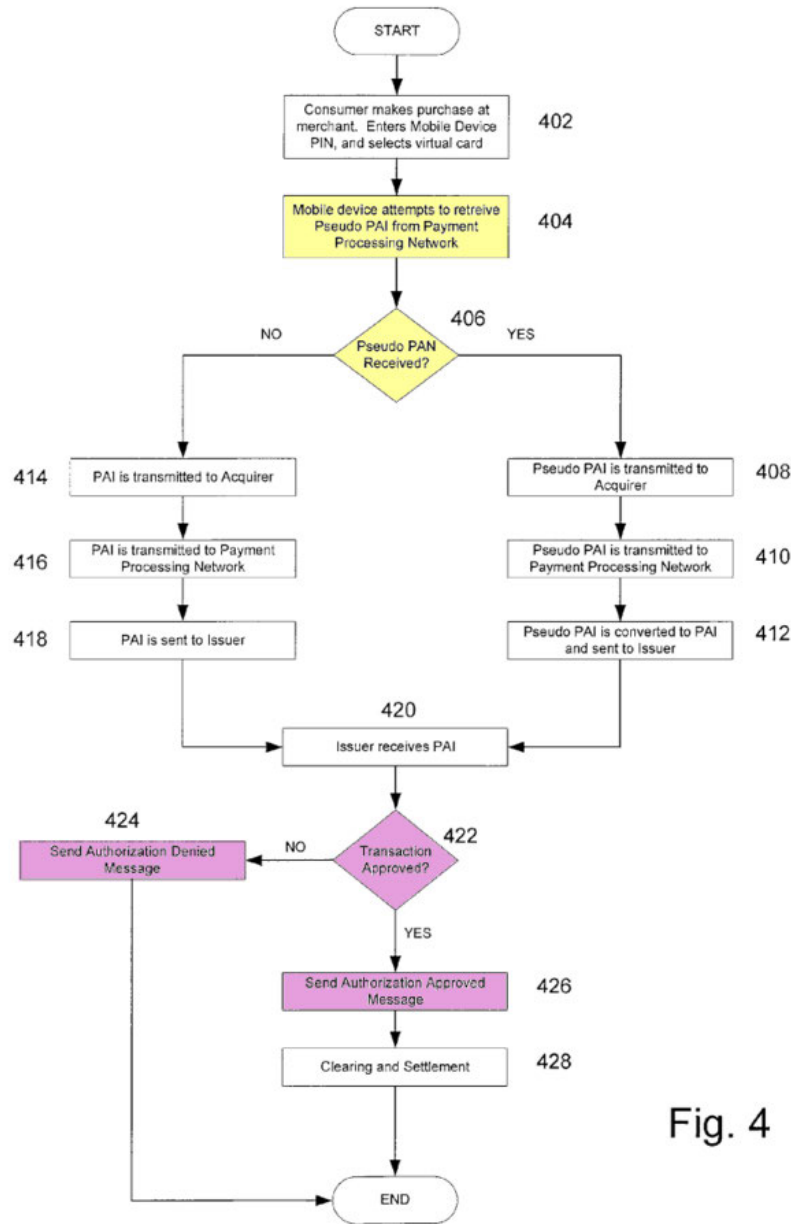


Fig. 4

Carlson, Fig. 4 (annotated). *Carlson* then discloses that “the issuer receives the transaction request that contains the primary account identifier,” and that “[u]sing any number of criteria, such as the account specified by the primary account identifier being in good standing, having sufficient funds available, having sufficient

credit available, etc., the issuer makes a decision at step 422 to either approve or deny the transaction.” *Carlson*, 14:34-40.

113. Mr Lippoff appears to appreciate that *Carlson* does not require receiving a PPAI to conduct a financial transaction. Instead, Mr. Lipoff addresses this major shortcoming in *Carlson* in a footnote. Mr. Lipoff states that, because “[t]he proposed grounds rely on the PPAI-based financial transaction,” then “in the context of the proposed grounds, [the failure to receive the PPAI] serves as an indication that the function to conduct the PPAI-based financial transaction has not been established.” Ex. 1003, ¶122, n. 6. Mr. Lipoff then states that, “[w]hile it may still be possible in *Carlson*’s system to conduct a different financial transaction (e.g., a less secure process that uses a PAN, rather than PPAI), the [PPAI-based] function relied upon in the Proposed Grounds is not established absent a PPAI.” *Id.* I disagree. Mr. Lipoff invents these two distinct secure and less secure transactions. *Carlson* contemplates one exchange—one where, regardless of whether a PPAI is received in response to a request for the PPAI or not, the exact same financial account is debited for the exact same amount for the exact same purchase. *Carlson*, 14:34-46 (referring to Figure 4, regardless of whether a PPAI is received, “settlement and clearing processes occur at step 428 to actually transfer funds from the account held at the issuer to the merchant”). Further, Mr. Lipoff continues to fail to appreciate that a PPAI-based financial transaction is still possible in *Carlson* without a response

to a request for PPAI.¹⁵ Because a PPAI-based financial transaction is still possible in *Carlson*, a PPAI is not an authorization to perform a PPAI-based financial transaction.

114. Even if Mr. Lipoff was correct that *Carlson* could be limited to a PPAI-based transaction, as described above, it is not true that a PPAI-based transaction requires requesting and receiving a PPAI before a PPAI-based transaction may proceed. For example, the particular transaction may still (1) go forward without a response to a request for PPAI, as set forth in Figure 4; or (2) go forward without any request, either because the PPAI was (i) pushed to the device independent of any request (*Carlson*, 7:3-15, 12:67-13:3) or (ii) generated by the device itself (*Carlson*, 7:16-19). There is no embodiment disclosed in *Carlson* where the “particular transaction or particular limited set of transactions” “requires requesting and receiving the PPAI” as Mr. Lipoff suggests. The PPAI therefore does not disclose “an authorization” to perform a particular financial transaction.

115. Additionally, a specific PPAI-based transaction may be authorized or unauthorized regardless of any use of the PPAI because *Carlson*’s “authorization request message”—sent by the merchant—is the functionality that actually

¹⁵ Mr. Lipoff’s error stems from his incorrect belief that the PPAI is required to be requested in *Carlson*’s system.

authorizes a particular transaction. *Carlson*, 13:18-20. *Carlson* explains that authorization for a particular transaction in response to the “authorization request message” can be based on whether “the consumer conducting the transaction has sufficient funds or credit to conduct the transaction.” *Carlson*, 9:11-25. Thus, a POSITA would not have understood *Carlson*’s PPAI to be “an authorization.”

116. Therefore, both *Carlson* in view of *Holloway* and/or *Jazayeri* and *Carlson* in view of *Murakami* and/or *Jazayeri* fail to disclose or render obvious “requesting . . . from a second device an authorization to enable a function for conducting a financial transaction by the device” of independent claims 11 and 14 and dependent claims 3 and 8, and thus all claims that depend therefrom as well.

117. For at least these reasons, *Carlson* does not disclose this claim limitation.

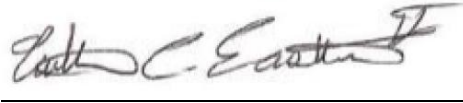
XIII. SUMMARY AND OTHER REMARKS

118. It is my opinion that Petitioner has failed to show that any of the Challenged Claims set forth in Grounds 1-6 are unpatentable as obvious as explained above.

119. My opinions expressed in this Declaration are based on the information available to me at this time. To the extent that any additional information becomes available, I reserve the right to supplement any opinions contained herein.

I hereby declare that all statements made herein of 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 by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on November 7, 2025.

A handwritten signature in dark ink, appearing to read "William C. Easttom II", written over a horizontal line.

William C. Easttom II (Chuck Easttom)