

**IN THE UNITED STATES PATENT AND
TRADEMARK OFFICE**

**BEFORE THE PATENT TRIAL AND APPEAL
BOARD**

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

U.S. Patent No. 10,810,579
Issued: October 20, 2020

Title: SMART TOKENIZING PAYMENT
CARD AND DEVICE AND TRANSACTION
PROCESSING THEREOF, SYSTEM AND
METHOD

DECLARATION OF MICHAEL I. SHAMOS, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION AND QUALIFICATIONS	1
II. SUMMARY OF MY OPINIONS.....	4
III. UNDERSTANDING OF THE GOVERNING LAW	5
A. Invalidity By Obviousness.....	5
B. Relevant Time Period for the Obviousness Analysis	8
C. Materials Considered	9
IV. OVERVIEW OF THE '579 PATENT.....	9
V. THE '579 PROSECUTION HISTORY	11
VI. LEVEL OF ORDINARY SKILL IN THE ART IN THE RELEVANT TIMEFRAME	12
VII. TECHNOLOGY BACKGROUND	14
A. Cryptographic Hashing.....	15
B. Near-Field Communication (NFC) Interfaces.....	16
C. Touch Screen Displays	18
D. Static and Limited-Use Numbers	19
E. Sequence Counters.....	22
VIII. CLAIM CONSTRUCTION.....	23
IX. OVERVIEW OF PRIOR ART REFERENCES	23
A. U.S. Patent Application Publication 2010/0185545 (“Royyuru”)	23
B. U.S. Patent Application Publication 2012/0310760 (“Phillips”)	26
C. U.S. Patent 8,255,323 (“Casey”)	28
D. U.S. Patent Application Publication 2008/0172317 (“Deibert”)	30
E. U.S. Patent 8,423,462 (“Amacker”)	31
F. U.S. Patent 9,600,808 (“Gomez”)	34
G. U.S. Patent Application Publication 2008/0319905 (“Carlson”)	37
H. U.S. Patent Application Publication 2012/0123937 (“Spodak”)	39

TABLE OF CONTENTS

(continued)

	Page
I. U.S. Patent Application Publication 2013/0036050 (“Giordano”)	42
J. U.S. Patent 8,052,052 (“Power”).....	45
X. THE CHALLENGED CLAIMS ARE INVALID	47
A. Ground 1A: Claims 1, 2, 4, 6-9, 11-12, and 15-23 of the ’579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips and Casey	47
1. Motivation to Combine Royyuru with Phillips and Casey	47
2. Claim 1	55
3. Claim 2	64
4. Claim 4	65
5. Claim 6	68
6. Claim 7	70
7. Claim 8	71
8. Claim 9	72
9. Claim 11	75
10. Claim 12	79
11. Claim 15	80
12. Claim 16	85
13. Claim 17	86
14. Claim 18	87
15. Claim 19	89
16. Claim 20	95
17. Claim 21	96
18. Claim 22	99
19. Claim 23	101
B. Ground 1B: Claim 3 of the ’579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, and Spodak	102

TABLE OF CONTENTS
(continued)

	Page
1. Claim 3	102
C. Ground 1C: Claim 5 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, Spodak, and Giordano	107
1. Claim 5	107
D. Ground 1D: Claims 10 and 14 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, and Deibert	110
1. Motivation to Combine Deibert with the Combination of Royyuru, Phillips, and Casey	110
2. Claim 10	112
3. Claim 14	113
E. Ground 1E: Claim 13 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, Deibert, and Power	115
1. Motivation to Combine Power with the Combination of Royyuru, Phillips, Casey, and Deibert	116
2. Claim 13	117
F. Ground 1F: Claims 4, 21 and 22 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey and Carlson.....	120
1. Motivation to Combine Carlson with the Combination of Royyuru, Phillips, and Casey	120
2. Claims 4, 21, and 22	122
G. Ground 2A: Claims 1-9, 11-12, 15-20, and 22-23 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker and Spodak.....	124
1. Motivation to Combine Gomez, Amacker, and Spodak	124
2. Claim 1	132
3. Claim 2	142

TABLE OF CONTENTS
(continued)

		Page
4.	Claim 3	143
5.	Claim 4	149
6.	Claim 5	151
7.	Claim 6	153
8.	Claim 7	155
9.	Claim 8	156
10.	Claim 9	157
11.	Claim 11	160
12.	Claim 12	161
13.	Claim 15	162
14.	Claim 16	167
15.	Claim 17	168
16.	Claim 18	169
17.	Claim 19	170
18.	Claim 20	175
19.	Claim 22	176
20.	Claim 23	178
H.	Ground 2B: Claims 10 and 14 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Spodak, and Deibert.....	179
1.	Motivation to Combine Gomez, Amacker, Spodak, and Deibert	179
2.	Claim 10	180
3.	Claim 14	182
I.	Ground 2C: Claim 13 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Spodak, Deibert, and Power	185

TABLE OF CONTENTS
(continued)

	Page
1. Motivation to Combine Power with the Combination of Gomez, Amacker, Spodak, and Deibert.....	185
2. Claim 13	187
J. Ground 2D: Claims 4 and 22 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Spodak, and Carlson	190
1. Motivation to Combine Carlson with Gomez, Amacker, and Spodak	190
2. Claim 4	191
3. Claim 22	192
K. Ground 2E: Claim 21 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker Spodak, Carlson, and Royyuru	193
1. Motivation to Combine Royyuru with Gomez, Amacker, Spodak, and Carlson.....	193
2. Claim 21	195
XI. JURAT	196

I, Dr. Michael I Shamos, hereby declare as follows:

I. INTRODUCTION AND QUALIFICATIONS

1. I have been retained by Google LLC (“Google”) to provide my opinions concerning the validity of claims 1-23 (“Challenged Claims”), constituting all claims of U.S. Patent No. 10,810,579 (“’579 Patent” or the “Patent”) in support of Google’s Petition for *Inter Partes* Review of the Patent (the “Petition”).

2. I am being compensated at a rate of \$625 per hour for my work in this proceeding and my compensation is in no way contingent on the nature of my findings, the presentation of my finding in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding or in Patent Owner. It is conceivable that I may own investments in mutual funds which themselves own shares in Patent Owner. I have no knowledge of any such holder, which, in any event, would not constitute a material portion of my net worth.

3. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities, is contained in my curriculum vitae, a copy of which is provided as Exhibit 1014. Below is a short summary of my professional qualifications.

4. I have a A.B. degree from Princeton University in Physics (1968), a M.A. degree from Vassar College in Physics (1970), a M.S. degree from American

University in Technology of Management (1972), a M.S. degree from Yale University in Computer Science (1973), a M. Phil. from Yale University in Computer Science (1974), a Ph.D. from Yale University in Computer Science (1978), and a J.D. degree from Duquesne University (1981).

5. I currently hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I am a member of two departments in that School, the Institute for Software Research and the Language Technologies Institute. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 was Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. Since 2018, I have been Director of the M.S. in Artificial Intelligence and Innovation degree program at Carnegie Mellon.

6. I have taught graduate courses at Carnegie Mellon in Electronic Commerce from 1999-present, including eCommerce Technology, Electronic Payment Systems, Electronic Voting, Internet of Things, Ubiquitous Computing, Electronic Payment Systems and eCommerce Law and Regulation, as well as Analysis of Algorithms. Since 2007, I have taught an annual course in Law of Computer Technology. I currently also teach Artificial Intelligence and Future Markets.

7. From 2001-2021, I was a Visiting Professor at the University of Hong Kong, where I taught an annual course in Electronic Payment Systems. This was one of only a handful of graduate courses taught on this subject in the world.

8. I was the Director of Carnegie Mellon's graduate degree program in eBusiness Technology from 1999-2018 and am now a faculty member in the Privacy Engineering degree program at Carnegie Mellon. My course on Law of Computer Technology is required for all students in that program and in the Societal Computing Ph.D. program. My principal role currently is as Director of the graduate program in Artificial Intelligence and Innovation.

9. From 1979-1987 I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

10. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981. I have been asked to render opinions in this Declaration as a technical expert. I have not been asked to offer any opinions on patent law in this proceeding.

11. I am a named co-inventor on the following six issued patents relating to electronic commerce: U.S. Patent Nos. 7,330,839, 7,421,278, 7,747,465, 8,195,197, 8,280,773, and 9,456,299.

12. I have previously served as an expert in over 400 cases concerning computer technology. In particular, I have been involved in more than 45 cases involving electronic payment systems.

13. The statements made and opinions provided in this Declaration are based on my own personal knowledge and, if called as a witness, I could and would testify in a manner consistent with this Declaration.

II. SUMMARY OF MY OPINIONS

14. It is my understanding that the following table summarizes the grounds of challenge (“Grounds”) raised in the Petition:

15. Ground 1A: Claims 1, 2, 4, 6-9, 11-12, and 15-23 are unpatentable under 35 U.S.C. §103 as being obvious in view of Royyuru (EX1004), Phillips (EX1005), and Casey (EX1006).

16. Ground 1B: Claim 3 is unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, and Spodak (EX1009).

17. Ground 1C: Claim 5 is unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, Spodak, and Giordano (EX1010).

18. Ground 1D: Claims 10 and 14 are unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, and Deibert (EX1012).

19. Ground 1E: Claim 13 is unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, Deibert, and Power (EX1016).

20. Ground 1F: Claims 4, 21, and 22 are unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, and Carlson (EX1013).

21. Ground 2A: Claims 1-9, 11-12, 15-20, and 22-23 are unpatentable under §103 as being obvious in view of Gomez (EX1007), Amacker (EX1008), and Spodak.

22. Ground 2B: Claims 10 and 14 are unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, and Deibert.

23. Ground 2C: Claim 13 is unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, and Power.

24. Ground 2D: Claims 4 and 22 are unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, and Carlson.

25. Ground 2E: Claim 21 is unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, Carlson, and Royyuru.

26. After a review of the '579 Patent and the prior art asserted by Petitioner, it is my opinion that the Challenged Claims are invalid for obviousness. My opinions, and the bases therefor, are detailed throughout this Declaration.

III. UNDERSTANDING OF THE GOVERNING LAW

A. Invalidity By Obviousness

27. I understand that obviousness of a claim requires that the claim as a whole be obvious from the perspective of a person of ordinary skill in the relevant

art (“POSITA”), at the time of invention. A claim is unpatentable for obviousness under 35 U.S.C. § 103 “if the differences between the subject matter sought to be patented 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 said subject matter pertains.” Obviousness may be based upon a combination of references.

28. If a patented invention is a combination of known elements, there must be some 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 POSITA. Identifying a reason the elements should be combined is 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, was already known. The prior art references themselves may provide a suggestion, motivation, or reason to combine, but the nexus linking two or more prior art references is sometimes simple common sense.

29. An obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) any objective

indicia of non-obviousness, such as commercial success, long-felt but unresolved need, failure of others, industry recognition, copying, and unexpected results.

30. 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 their skill.

31. Practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. A POSITA looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. An obviousness analysis therefore considers the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

32. A proper obviousness analysis focuses on what was known or obvious to a POSITA at the time of invention, not to the patentee. Accordingly, 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.

33. Prior art teachings are properly combined if 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.

34. I understand that 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.” 35 U.S.C. §316(e).

B. Relevant Time Period for the Obviousness Analysis

35. I understand that the ’579 Patent claims priority to U.S. Provisional Patent Application 61/794,891 (“’891 Provisional”), filed on March 15, 2013. I have been asked, for purposes of this proceeding only, to treat March 15, 2013 as the Critical Date in my analysis. However, my opinions as to the obviousness of claims 1-23 of the ’579 Patent would remain substantially unchanged even if a later date were deemed to be the Critical Date and if post-AIA §§ 102 and 103 were to apply. I understand that Petitioner does not concede that any of the Challenged Claims enjoy priority to the ’891 Provisional. However, I have been asked to assume, for purposes of this proceeding only, that pre-AIA 35 U.S. §§ 102 and 103 apply.

36. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the ’579 Patent. Unless otherwise stated, my testimony below refers to the knowledge of a POSITA as of the Critical Date, or before. Any annotated Figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the ’579 Patent and the prior art discussed below.

C. Materials Considered

37. In forming my opinions, I have reviewed and am familiar with the '579 Patent and its prosecution history, the materials cited herein, and exhibits to the Petition.

IV. OVERVIEW OF THE '579 PATENT

38. The '579 Patent was filed on July 1, 2019 and issued on October 20, 2020. Through a series of continuation and divisional applications and a provisional application, it claims priority to March 15, 2013. The '579 Patent discloses “a credit card device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card.” EX1001, Abstract. However, the Challenged Claims are not drawn to any such device, and do not claim “generating a programmed magnetic field” or any “emulation” of a “standard credit card.”

39. The '579 Patent discloses generating a “limited-duration number” for use in a payment transaction. EX1001, 2:23-28, 2:48-61, 10:4-11:55, FIG 7.

40. The claims recite, at times, a “limited-use number,” which can take the form of a “limited-duration number” by being limited by time or number of transactions in which it may be used or may be limited in use in other manners, such as limited in use to specific transactions or use by a specific device. FIG. 7 of the Patent is a flowchart illustrating an example process for generating a limited-use number:

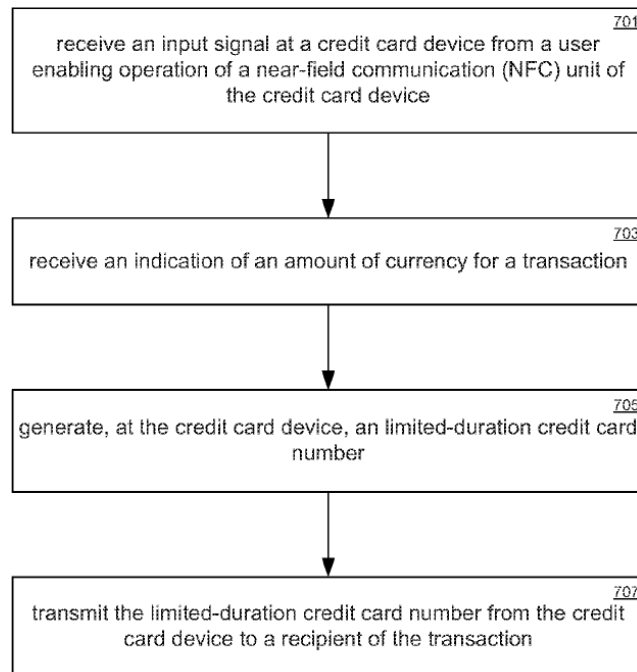


FIG. 7

EX1001, FIG. 7

41. Various other portions of the specification of the Patent (“Specification”) give further details of the generation of a limited-use number. For example, “[t]he credit card device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction.” EX1001, 10:7-9. “The power source is able to activate the processor unit such that a unique number may be generated by the credit card device and verified by the credit authority according to the timestamp and the transmitted user information.” *Id.*, 10:9-13. “The limited duration credit card number is able to be produced at the time the credit card device is performing a transaction, and is able to be generated according to the user’s private information, a bank information, information regarding the facility performing the transaction, and the time of day.” *Id.*, 10:13-18. Further, the “limited-

duration credit card number is able to be limited to only one transaction, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid.” *Id.*, 10:18-23.

42. The Specification further explains how “the number on the front of the card” can be static, dynamic, or a combination of static and dynamic digits. *Id.*, 10:32-52. “For example, the first four and last four digits of the credit card number are able to be fixed, while the remaining eight digits can be dynamically generated.” *Id.*, 10:37-41.

V. THE ’579 PROSECUTION HISTORY

43. I have reviewed the prosecution history of the ’579 Patent (EX1002). On July 1, 2019, Applicant filed continuation application 16/459,150, which became the ’579 Patent. EX1002, 218. Prosecution was brief. In a first office action dated May 8, 2020, the Examiner allowed claims 1-14 and 20-24, rejected claims 15-18 as anticipated by Brudnicki et al. (US 2013/0159186), and objected to claim 19 as depending on a rejected base claim. *Id.*, 112-116.

44. In response, Applicant amended claim 15 to add additional limitations and canceled claim 19. *Id.*, 97-108.

45. A Notice of Allowance was mailed June 30, 2020. Claims 1-18 and 20-24 were allowed. *Id.*, 65-71. Issued claims 1-18 correspond to original claim claims 1-18. Issued claims 19-23 correspond to original claims 20-24. *Id.*, 77.

46. The Notice of Allowance stated:

None of prior art teaches a method of performing a transaction comprising receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises a near field communications (NFC) interface coupled to the processor, receiving a request for a transaction payment at the electronic device via the NFC interface, generating, by the processor, a limited-use payment information, and using the limited-use payment information in place of the card issuer supplied payment information, transmitting the limited-use payment information from the electronic device to an NFC recipient of the transaction via the NFC interface, and visually conveying a status of the transaction via a user-interface displayed on the touch-screen display, and obtaining a user payment approval through at least one user-interface of the electronic device as set forth in the claims.

Id., 70.

47. More than three months after the Notice of Allowance, Applicant filed its first and only IDS, and there is no indication that any of the art cited in the IDS was considered by the Examiner. The face of the Patent lists only three references, all found by the Examiner.

48. None of the prior art cited in the Petition was considered by the Examiner. None of the prior art cited in the Petition was listed in any IDS.

VI. LEVEL OF ORDINARY SKILL IN THE ART IN THE RELEVANT TIMEFRAME

49. The '579 Patent defines its field of invention as follows:

Embodiments according to the present disclosure generally relate to multi-function electronic devices or smart cards and, more particularly, to systems and methods of smart tokenizing payment cards and devices and transaction processing thereof.

EX1001, 1:23-27.

50. The '579 Specification asserts a need for security in credit cards that employ RFID technology:

A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

A concern with each of these types of credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise. Therefore, these types of credit cards have security limitations. Further, cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.

EX1001, 1:55-2:3

51. The Specification describes generating limited-use credit card numbers and using them to engage in secure payment transactions, including the use of cryptograph hash algorithms.

52. The claims of the '579 Patent are directed to devices and methods for communicating payment information using limited-use numbers.

53. In my opinion, in order to understand the Specification and make and use the claimed invention without undue experimentation at or near the Critical Date, one of ordinary skill in the art of the '579 Patent would have been someone with (1) a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and; (2) in addition, one to two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technologies such as RFID technology. Graduate education could substitute for professional experience, or significant experience in the field could substitute for education.

54. I qualify as at least a POSITA as of March 15, 2013, and I have a sufficient level of knowledge, experience and education to provide an opinion in the field of the '579 Patent. I am familiar with what a person of ordinary skill in the art knew in 2013 because of my lengthy experience with subjects similar to those of the concepts presented in the '579 Patent. In addition, I was teaching such subjects prior to 2013.

VII. TECHNOLOGY BACKGROUND

55. In this section, I discuss the state of the art as of the Critical Date with respect to certain technologies relevant to the subject matter of the '579 Patent.

56. The art of credit card payments is extremely crowded and extensive. Prior to the Critical Date, over 50,000 U.S. patent applications and issued U.S. patents had been published containing the strings "credit card" and "payment."

Furthermore, major credit-card networks, such as Visa, MasterCard, Europay and EMV (“Europay-MasterCard-Visa”) had collaborated to develop industry-wide standards for credit card processing. Such standardization was necessary to enable the use of cards at tens of millions of merchants around the world, given that many different types of point-of-sale (POS) terminals were in use at various establishments. These standards set forth requirements for equipment and software used to process card payments.

57. One major standardization effort was undertaken by the Payment Card Industry (PCI), an association of organizations that store, process and transmit cardholder data. In 2006, American Express, Discover Financial Services, Japan Credit Bureau, MasterCard and Visa International formed the Payment Card Industry Security Standards Council (PCI SSC) which, by 2014, included 688 “participating organizations.” PCI SSC issued a series of published security standards. As of the Critical Date, Version 2.0 of the PCI security standards were in effect, as described in “PCI Data Security Standard (PCI DSS) Version 2.0 January 2013,” (EX1022) and “Payment Card Industry (PCI) Data Security Standard Navigating PCI DSS Version 2.0 October 2010.” (EX1026)

A. Cryptographic Hashing

58. The PCI Standards describe the requirement of cryptographic hashing of card numbers. For example:

Protect Cardholder

Data Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

EX1026, 20.

59. A POSITA familiar with payment processing would have been familiar with these standards.

B. Near-Field Communication (NFC) Interfaces

60. A fundamental problem in electronic payments is how to communicate digital information, such as a credit card number, from the card itself or another device held by the user, to a POS device operated by a merchant. An early method was to provide the card with a magnetic stripe with encoded data including the credit card number. The user or merchant would then “swipe” the card through a magnetic reader of the POS device.

61. A later method was to build a processor chip into the card. The user or merchant would insert the card into a slot in the POS device, where electrical contact would be made with the chip, and payment data, including a credit card number, would be sent to the POS device.

62. A third method was to provide the card with a radio frequency identification (RFID) chip so that it could communicate wirelessly. The user would bring the card close to the POS device, and card information would be transmitted by radio waves over the very short distance between the card and the POS device. The '579 Patent uses the terms “radio frequency identification,” “RFID,” “near-field communication” and “NFC” interchangeably. It acknowledges that RFID credit cards were “in circulation”:

A different type of credit card device in circulation employs radio frequency identification (“RFID”). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

EX1001, 1:55-61.

63. Indeed, NFC credit cards were well-known in the industry. I personally was teaching about RFID credit cards in my Electronic Payment Systems course as early as 2002. A 2009 paper by Kadambi et al., “Near-Field Communication-Based Secure Mobile Payment Service,” was published by the Association of Computing Machinery in the Proceedings of the 11th International Conference on Electronic Commerce in August 2009 (“Kadambi,” EX1025). Kadambi notes that:

Unfortunately, innovating in the Point of Sale (PoS) space is hard because the protocols have been standardized, tightly constraining new ideas. Using mobile phones as payment devices opens up some opportunities, but any solution must minimize changes in the back-end processing. This paper describes a Near

Field Communication (NFC) based mobile phone payment solution in a service-oriented environment, which provides the needed data protection without requiring costly changes to the payment processing infrastructure.

EX1025, Abstract.

64. I note that Kadambi discloses a mobile phone used as an NFC payment device.

C. Touch Screen Displays

65. The '579 Patent apparently uses the terms “touch screen” and “touch sensor array” synonymously:

A user input may be made via the touch sensor array 245, which may comprise a touch screen panel, a keypad, or a combination thereof.

EX1001, 6:31-33.

66. Mobile phones have had touchscreens for display since at least 1992, with the introduction of the IBM Simon. EX1031, 2-3. More recently, the Apple iPhone 1 in 2007 had a touchscreen. *Id.*

67. It was somewhat later that cards had touch screens, although they had them prior to the critical date. On November 9, 2012, the Sydney Morning Herald, an Australian newspaper, published an article entitled, “New credit card has LCD screen, touch-sensitive buttons” (EX1029). It states:

MasterCard is billing a new credit card it is issuing in Singapore as the “next generation of payment cards.”

With security in mind, the Display Card has an LCD screen and touch-sensitive buttons that let the user employ a one-time password (OTP). Such OTPs are often delivered via text messages or chip-based authentication devices.

The card is designed for “banking institutions that necessitate a higher level of security for their online banking services require the use of a separate authentication token or device,” according to a press release from MasterCard.

EX1029, 1-2.

68. The photo below is from the same article:



Id., 1.

D. Static and Limited-Use Numbers

69. The use of a surrogate or “token” in place of an actual credit card number was a well-known security practice long before the Critical Date. It was long known that fraud can occur if an unauthorized party obtains a user’s credit card number. Unfortunately, in older credit card transactions, there was no way to prevent the merchant itself from obtaining the user’s credit card number, as the merchant had to present that number to a credit card network in order to be paid.

70. In 2001, the idea of token was introduced by the company TrustCommerce, which replaced the primary account number (PAN) with a randomized number, called a token. When a merchant needed to process a payment, it could use the token and TrustCommerce would process the payment on their behalf, replacing it with the true credit card number before introducing the transaction into the credit card network. In this manner, the merchant never learns the user's credit card number.

71. Tokenization was adopted by PCI, which established a Tokenization Taskforce. In August 2011, it published "PCI DSS Tokenization Guidelines" (EX1030) to supplement Version 2.0 of the PCI Data Security Standard. It explains different ways of generating tokens, stating:

One of the primary goals of a tokenization solution should be to replace sensitive PAN values with non-sensitive token values. For a token to be considered non-sensitive, and thus not require any security or protection, the token must have no value to an attacker. Tokens come in many sizes and formats. Examples of some common token formats are included in the following table.

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwI5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

** Note: This table provides a selection of examples only, and does not include all possible token formats.*

EX1030, 5.

72. The Tokenization Guidelines go on to explain the difference between single-use and multi-use tokens:

Tokens can be generally identified as either single-use or multi-use. A single-use token is typically used to represent a specific, single transaction. A multi-use token represents a specific PAN, and may be used to track an individual PAN across multiple transactions. A multi-use token always maps a particular PAN value to the same token value within the tokenization system. Determining whether single-use or multi-use tokens, or a combination of both, are appropriate for a particular merchant environment will depend on the merchant's specific business need for retaining tokens.

Id.

73. I note that the last row of the table above shows generating a token by taking a portion of the credit card number (PAN) to yield a truncated PAN and replacing the middle digits with “alphabetic and numeric characters.”

E. Sequence Counters

74. The '579 Patent claims a “device transaction sequence counter” (claims 2, 3, 5), “transaction sequence count information” (claim 6), and a “sequence counter” (claim 23). None of these are described, or even mentioned, in the Specification and all were added through amendment during prosecution.

75. There is disclosure of a “transaction count,” however:

As detailed above, if an expired limited-duration credit card is attempted to be used for a transaction, the transaction is denied and an automatic notification is able to be made to a credit authority in order to notify the user and to prevent transactions on the account. The transaction count is able to be determined through the action of passing the card through magnetic reader, and the process of transmitting said card number to said card reader.

EX1001, 10:23-31.

76. It appears from the Specification that the “transaction count” is to be used to determine whether the card has been used a given number of times, after which it can no longer be used. The term “transaction count” is not used in any of the claims.

77. I believe a POSITA would understand “device transaction sequence count,” “transaction sequence count information,” “sequence counter,” “and “sequence code” to be synonymous because the Patent appears to use them that way (and provides no other explanation). I take the terms to refer to some kind of sequential counter, which could include a transaction count or a transaction number.

78. Concluding this section, all of the technology claimed in the Challenged Claims predates the Critical Date and would have been within the knowledge of a POSITA.

VIII. CLAIM CONSTRUCTION

79. I understand that claim terms, in the absence of an express definition or disclaimer, are given their ordinary and customary meaning, as would have been understood by a POSITA at the time of the alleged invention.

80. In considering the meaning of the claims, however, I understand that one must consider the language of the claims in light of “the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.” 37 C.F.R. § 42.100(b).

81. I have applied these principles in interpreting the Challenged Claims for purposes of my analysis in this Declaration.

82. I understand that Petitioner does not assert that any claim terms require express construction in this proceeding.

IX. OVERVIEW OF PRIOR ART REFERENCES

A. U.S. Patent Application Publication 2010/0185545 (“Royyuru”)

83. Royyuru et al. U.S. Patent Application Publication 2010/0185545 (EX1004) is entitled “Dynamic Primary Account Number (PAN) and Unique Key Per Card,” and lists Vijay K. Royyuru as the first named inventor.

84. Royyuru was filed January 22, 2009 and published on July 22, 2010. I understand that Royyuru is prior art to the '579 Patent under pre-AIA 35 U.S.C. §§ 102(a), 102(b), and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

85. Royyuru discloses a system for conducting contactless financial transactions through RFID or NFC communication between a user device and a Point-of-Sale (POS) device (e.g., at a merchant location). EX1004, [0034]-[0035], [0047]. The user device generates “a set of dynamic cryptograms that are valid for a single transaction” including a “Dynamic Transaction Cryptogram (DTC)” and a “dynamic PAN” using various values and other data that are stored on the device, generated by the device, or received from outside sources such as a payment processor, a payment card issuer, another associated financial institution, systems associated with the merchant (such as the POS terminal) or the user himself. EX1004, [0005]-[0010], [0032]-[0034], [0047]-[0048], [0051], [0057]. The user device transmits the DTC and dynamic PAN to the POS terminal such that “[t]he transaction can be authenticated based on the DTC at the payment processor system or at the financial institution” and the real PAN can be determined to process the transaction. *Id.*, [0034].

86. In this manner, the merchant never learns the true PAN, but only receives a one-time PAN that cannot be reused, thus enhancing the security of a card payment.

87. Fig. 3 of Royyuru is reproduced below:

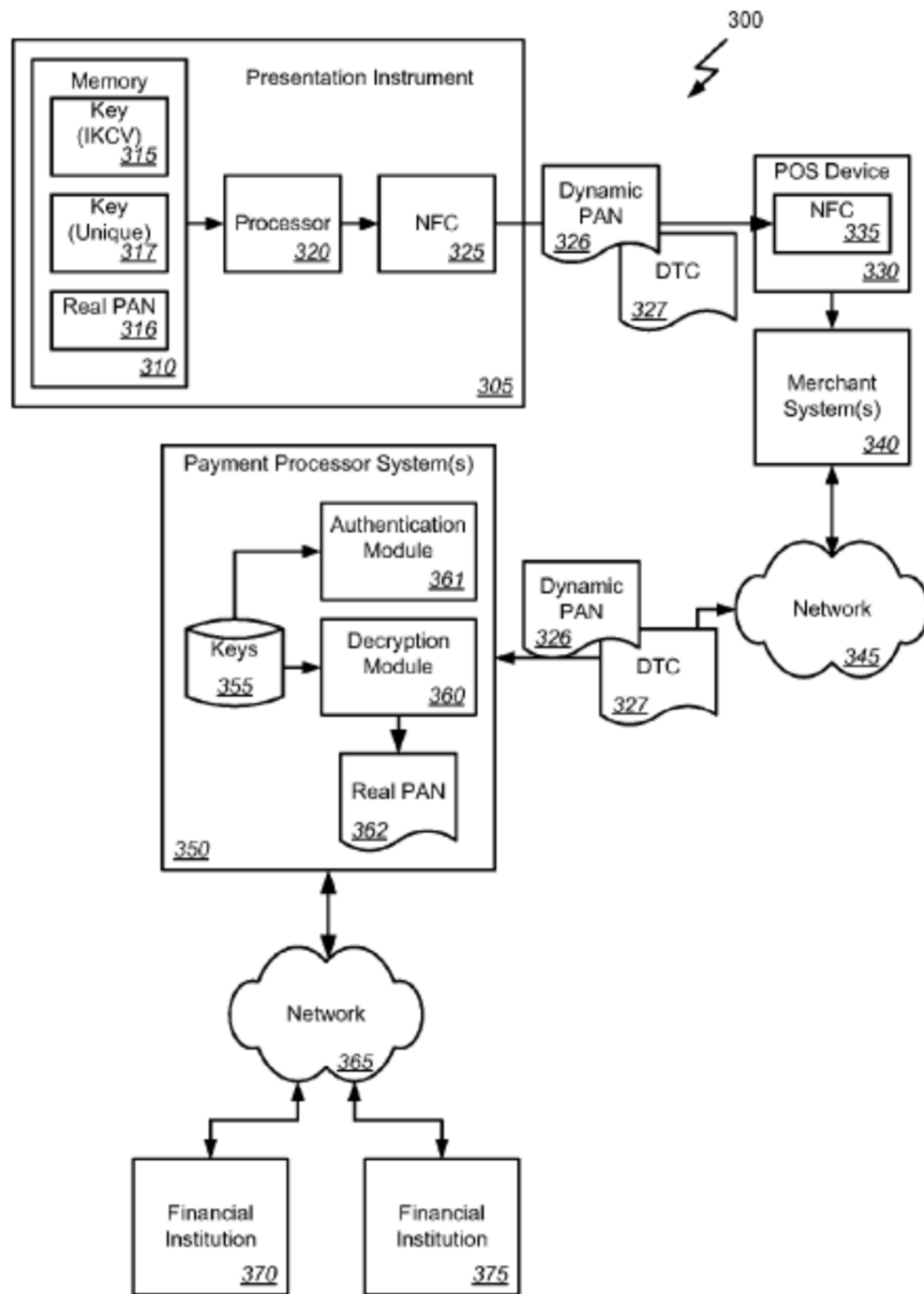


FIG. 3

88. The user device is “Presentation Instrument 305.” The merchant POS device is “POS Device 330.” The Real PAN 316 is stored in the user device. However, as can be seen, the Real PAN is not emitted by the user device. Instead, a Dynamic PAN 326 and DTC 327 are sent via NFC to POS Device 330.

B. U.S. Patent Application Publication 2012/0310760 (“Phillips”)

89. Phillips et al. U.S. Patent Application Publication 2012/0310760 (EX1005) is entitled “Mobile Device Automatic Card Account Selection for a Transaction,” and lists Simon Phillips as the first named inventor.

90. Phillips was filed September 1, 2011 and published on December 6, 2012. I understand that Phillips is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

91. Phillips describes a mobile telephone having a virtual wallet that allows a user to select from among multiple payment options or use “an automatic card selection option.” EX1005, [0017], [0029], [0033]-[0035], [0059]. An exemplary screen of the virtual wallet is shown below:

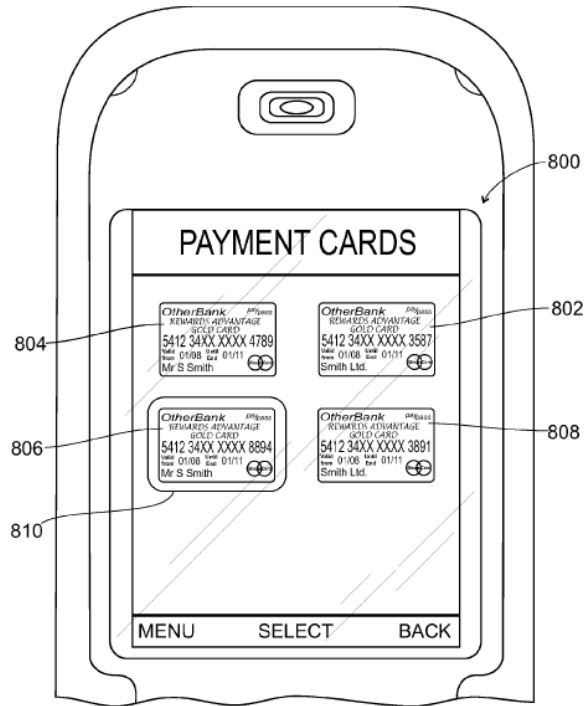


FIG. 8

Id., FIG. 8.

92. The “Payment Cards’ sub-menu” includes faces of “payment card account[s] issued to” the user along with various indicia to allow “selection of the payment card account that corresponds to the payment card represented by the card-face image.” *Id.*, [0039]-[0041], [0036]. “[T]he user may be required to enter a PIN or code before selecting a payment card” or to otherwise approve a financial transaction. *Id.*, [0038]-[0039], [0059], [0066].

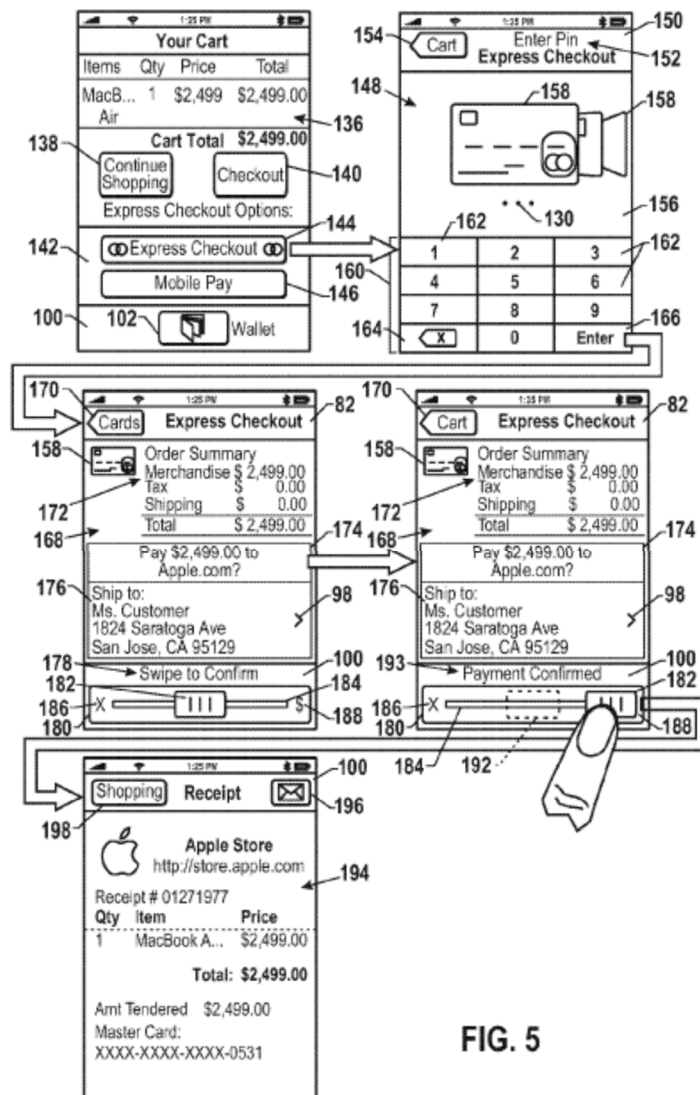
93. Phillips further describes receiving “a payment request that includes a merchant identifier (merchant ID)” that initiates the card selection and payment transaction functions. *Id.*, [0072]. The request can come in the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057].

C. U.S. Patent 8,255,323 (“Casey”)

94. Casey et al. U.S. Patent 8,255,323 (EX1006) is entitled “Motion Based Payment Confirmation,” and lists Brandon J. Casey as the first named inventor.

95. Casey was filed January 9, 2009 and issued on August 28, 2012. I understand that Casey is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

96. Casey describes a mobile payment system that allows a user “to confirm or decline a payment transaction using a selected payment instrument” before transmitting “payment information for the payment transaction...to a merchant or payment recipient.” EX1006, Abstract. Specifically, Casey discloses interfaces for receiving “a request for payment” via NFC or other communication, displaying payment card and transaction information, and receiving a PIN or user movement of a graphical element (slider) to confirm or deny a transaction. *Id.*, 8:52-9:36, 12:66-13:51, 14:11-49, 15:24-59; FIGs. 4-5. FIG. 5 of Casey, showing sliding by finger, is reproduced below:



97. Casey also discloses that the user device can receive input by sensing motion:

In addition to receiving user input through the input structures 60 and the touchscreen 54, the device 10 may include a motion sensing device 62 for receiving user input. The motion sensing device 62 may be any device configured to measure motion or acceleration, Such as an accelerometer or a gyroscope. In one embodiment, the motion sensing device 40 may be a three-axis accelerometer that includes a sensing element and an integrated

circuit interface for providing the measured acceleration and/or motion data to the CPU 46.

Id., 7:59-67.

98. Motion can be used to confirm a payment transaction:

Motion data acquired by the motion sensing device 62 may be used to confirm a payment transaction. As discussed further below, the motion sensing device 62 may be configured to sense motion of the device 10 and transmit motion data to the CPU 46 to adjust one or more graphical elements shown on the display 24. For example, a graphical element, such as a slide bar, may be moved across the display 24 in response to sensed motion.

Id., 8:6-11.

D. U.S. Patent Application Publication 2008/0172317 (“Deibert”)

99. Deibert et al. U.S. Patent Application Publication 2008/0172317 (EX1012) is entitled “Mobile Phone Payment with Disabling Feature,” and lists Doug Deibert as the first named inventor.

100. Deibert was filed January 9, 2008 and published on July 17, 2008. I understand that Deibert is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a), 102(b), and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

101. Deibert addresses a problem encountered in using mobile payment applications. In the prior art, when a user enabled a mobile payment application, it remained enabled, thus capable of making a payment, until a transaction actually occurred. If the user did not complete a transaction or decided against making one, the application might inadvertently make a payment when passed near an

“unauthorized contactless reader.” EX1012, [0024]. The user could avoid this risk by remembering to disable the payment application. However, if the user did not do so, the risk would remain. *Id.*

102. Deibert purports to solve the problem by disabling the payment application automatically after a predetermined time has elapsed if no transaction is completed. *Id.*, [0025].

103. The user can set “a predetermined timeout time such that the mobile payment application is disabled after the predetermined timeout time has elapsed” to “help prevent the accidental transmittal of [payment] information.” *Id.*, [0009], [0023]. Deibert also discloses that the user can manually activate a mobile payment application and further describes multiple techniques for disabling the mobile application to prevent unintentional transmittal of payment information, including completion of a transaction, manual disabling based on user input, and expiration of a predetermined timeout time. *Id.*, [0023]-[0025], [0058]-[0059].

E. U.S. Patent 8,423,462 (“Amacker”)

104. Amacker et al. U.S. Patent 8,423,462 (EX1008) is entitled “Real-Time Mobile Wallet Server,” and lists Matthew W. Amacker as the first named inventor.

105. Amacker was filed May 1, 2009 and issued on April 16, 2013. I understand that Amacker is prior art to the ’579 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

106. Amacker discloses a “mobile wallet server” (located on a user’s device, not at a remote server location) that allows a user to “control the distribution of personal/payment information... by selectively approving or rejecting requests for personal information using the mobile wallet server.” EX1008, 2:13-57. “The person may respond to the request by interacting with the mobile wallet server (e.g., select ‘accept’ or ‘reject’ button, etc.) using a user interface of an application that is triggered (executed) upon receipt of the request from the entity. Upon a selection of ‘accept’ (or similar approval), the mobile wallet server may transmit the requested information (e.g., personal/payment information, etc.) to the retailer to complete a pending process. In this way, the person may complete a complicated transaction, such as a purchase.” *Id.* The mobile wallet allows the user to select from among multiple “payment card” options. *Id.*, 5:18-41, Cl. 1. Such a selection is illustrated in FIG. 2 of Amacker, reproduced below:

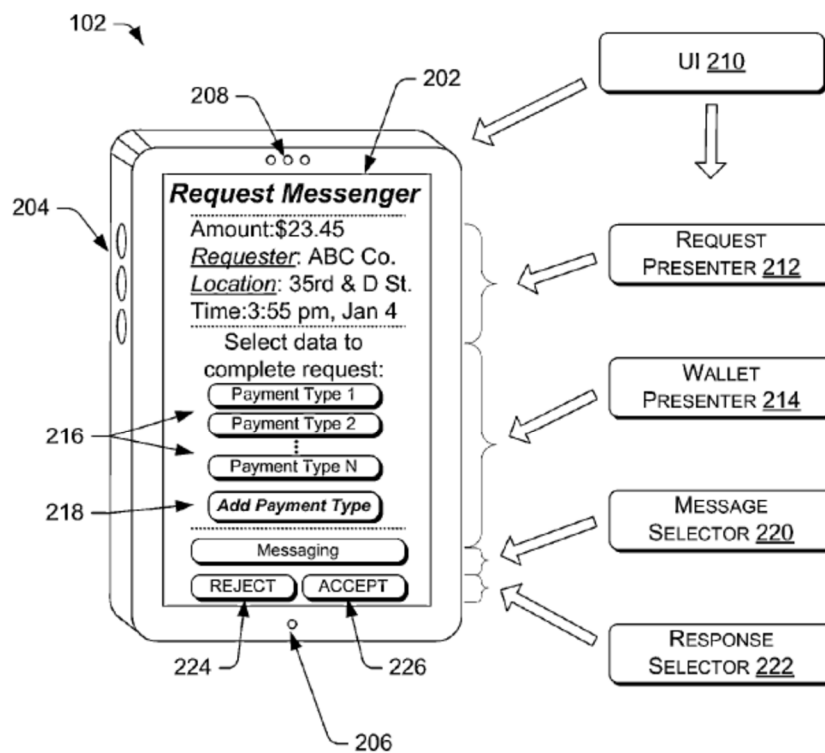


Fig. 2

107. Amacker uses the term “server” in an unusual manner. The “mobile wallet server 102” is a client-side application that hosts a “mobile wallet 108.” *Id.*, 3:4-22.

The MWS 102 may be any computing device capable of storing and processing data. For example, the MWS 102 may be a mobile server that is configured to operate on a smart telephone platform or other mobile computing device platform.

Id., 3:23-27.

F. U.S. Patent 9,600,808 (“Gomez”)

108. Gomez Sr. et al. U.S. Patent 9,600,808 (EX1007) is entitled “Secure Payment Card, Method and System,” and lists William Gomez. Sr. as the first named inventor.

109. Gomez was filed June 22, 2012 and published on March 21, 2017. I understand that it is prior art to the ’579 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

110. Gomez discloses a payment card system that purports to address “[t]he problems of fraud and identity theft that result from the use of payment cards, such as credit and debit cards” when cardholders conduct a payment transaction that “leave[s] behind all the information necessary for another person to be able to make an unauthorized transaction.” EX1007, 1:32-48.

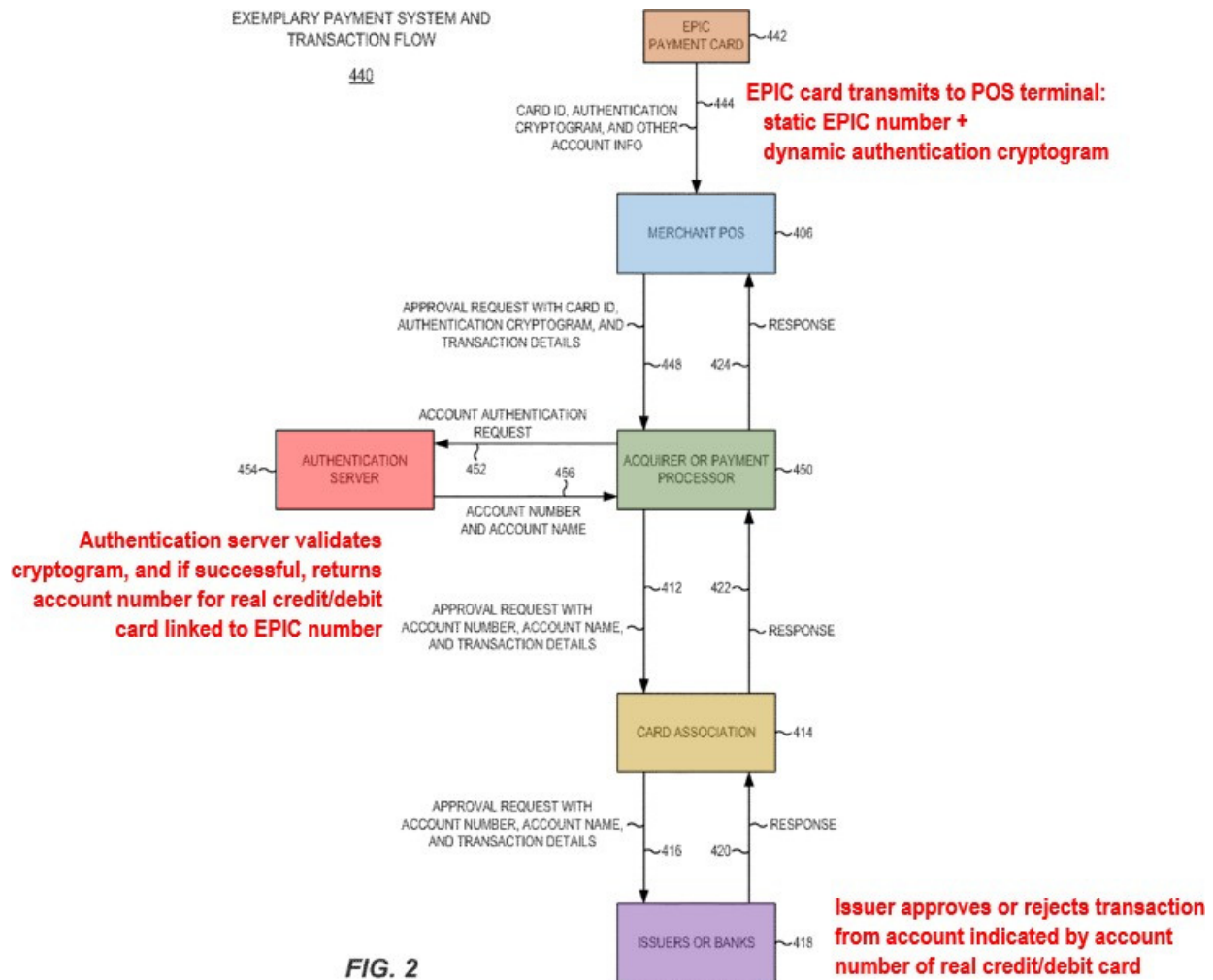
111. Gomez proposes a payment card “utiliz[ing] a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card, and which expires within a short period of time thereafter.” *Id.*, 1:58-63. Because the authentication cryptogram is time-limited, “the information that can be gleaned from a payment card ... is rendered useless for making an unauthorized subsequent transaction.” *Id.*, 5:7-11, FIG. 7.

112. Customers of the system described in Gomez are issued an electronic payment card, referred to as an “EPIC” card. *Id.*, 2:19-39. The EPIC card has a static payment card identifying number corresponding to the customer’s EPIC account.

Id. The customer can link one or more actual credit/debit cards to his or her EPIC account by entering the account numbers and other pertinent information of these credit/debit cards into an online EPIC portal, which the EPIC system then stores and links to the customer's static EPIC payment card identifying number. *Id.*, 20:1-29. The customer can then use the EPIC card to make payment transactions with any of the linked card accounts. In this manner, "there is no need to carry the actual credit cards, they may be stored safely at home or in a safe deposit box." *Id.*, 2:35-37.

113. When a customer initiates a transaction with an EPIC card, the card dynamically generates an "authentication cryptogram" based on a unique "seed value" stored securely in the card and a "temporal signal" that changes with each attempted use or transaction. *Id.*, 7:17-48. The payment card transmits the static EPIC number and the dynamically-generated authentication cryptogram to the point-of-sale (POS) terminal, which is then conveyed to an authentication server (e.g., EPIC) before the transaction request is sent to an issuer or bank for approval. *Id.*, 7:49-8:2. The authentication server authenticates the transaction using the cryptogram, and if successful, the authentication server returns the actual account number for one of the customer's linked credit/debit cards to the acquirer or payment processor, which information is then forwarded to the appropriate card association and issuer or bank for approval. *Id.*, 18:4-42, FIGS. 17-18.

114. Below is Fig. 2 from Gomez, annotated in color, illustrating a payment transaction approval process:



115. Gomez also discloses cryptographic hash functions:

At step 294 the message is processed, such as by using a cryptographic hash function, to generate a message “digest.” A cryptographic hash function is typically viewed as a deterministic procedure that takes an arbitrary block of data, known as a “message,” and returns a fixed-size string, known as a hash value or “message digest.” Such that any change to the message will change the message digest. Such functions are well known in the art, and include MD5, SHA-1, and SHA-2. For

example, MD5 returns a 128-bit message digest, while SHA-1 returns a 160-bit digest.

Id., 8:42-51.

116. Gomez also discloses a sequence code:

At step 256 a temporal signal value is generated which corresponds to the instance of attempted use. In some embodiments such a temporal signal value may reflect the date/time of the attempted use. The date and time may be determined by a real-time clock device included within the payment card, or may be communicated by the merchant POS terminal to the payment card, or by some other technique. **In some embodiments such a temporal signal value may reflect the sequence value (or sequential number) of the attempted use.**

Id., 7:17-26 (emphasis added).

G. U.S. Patent Application Publication 2008/0319905 (“Carlson”)

117. Carlson U.S. Patent Application Publication 2008/0319905 (EX1013) is entitled “Secure Mobile Payment System,” and lists Mark Carlson as sole inventor.

118. Carlson was filed June 24, 2008 and published on December 25, 2008. I understand that it is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a), 102(b), and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

119. Carlson describes techniques by which to “conduct[] transactions using pseudo primary account identifiers.” EX1013, [0012], [0029]. A pseudo account identifier is a false account number or other identifier that corresponds to an actual

account number of a real payment account. *Id.*, [0030]. The pseudoaccount identifier can be “similar in format to a consumer’s real account identifier” without revealing the true sequence of numbers or characters in the real account identifier. *Id.* Carlson notes that the use of a pseudo account identifier can be used to reduce instances of fraud and skimming by the merchant:

Embodiments of the invention have a number of advantages. First, since a pseudo account identifier 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***. There are many fraudulent merchants and this process reduces fraud as the merchant does not see the consumer’s real account number.

Id., [0083] (emphasis added).

120. The disclosed “pseudo account identifier” is of course a “token” or limited-use identifier,” as previously discussed.

121. Carlson discloses that the pseudo account identifiers can be generated remotely at a server, and downloaded to the user’s payment device wirelessly over a communications network. *Id.*, [0032]-[0034]. This allows new pseudo account identifiers to be updated on the device from time to time, thereby increasing security since unauthorized actors will be prevented from successfully using an expired pseudo account identifier to complete a payment transaction. *Id.*, [0044], [0083].

122. Carlson discloses NFC payments:

At least one major manufacturer of cellular phones has introduced a phone that is capable of being used as a payment card. In addition to the standard elements and capabilities of a cellular phone, the device also contains an additional element that is capable of storing a user's payment card information, such as their credit card account number, in the element on the phone. This element is further tied in with a short range wireless transmission element, such as a Radio Frequency Identification (RFID) tag, to allow the phone to transmit the account number over a short range to a contact less reader.

Id., [0004].

Near field communications capability is a short-range communications capability, such as RFID, BluetoothTM, infra-red, or other data transfer capability that can be used to exchange data between the portable wireless device 602 and an interrogation device. Thus, the portable wireless device 602 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

Id., [0089].

H. U.S. Patent Application Publication 2012/0123937 (“Spodak”)

123. Spodak U.S. Patent Application Publication 2008/0319905 (EX1009) is entitled “Portable e-wallet and universal card,” and lists Douglas Spodak as sole inventor.

124. Spodak was filed January 26, 2012 and published on May 17, 2012. I understand that it is prior art to the '579 Patent under pre-AIA 35 U.S.C. §§ 102(a) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

125. Spodak discloses a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002]. The universal card is similar to a mobile device such as a phone except that the universal card is shaped like a credit card.

Also depicted in FIG. 1 is a universal card 110. The universal card 110 may include components such as a display 112, a power source 113, a processor 114, and memory 115. Each of those components are similar in function to the corresponding components of the mobile device 100, except that the component of the universal card 110 may be physically configured differently so as to fit in the shape of the universal card 110. For example, the display 112 of the universal card 110 may be integrated into universal card 110 via hot lamination processes and standard inlay constructs so that the universal card 110 will be the approximate shape and size of a traditional credit card and generally compliant with ISO 7810 standards.

Id., [0027], [0034].

126. The universal card includes both a dynamic magnetic stripe and a short range transceiver. *Id.*, [0033], [0035]. The universal card can use the dynamic magnetic stripe to communicate with a traditional credit card magnetic stripe reader, and the short range transceiver to communicate with a contactless payment terminal such as via NFC:

The instructions sent from the mobile device 1591 to the universal card 1593 can include instructions for the universal card to emulate either or both of a magnetic stripe of the traditional card and a contactless payment form of the traditional card.

Id., [0088].

In one embodiment, the universal card 110 configures both the dynamic magnetic stripe 111 to emulate the magnetic stripe of the selected traditional credit card and the short range transceiver 116 to emulate the selected traditional credit with a contactless payment terminal. In this manner, the user needs only to select the desired traditional card using the e-wallet software 105, without having to make a selection of magnetic stripe or contactless payment, and the user can use the traditional card with either a magnetic swipe terminal or a contactless payment terminal.

Id., [0089]. The universal card can include a display. *Id.*, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A.

127. To emulate the magnetic stripe and authenticate the transaction, the universal card generates a dynamic authentication value in the field typically used for a CVV value:

In another embodiment, the traditional card may have a field on the static magnetic stripe for a CVV value. When the universal card is configured to emulate the traditional card that normally has a static CVV value field, the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value. The dynamic authentication value could have the same format as the static CVV and be located in the same location that the static CVV field would be located in the static magnetic stripe of the traditional card. In this scenario, there would be no need to reconfigure the terminal with the magnetic stripe reader because it would already be configured to read a value from the

static CVV field location. Using dynamic authentication values with traditional magnetic stripe reader terminals allows for the added security of the dynamic authentication value authentication without requiring terminals to add a contactless payment terminal to the magnetic stripe reader.

Id., [0094].

I. U.S. Patent Application Publication 2013/0036050 (“Giordano”)

128. Giordano et al. U.S. Patent Application Publication 2013/0036050 (EX1010) is entitled “System and method for using a near field communication device to conduct a transaction with an alias,” and lists Joseph A. Giordano as the first named inventor.

129. Giordano was filed January 1, 2012 and published on February 7, 2013. I understand that it is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

130. Giordano describes a mobile payment system for a person-to-merchant (P2M) payment service:

Embodiments of the present invention provide a system and method for mobile banking person-to-merchant (P2M) payments conducted via a Near Field Communication (NFC) device. Embodiments of the invention allow users of a financial entity to make payments directly from their accounts, whether their accounts be checking, savings, line of credit, credit card, and/or other accounts, to a business, including small business users and national-scale business users, without having to share any confidential account information and without having to know account information for the intended recipient. Embodiments of the invention also allow users to receive payments from businesses directly into their financial institution accounts without requiring the user to share account information with the

business. It should be noted that some embodiments of the invention allow a user to make payments to and/or receive payments from a merchant in the same way that a user can make payments to and/or receive payments from another person. As such, as used herein, the phrase person-to-merchant (P2M) is intended to include person-to-person (P2P), merchant-to-merchant (M2M), and merchant-to-person (M2P) unless specifically stated otherwise.

EX1010, [0028].

131. Giordano describes a mobile payment device that generates an “alias” for each transaction based on information unique to the device and other information related to the transaction:

In an embodiment, the computer-implemented method 100 establishes default aliases for users. The default alias may be a static alias stored in the user’s mobile device and used to conduct transactions via near field communication devices. In some embodiments, the static alias is a unique identifier for an individual. The static alias is not the account number but can be matched up to the account number by the financial institution. In one embodiment, static aliases are established as default aliases for users when registering for the P2M service. In another embodiment, the computer-implemented method 100 prompts the user to approve a random or default static alias. When the user selects the static alias, the computer-implemented method may confirm that the static alias meets pre-defined criteria. For example, the pre-defined criteria may include that a user cannot register another user's static alias, that the static alias does not map to an existing account number, or that the static alias is not easily guessed or otherwise inappropriate. In some embodiments, the computer-implemented method 100 receives the static alias from the point-of-sale device and associates the static alias with the user.

Id., [0032].

In further embodiments, the computer-implemented method 100 receives a dynamic alias that has been dynamically-generated for

the user. For example, when the user activates a P2M application on a mobile device, a dynamic alias may be generated by the P2M application for a one-time transaction. The P2M application may generate the dynamic alias when the user's mobile device communicates with the point-of-sale device via the near field communication device. In one embodiment, the dynamic alias is randomly generated. The P2M application generates a random or pseudo-random alias comprising an issue identification number, a bank identification number, a user identification number, and a payment identification number. In some embodiments, the user identification number is modified based on an algorithm to change the user identification number for each transaction. In further embodiments, other elements of the alias are modified, such as the bank identification number, is modified by an algorithm so that the alias changes with each transaction. In this manner, the alias is a number that can be used in a similar manner to a standard account number but with increased security.

Id., [0033].

132. To manage the alias, the user can use a web browser or the P2M application on a device that displays graphical user interfaces on its display:

In block 108, the computer-implemented method 100 determines the account number associated with the alias. If the alias is a static alias, the computer-implemented method 100 matches the user identification number in the static alias with a user by means of a database of static aliases available to the financial institution. In some embodiments, the user is able to change the static alias using the P2M application, a web-based module, or by communicating with the financial institution (e.g., over the phone, at an ATM, at a bank branch, etc.). In some embodiments, the static alias is only available for a limited time or limited number of transactions before it expires and must be changed.

Id., [0038].

It should be understood that the memory device 650 may include one or more databases or other data structures/repositories. The

memory device 650 also includes computer-executable program code that instructs the processing device 620 to operate the network communication interface 610 to perform certain communication functions of the banking system 600 described herein. For example, in one embodiment of the banking system 600, the memory device 650 includes, but is not limited to, a network server application 670, an authentication application 660, a user account data repository 680, which includes user account data repository 680 and user account information 684, a banking application 690, which includes an alias determination server interface 692, and other computer-executable instructions or other data. In some embodiments the banking application 690 comprises a mobile web server application 693 that allows the user to change the static alias. The computer-executable program code of the network server application 670, the authentication application 660, or the banking application 690 may instruct the processing device 620 to perform certain logic, data-processing, and data-storing functions of the banking system 600 described herein, as well as communication functions of the banking system 600.

Id., [0066]

J. U.S. Patent 8,052,052 (“Power”)

133. Power U.S. Patent 8,052,052 (EX1016) is entitled “User-Activated Payment Card,” and lists Michael J. Power as sole inventor. Power was filed December 4, 2008 and issued on November 8, 2011. I understand that it is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

108. Power discloses a payment card designed to address a security problem that arises in wireless payments:

Unfortunately, this capability [RFID] allows thieves to steal customers' personal financial information without stealing their credit cards, and thus, without the customers knowledge. For example, a thief, who is proximate to a customer, can generate the external signal and receive the customer's personal financial information while the customer's credit card is still in the customer's wallet.

EX1016, 1:29-35.

109. Power's solution is to provide a payment card containing one or more sensors to detect a physical phenomenon to enable operation of the card. *Id.*, 1:39-53. When the card sits passively in a user's pocket or physical wallet, it is not enabled, so a thief cannot read the information it contains. When the user wants to enable the card, they must perform some physical action that is detected by a sensor and this causes the card to be energized. For example, when the user touches the card, an increase in temperature can be detected due to the user's body heat.

128. Power provides many examples of physical phenomena and associated sensors, including:

a resistive sensor that detects a resistance change when the user is holding the payment card; a capacitive sensor that detects a capacitance change when the user is holding the payment card; a pressure sensor that detects a pressure change when the user is holding the payment card; a photo detector sensor that detects a light-intensity change when the user removes the payment card from a storage location (Such as the user's wallet); and/or an acceleration sensor that detects an acceleration change when the user removes the payment card from the storage location.

Id., 1:58-67.

129. Note that the capacitive sensor detects when the user is holding (i.e. is in proximity to) the payment card.

X. THE CHALLENGED CLAIMS ARE INVALID

A. Ground 1A: Claims 1, 2, 4, 6-9, 11-12, and 15-23 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips and Casey

130. In my opinion, the combination of Royyuru, Phillips, and Casey renders obvious as a whole claims 1, 2, 4, 6-9, 11-12, and 15-23 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Royyuru with Phillips and Casey

131. All three references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS terminals. Royyuru focuses on the generation of a dynamic PAN and a cryptogram for use in a payment transaction. Royyuru does not disclose the details of the user interface of its user device. *See e.g.*, EX1004, [0046] (“a presentation instrument 305 can comprise a smart card, mobile device, or any other device.”). A POSITA would have been motivated to apply the teachings of Phillips and Casey to Royyuru to provide a suitable user interface for Royyuru’s mobile payment, in addition to the other modifications that I address below, to provide an intuitive interface for reviewing payment transaction details, selecting from available payment options, and completing the payment transaction. Additionally, a POSITA would have recognized that the features described below for authenticating that a valid user is

conducting the transaction would have improved security of the system. *See e.g.*, EX1005, [0035], [0038], [0062], [0070]; EX1006, 13:6-15.

132. First, a POSITA would have modified Royyuru based on Phillips (and Casey) such that the device receives a payment request from a POS terminal or other merchant device that includes information regarding the merchant and transaction. EX1005, [0072]; EX1006, 8:52-9:8, FIGs. 5-8. Royyuru discloses NFC communication between the user device and merchant device for exchanging information between the two devices. EX1004, [0022], [0044], [0047], [0051], [0057]. Phillips provides additional disclosure regarding the types of information that can be beneficially exchanged during such NFC communications between a user device and a merchant device. For example, Phillips discloses that NFC communications between the user device and the POS terminal can include a payment request that includes useful information for facilitating the transaction, such as a merchant identifier (although this was very well known, one of the major purposes of a merchant POS device having been to receive payment information). EX1005, [0072], [0023], [0027], [0057]. A POSITA would have recognized that receiving a request for a payment transaction via NFC communication, as disclosed by Phillips, was a well-known technique for facilitating payment transactions and would have provided useful information that could be used in the transaction, including in generating the cryptograms disclosed by Royyuru. Casey provides

additional disclosure regarding what type of information can be included in a payment request and further discloses displaying this request information to allow the user to visually review the transaction information prior to approving the transaction and causing the device to transmit payment information. EX1006, FIG. 5, 8:52-9:8, 15:24-16:20. As shown by, for example, FIG. 5 of Casey, the request can include information about the merchant, products being purchased, price, tax, etc. and such information can be displayed on the user device for verification by the user. *See, e.g.,* EX1006, FIG. 5 (reproduced above).

133. Modifying Royyuru's system such that the user device receives a payment request from a merchant device would have improved the system by allowing the user to better ensure that they are approving a payment transaction and transmitting payment information to a correct merchant terminal. A POSITA would have recognized that adding such known functionality to Royyuru's system would have beneficially prevented fraudulent transmittal of payment information to an incorrect terminal. Such a modification would also allow the user to visually review transaction data before approving the transaction to ensure that the items included in the transaction are correct, that the payment amount is correct, and or that other information is correct (e.g., a delivery or pickup location, discounts, coupons, etc.) prior to the user confirming the transaction to cause the device to transmit payment information. EX1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49. Additionally, Royyuru

discloses using any information “generated by the Presentation Instrument 305 or received by the Presentation Instrument 305, for example from the POS device 330 via the NFC modules” to generate the DTC and dynamic PAN. EX1004, [0051]. Based on this (and other similar) disclosure of Royyuru, a POSITA would have been prompted to beneficially turn to Phillips and Casey to identify additional data that would be received at the device and used in generating the dynamic cryptograms described by Royyuru. Specifically, a POSITA would have recognized that the request from the POS terminal would include such information for use in generating these cryptograms (as described by Royyuru and Casey) and that using such additional request information would have increased the set of possible values that would have been beneficially used in generating Royyuru’s cryptograms, thereby increasing security of the system. *Id.*, [0051].

134. Second, a POSITA would have been motivated to modify Royyuru based on Phillips (and Casey) such that the user authorizes the payment transaction prior to payment information being provided to the merchant terminal, using any of the well-known authentication and confirmation techniques described by both Phillips and Casey. Such an authorization could be by entering a PIN (as was well known and as taught by Phillips) or moving a graphical element to confirm or deny the transaction (as taught by Casey). EX1005, [0035], [0038]-[0039], [0059], [0066], [0061], [0068]; EX1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49. As Phillips

acknowledges, including a requirement that the user enter a valid PIN before receiving access to payment information and/or prior to transmitting payment information for completing the transaction “adds a layer of security to the process” by “guard[ing] against the possibility that the user of the mobile device is not the owner of a selected payment card account.” EX1005, [0035], [0038]. Thus, application of this technique to Royyuru would have ensured that an authorized user of the payment method is conducting the transaction based on confirmation of a valid PIN entry. Requiring such user authorization/confirmation would have provided additional benefits that would have been readily recognizable to a POSITA. For example, requiring such authorization/confirmation prior to allowing access to and/or transmitting payment information would have allowed the user to review transaction information (e.g., price, purchase items) prior to completing the transaction. This additional review would have ensured that the correct items and payment amount (and other information) were included in the transaction. This additional review also would have allowed the user extra opportunity to change their mind regarding a transaction and Casey provided a simple mechanism for confirming or denying the transaction after reviewing this information. *See e.g.*, EX1006, FIGs. 5-6, 8:52-9:8, 15:24-16:20. A POSITA also would have recognized that requiring authorization/confirmation of a payment transaction would have provided extra

assurance that the user intends to initiate a payment transaction rather than having inadvertently opened (or failed to close) a payment application.

135. Third, a POSITA would have been motivated to modify Royyuru based on Phillips (and Casey) such that the device stores information for multiple payment options and provides a graphic user interface, including payment method indicia, to allow user selection of a payment method from among a plurality of payment methods. It was well-known that mobile wallets accommodated multiple payment methods—as much is suggested by the very term “wallet.” EX1005, [0036]-[0041]; FIGs. 8, 11; EX1006, 9:4-28, 9:58-10:2, 12:46-65; FIGs. 5-8. Allowing a user to select from among multiple payment options would have provided more choice and options with respect to how the user spent their money, would have allowed the user to select payment options that are the most appropriate for a given scenario (e.g., due to budgeting or credit card rewards considerations), and reduced or eliminated the need for the user to carry additional physical payment instruments. Displaying payment method information, including card indicia, as taught by Phillips and Casey would have allowed the user to more readily recognize a payment method and would have provided assurance that the user was selecting the correct card. A POSITA would have recognized that such benefits would have outweighed any minor increases in memory usage to store the additional cards and information.

136. Fourth, a POSITA would have been motivated to modify Royyuru based on Phillips to allow the user to preselect one or more default payment options for different transaction scenarios. EX1005, [0005], [0017], [0059], [0066], [0029]. Such a modification to Royyuru's system would have increased the ease/speed of financial transactions by allowing the user to make some payments using a default payment option (thus eliminating the need to select a payment option at all). Applying such a modification in conjunction with Phillips' disclosure of allowing a user to select a preferred payment method when the user so desires would have provided the user with the full flexibility to select a payment option in some scenarios, while providing the easy and convenience of not having to select a specific payment method for each individual transaction in scenarios in which the user does not wish to take the additional time to make such a specific selection, thus providing both convenience and control to the user depending on what is more important to the user during any given transaction.

137. Fifth, a POSITA would have modified Royyuru based on Casey so that the user device displays transaction status information, including a received payment receipt information confirming that the transaction was successful and showing details on the completed transaction. EX1006, 10:47-53, *see also* 10:20-29, 16:3-20. Such a modification would have provided additional assurance to the customer that the correct transaction occurred. Additionally, providing such information to the user

at the completion of a transaction would have allowed the user to more quickly take steps to correct an incorrect transaction, thus increasing user satisfaction and eventually increasing the customer base by providing an improved system. Such a modification would have also allowed the user to more easily keep digital records of financial transactions. Furthermore, it is typical in payment transactions to provide the customer with a receipt. Providing the receipt in a digital format, as taught by Casey, would have eliminated the waste of traditional paper receipts while also providing a more convenient method for storing, organizing and retaining receipts. Casey also discloses that the receipt can include additional useful information regarding the transaction such as “a notification message from the store indicating that the order is ready for pickup” or “a map of the store showing the pickup location” among other beneficial information that would have improved the shopping experience for the user. *Id.*.

138. Lastly, a POSITA would have been motivated to modify Royyuru based on Phillips and Casey because doing so would have been merely the application of known techniques to a known system ready for improvement to yield predictable results. Here, all three references describe aspects of conducting contactless payment transactions using payment information stored on or generated by a device and Phillips and Casey describe improvements that would have been beneficially applied to Royyuru’s system to improve the overall user experience and

transaction security. Furthermore, a POSITA would have had a reasonable expectation of success in modifying the mobile payment system of Royyuru based on Phillips and Casey as they all are directed toward similar mobile payment systems and all rely on common capabilities of devices. Specifically, as described above and in greater detail below, the disclosures of Phillips and Casey complement the teachings of Royyuru. Royyuru's disclosure focuses on generation of the dynamic cryptograms (the DTC and dynamic PAN) for increasing security of transmitted payment information, while Phillips and Casey provide additional user interface details and user authentication details that would have readily integrated with the dynamic cryptogram generation disclosures of Royyuru, thus giving the POSITA a reasonable expectation of success combining the teachings of these references into a single system.

2. Claim 1

[1pre]: A method of performing a transaction, the method comprising:

139. Whether or not the preamble is limiting, it is disclosed by all three of Royyuru, Phillips, and Casey, which all disclose methods of processing a financial transaction using a device. EX1004, [0005]-[0010], [0002], [0035]; EX1005, Abstract; EX1006, Abstract.

[1a]: receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises:

140. Royyuru discloses that “[w]hen the cardholder wishes to execute a transaction, such as a financial transaction...[he] *passes or taps the presentation instrument 305 on or near the point-of-sale device 330.*” EX1004, [0047], *see also* [0005], [0044], [0050], [0053]. Before the device can conduct a transaction, the user confirms their identity with a PIN: “The processor 320 can also generate a dynamic transaction cryptogram (DTC) 327 based on the unique card-level key 317 and perhaps other information such as a Personal Identification Number (PIN) provided by the consumer.” *Id.*, [0047]. This primes the user device to enable it to conduct a transaction. Further, Phillips teaches that, in the combination, the user is required to “enter a PIN” to initiate a financial transaction. EX1005, [0035], [0038]-[0039], [0066]. The PIN confirms the identity of the user as a valid user. The PIN entry is the input that corresponds to a priming action that identifies the user as authorized to use the card for executing a transaction. *See also* EX1001, 11:34-42, 13:25-32 (the ’579 patent’s examples of priming). Without such priming, the transaction would not take place.

[1b]: a processor

141. All three of Royyuru, Phillips, and Casey disclose user devices having processors, e.g. processor 320 of Royyuru, main processor 204 of Phillips and CPU 46 of Casey. EX1004, [0046]; EX1005, [0024]; EX1006, 6:15-20.

[1c]: a touch screen display coupled to the processor

142. Royyuru describes “a mobile device” and that “a presentation instrument 305 can comprise a smart card, mobile device, or any other device.” EX1004, [0021], [0040], [0046]. Such devices commonly had touch screen displays. Royyuru incorporates by reference U.S. Patent Application Publication 2008/0017704, which discloses that the mobile device “include[s] a touch screen” display. *Id.*, [0021]; EX1011, [0006]. Furthermore, Phillips and Casey also disclose touchscreens. EX1005, [0018]; EX1006, 3:10-19. Phillips describes that a “display” is “in communication with and/or controlled by the control circuitry,” which “may be, for example, a main processor or microprocessor.” EX1005, [0018], [0020].

[1d]: a near field communications (NFC) interface coupled to the processor

143. This element is disclosed in all three of Royyuru, Phillips, and Casey. Royyuru’s mobile device includes “an NFC module 325 communicatively coupled with the processor 320.” EX1004, [0051], [0046], [0002], [0022]. Phillips in FIG. 2 discloses a “proximity payment controller 224” (an NFC interface) connected to

“main processor/control circuit 224.” EX1005, [0023]. Casey in FIG. 2 shows “NFC 44” connected to “CPU 46.” EX1006, 5:57-6:31.

[1e]: receiving a request for a transaction payment at said electronic device via the NFC interface

144. This element is disclosed in all three of Royyuru, Phillips, and Casey. Royyuru’s device can “detect initiation of the transaction.” EX1004, [0009]. Royyuru explains that the device uses NFC for “close proximity...short range communications between [the] mobile device and [the] POS device.” *Id.*, [0022], [0044], [0047]; EX1005, [0023]. Phillips discloses that, in the combination, “the mobile device...receives 1302 a payment request that includes a merchant identifier (merchant ID).” EX1005, [0072]. The request can come in the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057]. Casey discloses that “receiving information through...the NFC device...may include a request for payment.” EX1006, 8:52-9:8, FIGs. 5-8.

[1f]: displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card

145. FIG. 8 of Phillips, reproduced above, shows “a ‘Payment Cards’ sub-menu” displayed on the user interface of the device that includes faces of “payment card account[s] issued to” the user to allow “selection of the payment card account that corresponds to the payment card represented by the card-face image.” EX1005, [0039]-[0041], FIG. 8.

146. The Payment Cards sub-menu allows a user to “select one of the payment cards...to use in a current transaction.” *Id.*, [0037], [0039]. The displayed payment cards “include information such as the payment card account number [and] issuer bank name.” *Id.*, [0039], [0036]. As shown in FIG. 8, the displayed issuer card account numbers are partial numbers with the last four digits displayed. *Id.*, FIGs. 8, 11.

147. Casey also discloses displaying images of a card issuer payment method selection. EX1006, 9:4-28, 9:58-10:2, 12:46-65. FIG. 5 of Casey shows a receipt with only the last four digits of a PAN being displayed.

148. To the extent this limitation is interpreted narrowly, it would have been obvious to a POSITA to display *only* the last four digits of the issuer card account numbers to further enhance security by obscuring a larger portion of the credit card number while providing enough of the number to facilitate easy card recognition/selection by a user. This is disclosed by Royyuru. EX1004, [0032] (describing displaying only the last four digits of “the real PAN” on a payment receipt for security purposes).

[1g]: a card logo

149. It is of course obvious to display an image of a payment card when presenting the user with a choice of payment cards, and it was well-known that payment cards typically bore the logo of the issuing bank. Such indicia help users

more easily distinguish between payment card options when selecting a payment card for a particular transaction.

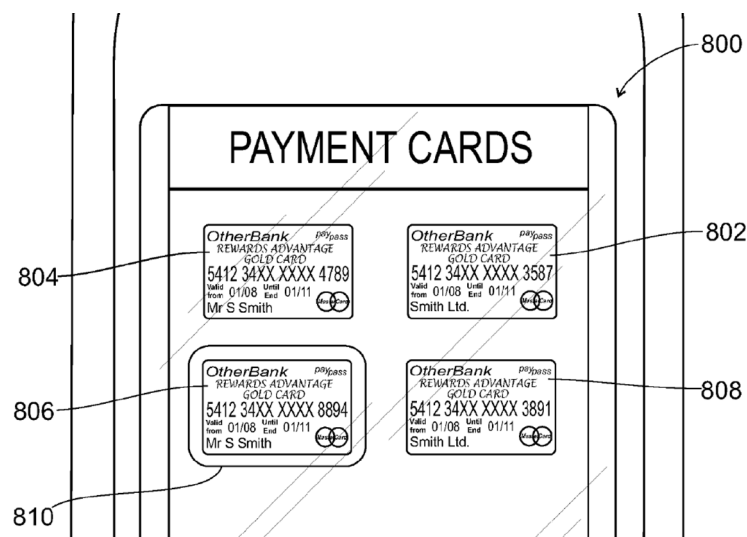
150. As shown in FIGs. 8 and 11 of Phillips, the Royyuru-Phillips-Casey combination discloses displaying an “issuer logo” on the touchscreen. EX1005, [0039], [0036], [0041], [0058], [0065].

151. Further, as shown in FIG. 5 of Casey, the MasterCard double-circle logo is shown as part of card 158. EX1005, FIG. 5.

[1h]: other iconography of the payment card

152. It is of course obvious to display an image of a payment card when presenting the user with a choice of payment cards, and such an image would also contain any accompanying iconography.

153. The image below is a portion of FIG. 8 of Phillips, showing “other iconography” of four different payment cards:



154. The displayed card-face “include[s] information such as the payment card account number, issuer bank name, issuer logo, card account holder name, the expiration date, a unique color or color combination, and/or other pertinent data.” EX1005, [0039], [0041], [0036]; FIG.8.

[1i]: generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information

155. Royyuru provides at least two examples of the claimed “limited-use payment information”: the “Dynamic Transaction Cryptogram (DTC)” and the “dynamic PAN.” EX1004, [0005]-[0010], [0032]-[0033], [0047]. “A Dynamic Transaction Cryptogram (DTC) can be *generated at the device*, using a unique card level key stored on the device.” *Id.*, [0005]. In another example, “[t]he DTC can be computed by the device by combining several fields including the PAN, service code, expiration date, unpredictable number, and ATC and encrypting them using the CK.” *Id.*, [0057]. The CK “is unique per card” and therefore the DTC is limited in use to the specific user device. *Id.*, [0057], [0032] (explaining that the term “card” refers to “a smart card” or “other device adapted for use as a payment instrument”), [0021]. The DTC is generated by processor 320. *Id.*, [0047].

156. Royyuru contains similar disclosures regarding the dynamic PAN, which is generated by the user device “based on the real PAN and an Institution Key Card Variant (IKCV) stored on the device.” *Id.*, [0005]. In another example, the

dynamic PAN is “computed by the device for each transaction by combining the digits from the card number with the ATC and with the unpredictable number sent by the RFID or NFC reader and then encrypting these digits with the KCV.” *Id.*, [0057]. Both the DTC and dynamic PAN are “valid for a single transaction” and are therefore limited-use. *Id.*, [0033]. The dynamic PAN or “Pseudo-PAN can be sent in place of the real PAN.” *Id.*, [0057], [0007] (describing the issuer supplied “Primary Account Number (PAN)”), [0032] (“This dynamic PAN can then be used in the transaction instead of the real PAN”); The DTC is generated by processor 320. *Id.*, [0047]. In other examples, Royyuru describes “providing the DTC and dynamic PAN to a Point-of-Sale (POS) device” and “from the POS device to a payment processor system” rather than the real PAN. *Id.*, [0006]-[0010].

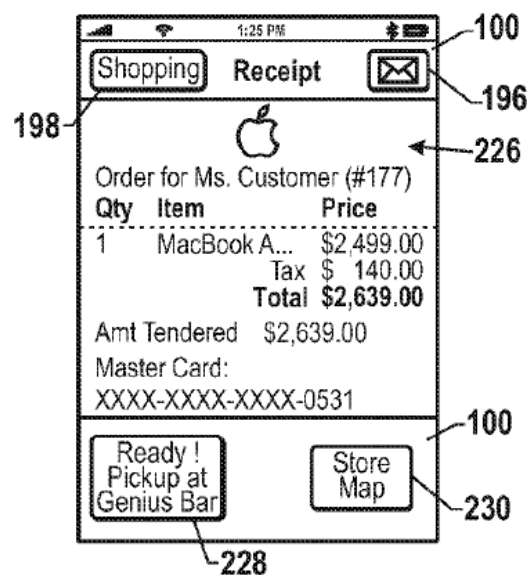
[1j]: transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface

157. In Royyuru, the purpose of the limited-use payment information is for it to be transmitted to an NFC recipient (e.g., a merchant NFC POS device) of the transaction. Royyuru discloses that “[t]he dynamic PAN can be provided to the merchant system 340, e.g., via the NFC module 325 of the presentation instrument and corresponding NFC module 335 of the POS device 330.” EX1004, [0047]. Royyuru states: “[t]he device can then provide the DTC **327** and the dynamic PAN **326** to the NFC module **325**” and then “providing the dynamic PAN to a Point-of-Sale (POS) device” via the NFC interface. *Id.*, [0051]-[0052], [0034], [0054],

[0057]. So much is evident from the transaction flow in Royyuru FIG. 3, reproduced above in Section IX.A.

[1k]: visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.

158. It is universal in payment transactions to provide a receipt indicating that the transaction is complete. As described by Casey, in the Royyuru-Phillips-Casey combination, “*the device 10 may receive and display (block 78) a receipt for the payment transaction.* For example, the receipt may identify the amount tendered, the payment recipient, and the payment instrument used.” EX1006, 10:47-53, *see also* 10:20-29, 16:3-20. FIG. 8 shows the receipt screen showing the completed status of the transaction:



Id., FIG. 8.

159. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 1 of the '579 Patent as a whole obvious to a POSITA.

3. Claim 2

[2] The method of claim 1, wherein the generating the limited-use payment information utilizes at least one information from a set of information comprising: a device transaction sequence counter; a device account number; device secret keys; card issuer keys; merchant information; NFC recipient information; payment reader information; a time; a timestamp; an amount; a location; an online location; transaction information; payment information; device information; user information; an email address; and a user identification entry.

160. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

161. I understand that a set of “at least one information from a set of information comprising” is disclosed by any single member of the recited set.

162. Royyuru discloses that “[t]he DTC can be computed by the device by combining several fields including the **PAN, service code**, expiration date, **unpredictable number**, and **ATC** and encrypting them using the **CK**.” EX1004, [0057]. Similarly, in one example, the dynamic PAN is computed using “the **digits from the card number** with the **ATC** and with the **unpredictable number sent by the RFID or NFC reader** and then encrypting these digits with the **IKCV**.” *Id.* A POSITA would have recognized that the PAN/card number are payment information;

the unpredictable number sent by the NFC reader is transaction, device, merchant, NFC recipient, and payment reader information; the IKCV and CK are card issuer keys; the IKCV is a device account number, and the ATC is a device transaction sequence counter or device secret keys. *Id.*, [0004], [0006], [0057], [0047] (“time of day”), [0051].

163. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 2 of the ’579 Patent as a whole obvious to a POSITA.

4. Claim 4

[4] The method of claim 1, wherein a limited-use number comprises a device account number, and wherein the device account number is of a limited time-duration of valid use, and wherein further a card issuing authority provides said device account number for use only by the electronic device, in place of card issuer information in performing payment transactions by the electronic device, and further comprising: performing payment transactions by the electronic device including the limited-use number; combining the limited-use number and said device account number within a device generated payment information; and conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.

164. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the ’579 Patent as a whole obvious.

165. Royyuru’s IKCV is a limited-use number that corresponds to the claimed “device account number.” The IKCV is “generated when each card (device)

is being customized” and is generated by the payment processor *or issuer* based on the PAN and “institution key of the issuer of the account.” EX1004, [0057], [0046], [0033], [0055]. Royyuru also expressly refers to the “IKCV *of the device.*” *Id.* Because the IKCV can be generated by the issuer, a POSITA would have recognized that it is provided, either directly or indirectly, to the device for use by the device in payment transactions. *Id.*, [0046], [0033], [0055], [0057]. A POSITA would have therefore recognized the IKCV as a device account number because it is specific to the device and based on payment account information. Royyuru describes that the IKCV is one of the card-level keys (CK). *Id.*, [0006], [0057]. The DTC is generated using one of the CKs (such as the IKCV) and the dynamic PAN is generated using the IKCV and, therefore, each comprises the device account number. *Id.*, [0057], [0005]-[0009].

166. The “expiration date” of the payment account is also used in generating the IKCV. *Id.*, [0091]-[0096]. As would have been recognized by a POSITA, the IKCV has a limited time-duration of valid use because after the expiration date has expired, a new IKCV would need to be generated based on the new expiration date to match the valid account information having the new expiration date. Alternatively, it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use tied to the payment account expiration date so that an

IKCV generated using an expired PAN could not be used for transactions. This would help ensure that the user's account is still valid. *Id.*

167. Because the IKCV is the device account number, the IKCV makes up part of the DTC and is therefore combined with the limited-use number (the dynamic PAN) as part of the device generated payment information. EX1004, [0057], [0005]-[0009]. As described with respect to claim 1, *supra*, the DTC and dynamic PAN are transmitted together to the POS terminal, and then the payment processor, in place of card issuer information (e.g., the real PAN and validation code) to perform payment transactions. *Id.*, [0032]-[0034], [0047], [0051]-[0052], [0057], [0032] (“This dynamic PAN can then be used in the transaction instead of the real PAN”). See the transaction flow in Royyuru FIG. 3, reproduced above.

168. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 4 of the '579 Patent as a whole obvious to a POSITA.

5. Claim 6

[6] The method of claim 1, wherein a payment processing authority verifies a limited-use number based on at least one information of the set of information comprising: a transaction sequence count information; a device account number; user account information; issuer secrets; issuer keys; issuer-provided device keys; transaction information; and a time of use, and further comprising: authorizing said transaction, by the payment processing authority, responsive to verifying a valid limited-use number appearing in place of card issuer information; and rejecting a limited-use number, by the payment processing authority, on at least one unverifiable condition, of a set of unverifiable conditions comprising: an invalid number generation; an invalid device account number; a use outside of a valid time window; an invalid re-use of a limited-use number; and an invalid use of an expired limited-duration number.

169. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

170. Royyuru discloses that “[t]he transaction can be authenticated at the payment processor system or at the financial institution **based on the DTC**. For example, **determining the real PAN** can comprise decrypting the dynamic **PAN using a key maintained by the payment processor system** and corresponding to one of the card-level keys of the device (e.g., the, IKCV).” EX1004, [0006], [0034]. Furthermore, “[a]uthenticating the transaction at the payment processor can **comprise validating the DTC using a key maintained** at the DTC validation system (e.g., the payment processor system or the financial institution), corresponding to the unique card level key on the payment device.” *Id.* “The real

PAN can then be sent from the payment processor system to a financial institution to affect processing of the transaction.” *Id.*

171. The payment processor can “decrypt the dynamic PAN to determine the real PAN for a transaction” using “a set of keys, i.e., private keys held by the payment processor and/or financial institution.” *Id.*, [0039], [0048] (describing an authentication module that authenticates DTC and dynamic PAN using “a key corresponding to each card-level key”). The real PAN is then used to “process the transaction, for example, by sending an authorization request, via financial network 365, to the issuing financial institution 370 or 375” that includes the real PAN. *Id.* Therefore, the keys are used to verify the limited-use number for use in processing the transaction. In another example, “[t]he real PAN can then be used to retrieve the card level key for that device and validate the DTC using the unique card level key. If the DTC is authenticated 435, the real PAN can then be sent 440 from the payment processor system to a financial institution to affect processing of the transaction.” *Id.*, [0055], [0050]. The financial institution provides a response “to indicate approval and/or completion of the transaction.” *Id.*

172. A POSITA would have recognized from these teachings of Royyuru that verification of the DTC and dynamic PAN by the payment processor are necessary to process the transaction and therefore the limited-use number (DTC or dynamic PAN) is rejected if invalid number generation (e.g., invalid DTC or

dynamic PAN) is detected. Furthermore, the DTC and dynamic PAN are valid only for a single transaction. Therefore, they will be rejected by the payment processor if used after the single transaction (invalid use of an expired limited-duration number). *Id.*, [0033], [0053]. In another example, the DTC and dynamic PAN are rejected based on comparing the ATC “to that in the previously received transaction to detect gaps...and duplication” indicating fraud. *Id.*, [0057].

173. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 6 of the '579 Patent as a whole obvious to a POSITA.

6. Claim 7

[7] The method of claim 1, wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: a device button; a device touch-screen interface; a device touch ID button interface; a device optical sensor array; a device skin touch sensor; a skin-contact sensor; a device motion detection interface; a device biometric sensor interface; and a device user-interface selection.

174. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

175. Phillips discloses that the device of the Royyuru-Phillips-Casey combination can be primed by entering a PIN to initiate a financial transaction to increase security. EX1005, [0035], [0038]-[0039], [0066]. Without the PIN, the device is not “primed” for a transaction. The combination has “a touch screen

capable of accepting user input” and therefore the user would enter the PIN using the device touch-screen interface. EX1005, [0020].

176. Casey is explicit that the device can be primed for a transaction by dragging a graphical element via a touch screen. EX1006, 14:11-24. Casey also discloses priming by having the user make a motion that is sensed by “any device configured to measure motion or acceleration.” *Id.*, 7:59-83.

177. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 7 of the ’579 Patent as a whole obvious to a POSITA.

7. Claim 8

[8] The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising: a button press; a touch ID button press; a button double-press; a touch ID sensor touch; a touch-screen touch; a touch-input sequence; a gesture or swipe over a sensor-array; a skin-contact sense; an optical-sensor array sense; an electronic device tap; a sequence of motions of the electronic device; a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation; and, further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a touching from an identified valid user; a user entry of a valid passcode; a user entry of a valid PIN; swiping of a recognized user skin over a device sensor array; a correct user swiping or gesturing on the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motioning of the electronic device; a skin-contact sensing of an identified user; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is

continuously remaining in the proximity possession of a valid user.

178. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

179. Phillips discloses that, in the combination of Royyuru, Phillips, and Casey, the priming operation can be entering a PIN on a touchscreen (a touch-input sequence) or selecting a payment method from the payment method selection menu. EX1005, [0036]-[0041], [0020]; *see also* EX1006, 9:4-28, 9:58-10:2, 12:46-65. Phillips and Casey disclose that, in the combination, the electronic device is enabled for payment through user entry of a valid PIN or correct user swiping. EX1005, [0059] (“a payment transaction...is not enabled unless the PIN had been recently entered into the phone”), [0062], [0066], [0070]; EX1006, 9:9-36 (“the device 10 may request...a PIN to verify the payment instrument”), 12:64-13:51 (“...prompt the user to move a graphical element 180 to confirm the payment transaction”), FIGs. 5-8.

180. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 8 of the '579 Patent as a whole obvious to a POSITA.

8. Claim 9

[9a]: The method of claim 1, further comprising: obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a

device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user

181. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

182. The device of the combination has a touchscreen for receiving input. *Supra*, Element [1c]. Casey teaches that a user can swipe, or select a control, on the touchscreen to approve the payment.



183. EX1006, FIG. 5, *see also* FIGs. 6-8, 9:9-36. As described by Casey, the device can “prompt the user to move a graphical element 180 to confirm the payment transaction.” *Id.* 13:24-51.

[9b]: displaying, on the display, at least one information of a set of information comprising: a priming status of the electronic device for payment; a default payment method; a plurality of selectable payment accounts; a payment request; transaction information; a payment amount; a merchant identification; a time; an expiration date; a location; an account balance; a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography;

184. As demonstrated by FIGs. 8 and 11 of Phillips, the device of the Royyuru-Phillips-Casey combination displays a plurality of selectable payment accounts, expiration dates, payment bank logos, card images, etc.:

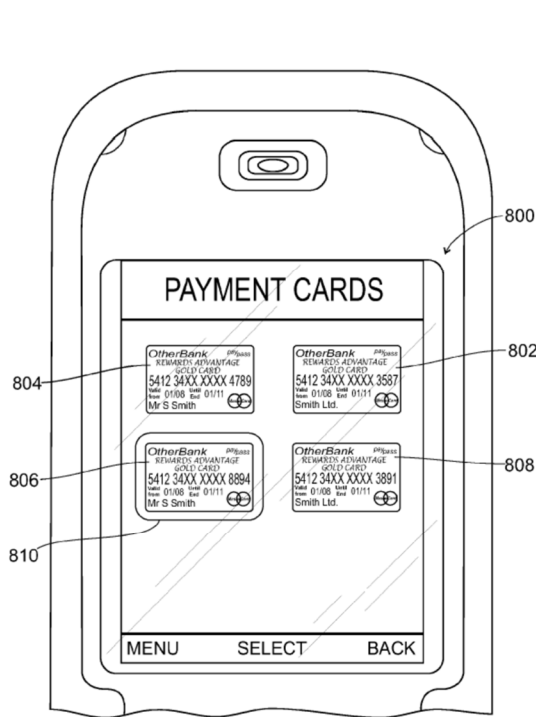


FIG. 8

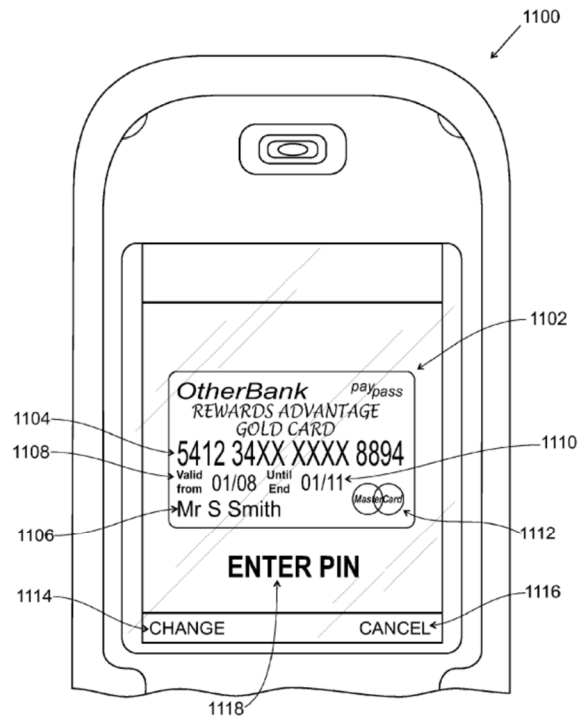


FIG. 11

EX1005, FIGs. 8, 11; [0036]-[0041]; *see also* EX1006, 8:52-9:28, 9:58-10:2, 12:46-65, 13:24-51, FIGs. 5-8.

[9c]: receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.

185. It is of course obvious in device payment transactions for a user to (i) select a payment method from a wallet; and (ii) authorize a transaction. The first is a matter of necessity, while the second is an error-prevention mechanism, letting the user confirm that they really want to complete the transaction.

186. Further, Phillips discloses receiving payment method selection user input. EX1005, [0036]-[0041]. The user can provide approval of an automatically selected card by entering a PIN. *Id.*, [0059], [0066]. The user can also cancel (deny) the transaction or adjust the transaction payment (change payment type). *Id.*, [0068].

187. Casey similarly discloses approving and denying the transaction such as by entering “a PIN to verify the payment instrument” or swiping in different directions to confirm or deny the transaction. EX1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49.

188. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 9 of the '579 Patent as a whole obvious to a POSITA.

9. Claim 11

[11] The method of claim 1, further comprising completing the transaction on the electronic device, wherein the completing further comprises: receiving an authorization input on the electronic device from a valid device user, in

response to at least one of a set of exceptional conditions comprising: the electronic device leaving the proximity of the NFC recipient; the incomplete identifying of a valid device user; the electronic device leaving the user's possession; the electronic device leaving the proximity contact of the user; the electronic device leaving the grasp of the user; a biometric sensing the electronic device leaving the possession of a user since a last user validation; the transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration; a card issuing authority requesting a security check; and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; continuing with the default payment method; selecting an alternate payment account; inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.

189. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

190. Claim 11 requires receiving an authorization input on the electronic device from a valid device user, in response to at least one of a set of claimed “exceptional conditions,” including “presenting the user with at least one of a set of selectable options,” which set includes selecting an alternate payment account or inputting an approval authorization to complete the transaction.

191. Phillips discloses the additional limitation of claim 11. In particular, in response to an exceptional condition, e.g., “a transaction in an amount above a certain limit,” the device receives an authorization input from the user approving an “automatically selected card” by entering a PIN and the device presents a selectable option for the user to select “a different choice of card account.” :

The user acknowledges 1012 in FIG. 10 that the automatically selected card is correct by entering 1014 her personal identification number (PIN) by use of the numeric keypad 112 of the mobile phone 100. In some embodiments, the mobile phone may operate such that a payment transaction (or at least a transaction in an amount above a certain limit) is not enabled unless the PIN had been recently entered into the phone. The mobile phone user/shopper then taps 1016 her mobile telephone on the POS reader associated with the POS terminal (cash register) in the retail store to consummate the transaction. Consummating the transaction may include the mobile phone wirelessly transmitting the selected payment card account number to the proximity/contactless reader, and exchanging other data between the reader and the contactless payment application/circuitry of the mobile phone. In accordance with some conventional practices, the mobile phone may cryptographically generate a dynamic security code (CVC3) for the transaction and transmit the dynamic security code to the reader.

EX1005, [0059].

192. Further:

Referring again to FIG. 10, if in step 1012 the mobile phone user decides, after viewing the large image of the automatically-selected card account, that she does not wish to make a purchase, then she can select 1020 the “Cancel” command icon 1116 by actuating soft-key 120 (FIG. 1) and the process ends 1022. However, if in step 1012 the mobile phone user wishes to complete the payment transaction with another payment card account then instead of actuating the Cancel command 1116, she can then select the “Change” command icon 1114 by pressing the soft-key 118 (FIG. 1) to display 1022 the payment card images (FIG. 8) to make a different choice of card account. The process then proceeds to step 1024, wherein if a choice is made then that payment card account is displayed 1010 as a large image of the card account and the user proceeds as explained above to consummate the transaction. If, in step 1024 the user does not make a choice of another payment card account, then the process may idle as shown by branch 1026 for a predetermined amount of time after which the mobile telephone may, for example, exit to display the main menu screen. In addition, if in step 1008 there is no match found to the merchant identifier and any of the automatic card use criteria, then the process continues to step 1022 wherein the shopper is presented with card account images and can select a payment card account to utilize in the transaction, as explained above.

EX1005, [0061], *see also id.*, [0066], [0068].

193. Casey similarly discloses approving and denying the transaction such as by entering “a PIN to verify the payment instrument” or swiping in different directions to confirm or deny the transaction. EX1006, 9:9-36, 13:24-51, 14:12-49, FIGs. 5-8. Confirming the transaction completes the transaction. *Id.*, 10:47-53.

194. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 11 of the '579 Patent as a whole obvious to a POSITA.

10. Claim 12

[12] The method of claim 1, further comprising: subsequent to the priming operation, offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display, including at least one of: a last four digits of a payment account number portion; a last four digits of a device account number portion; an expiration date; a card issuer icon; a bank logo; a card processing network logo; a card image; a card payment network icon; graphical images associated with the payment account; accepting a user input selection of a payment option, from said payment options, via said touch-screen display; and proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options.

195. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

196. As discussed in connection with limitation [1f], *supra*, Royyuru's "Payment Cards" sub-menu" allows "selection of the payment card account that corresponds to the payment card represented by the card-face image." EX1005, [0036]-[0041], FIG. 8; 9:58-10:2, 12:46-65. The displayed cards include expiration dates, card issuer icons, bank logos, card images, etc. EX1005, [0036]-[0041], FIG. 8. "[T]he user may be required to enter a PIN or code before selecting a payment

card” and therefore the card selection menu is presented subsequent to the priming operation. EX1005, [0039]. This action is subsequent to the priming operation because priming is required to activate the payment function.

197. Phillips also discloses that the device will proceed with a default payment option (“automatically selected card”) if the user does not select an alternative payment method. EX1005, [0059], [0066], [0017], [0029]. The default card is identified based on previously entered user criteria. *Id.*

198. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 12 of the ’579 Patent as a whole obvious to a POSITA.

11. Claim 15

199. Claim 15 contains limitations similar to those of claim 1, and would have been obvious in view of the combination of Royyuru, Phillips, and Casey, for the same reasons as articulated above with respect to claim 1, and as supplemented below.

[15pre]: A method of performing a transaction, the method comprising:

200. The preamble of claim 15 is identical to the preamble of claim 1. Hence, *see supra*, [1pre].

[15a]: receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient

proximity communication request to an NFC interface of the electronic device:

201. Limitations [1a], [1d] and [1e] recite:

[1a] **receiving an input at an electronic device**, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises

[1d] a **near field communications (NFC) interface** coupled to the processor;

[1e] **receiving a request for a transaction payment at said electronic device via the NFC interface**

202. Hence, *see supra*, [1a], [1d], [1e].

[15b]: displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device

203. Limitations [1c], [1f] and [9b] recite:

[1c] a **touch screen display** coupled to the processor

[1f] **displaying, on the touch-screen display**, images of: a **card issuer payment method selection**, including a last 4-digit partial number of a card issuer supplied account number of a payment card

[9b] (abridged) displaying, on the display, at least one information of a set of information comprising: . . . **a plurality of selectable payment accounts**; a payment request; transaction information; a payment amount...

[15c]: receiving, from a valid device user, a payment selection and approval authorization input on the electronic device

204. Limitations [1f], [9a], [9c], and claims [11]-[12] recite:

[1f] displaying, on the touch-screen display, images of: a **card issuer payment method selection**, including a last 4-digit partial number of a card issuer supplied account number of a payment card

[9a] (abridged) The method of claim 1, further comprising:
obtaining, by the electronic device, **a user payment approval...**

[9c] **receiving a user input of** at least one user action, from a set of actions comprising: **a payment method selection**; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.

[11] (abridged) completing the transaction on the electronic device, wherein the completing further comprises: **receiving an authorization input on the electronic device from a valid device user, . . . inputting an approval authorization**; inputting a transaction denial; and inputting an adjustment of the transaction payment . . .

[12] (abridged) subsequent to the priming operation, **offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display . . .**

205. A “user payment approval” can only be obtained from a valid device user. Hence, *see supra*, [1f], [9a], [9c], [11], [12].

[15d]: generating a limited-use number at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information

206. Limitation [1i] recites:

[1i] generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information

207. Hence, *see supra*, [1i].

[15e]: transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface

208. Limitation [1j] recites:

[1j] transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface

209. Limitation [15e] is nearly identical to [1j]. Hence, *see supra*, [1j].

[15f]: obtaining a user payment approval through at least one user-interface of the electronic device, of a set of user-interfaces comprising: a touch-screen interface of the touch-screen display user-interface; a touch ID button; input buttons; a touch key-pad; an optical sensor array; a sensor array operable to recognize a swiping of a recognized user skin over the sensor array; a motion detection unit; an accelerometer; a biometric user-sensor; a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient

210. Limitation [9a] recites:

[9a] obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user

211. Limitation [15f] is nearly identical to [9a]. Hence, *see supra*, [9a].

[15g]: displaying on said display at least one of a set of information comprising: transaction information; merchant information; a time; a location of the transaction; a payment bank logo; a card issuer icon; a payment card image; an amount

212. Limitations [1g], [1h] and [9b] recite:

[1g] a card logo

[1h] other iconography of the payment card

[9b] (abridged) **displaying, on the display, at least one information . . . comprising: . . . transaction information, a payment amount, a time; a location; . . . a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography**

213. Limitation [1g] is a subset of limitations [1g], [1h] and [9b]. Hence, *see supra*, [1g], [1h] and [9b].

[15h]: receiving a user input providing for at least one transaction action, from a set of actions comprising: approving a transaction; denying a transaction; and adjusting a transaction.

214. Limitations [9a], [9c] and claim [11] recite:

[9a] (abridged) obtaining, by the electronic device, a user payment approval . . .

[9c] (abridged) **receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.**

[11] (abridged) completing the transaction on the electronic device, wherein the completing further comprises: **receiving an**

authorization input on the electronic device from a valid device user, ... and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; . . . **inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.**

215. Limitation [15h] is a subset of limitations [9a], [9c] and claim [11].

Hence, *see supra*, [9a], [9c] and claim [11].

216. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 15 of the '579 Patent as a whole obvious to a POSITA.

12. Claim 16

[16] The method of claim 15, further comprising: visually conveying on the touch-screen display user-interface, information regarding the transaction, including at least one of: a payment amount requested; an indication requesting an authorization input; an indication of an authorization success; an indication of an authorization failure; an option to retry a transaction; an option to retry a user authorization; an option to retry validating a user identity; an indication of a payment successfully completed; an indication of a payment failure; and an indication of a payment retry option.

217. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 15 of the '579 Patent as a whole obvious.

218. The device of the Royyuru-Phillips-Casey combination has a touchscreen display. *Supra*, limitation [1c]; EX1004, [0021]; EX1011, [0006];

EX1005, [0018]; EX1006, 3:10-19. Matter displayed on a screen is “visually conveyed.” As described by Casey, the device presents a confirmation screen displaying “details about the sales order, such as the item price” and “a prompt asking a user to confirm the payment transaction.” EX1006, 13:24-51. The device “prompt[s] the user to move a graphical element 180 to confirm the payment transaction.” *Id.*



EX1006, FIG. 5; *see also* FIGs. 6-8

219. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 16 of the '579 Patent as a whole obvious to a POSITA.

13. Claim 17

[17] The method of claim 15, further comprising: visually presenting on the touch-screen display user-interface, a plurality of payment options, including at least one of a set

of payment method information for each payment option, the set comprising: a card image; a payment issuer logo; partial payment account numbers; a card payment network icon; a graphical image-encoding of a users payment account information; an amount of currency; an account balance; a credit limit; an amount of remaining credit; an amount of cryptocurrency; a cryptocurrency server network; and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface.

220. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 15 of the '579 Patent as a whole obvious.

221. The prior art need only disclose one of the “plurality of payment options.” Such an option is recited in each of [1f], [1g], [1h], [9b], [11]-[12], *q.v.*

222. The limitation “receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface” is contained in [9c], “receiving a user input of at least one user action, from a set of actions comprising: a **payment method selection**; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.” Hence *see supra*, [9c]. (The touch screen interface is recited in [9a], *q.v.*)

223. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 17 of the '579 Patent as a whole obvious to a POSITA.

14. Claim 18

[18] The method of claim 15, further comprising: receiving a priming operation at the electronic device for priming

the electronic device for imminent payment, wherein the priming operation causes the electronic device to successfully identify the user through completing at least one user-validation, of a set of user validations comprising: a touching of the device by an identified user; a user entry of a valid passcode; a user entry of a valid PIN; a swiping of a recognized user skin over a sensor array of the electronic device; a correct user swiping or gesturing on a touch sensor array of the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motions of the electronic device; a skin-contact sense of a valid user; and a device biometric recognition of a valid user.

224. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 15 of the '579 Patent as a whole obvious.

225. Limitation [1a] and claim [8] recite:

[1a] receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises:

[8] (abridged) wherein the priming operation comprises one operation of the set of operations comprising: . . . a touch ID sensor touch; a touch-screen touch; a touch-input sequence; a gesture or swipe over a sensor-array; a skin-contact sense; an optical-sensor array sense; an electronic device tap; a sequence of motions of the electronic device; a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation; and, further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a touching from an identified valid user; a user entry of a valid passcode; a user entry of a valid PIN; swiping of a recognized user skin over a device sensor array; a correct user swiping or gesturing on the electronic device; a correct sequence of

user taps on the electronic device; a correct user sequence of user motioning of the electronic device; **a skin-contact sensing of an identified user**; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.

226. Hence, *see supra*, [1a] and [8].

227. Therefore, in my opinion, the combination of Royyuru, Phillips and Casey would have rendered claim 18 of the '579 Patent as a whole obvious to a POSITA.

15. Claim 19

228. Claim 19 contains limitations similar to those of claim 1, and would have been obvious in view of the combination of Royyuru, Phillips, and Casey, for the same reasons as articulated above with respect to claim 1, and as supplemented below.

[19pre]: An electronic device comprising:

229. Each of Royyuru, Phillips, and Casey discloses “a mobile device,” which is an “electronic device.” EX1004, [0021]; EX1005, [0017]; EX1006, 3:10-19.

[19a]: at least one processor

230. Each of Royyuru, Phillips, and Casey discloses “a mobile device” having at least one processor. EX1004, [0021]; EX1005, [0017]; EX1006, 3:10-19.

[19b]: a memory coupled to the at least one processor

231. Each of Royyuru, Phillips, and Casey discloses “a mobile device” having at least one processor and a memory coupled to the processor. EX1004, FIG. 3 (memory 310); [0007]; EX1005, [0020]; EX1006, 6:15-25.

[19c]: a display operable to present a visual user-interface comprising device inputs; display output

232. Each of Royyuru, Phillips, and Casey discloses a touch screen display that comprises inputs and outputs. *See supra*, [1c].

[19d]: a device input

233. It is unclear what is meant by “a device input,” as the act of inputting information to a device is not an apparatus element. I believe a POSITA would understand “a device input” to mean “an input device,” such as the “device input button” of claim 9.

234. With this understanding, each of Royyuru, Phillips, and Casey discloses an input device. EX1004, [0040], [0021]; EX1011, [0006] (incorporated in EX1005); EX1005, [0018].

[19e]: an NFC interface operable to receive a transaction request when in proximity to an NFC recipient

235. Limitation [1c] recites “a near field communications (NFC) interface coupled to the processor.” Limitation [1e] recites “receiving a request for a transaction payment at said electronic device via the NFC interface.” Hence, *see supra* [1c].

[19f]: wherein the processor is operable to execute a program to implement a method comprising

236. Each of Royyuru, Phillips, and Casey discloses a processor operable to execute a program. *See supra* [1b].

[19g]: accepting a priming action of the electronic device by an identified device user, from the device input

237. The combination provides accepting a priming action of the electronic device by an identified device user, from the device input. *See supra*, [1a], [7]-[8].

[19h]: enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user

238. As Royyuru describes, in the combination “a consumer can use the presentation instrument **305** to *initiate a transaction* at the POS device **330**, for example by *scanning or tapping the presentation instrument 305 on or near the POS device 330* at the time of payment for a purchase.” EX1004, [0044]. In another example, “[p]assing or tapping the presentation instrument near the POS device 330 can trigger” the device to generate the dynamic PAN and DTC and provide them “to the merchant system 340, e.g., via the NFC module 325 of the presentation instrument and corresponding NFC module 335 of the POS device 330” to facilitate the transaction. *Id.*, [0047]. After the priming action, the device is enabled for imminent performance of a payment action.

239. Phillips and Casey provide additional disclosures that, in some arrangements of the combination, the electronic device is enabled for payment by priming actions such as user entry of a valid PIN or correct user swiping. EX1005, [0059] (“a payment transaction...is not enabled unless the PIN had been recently entered”), [0062], [0066], [0070]; EX1006, 9:9-36 (“the device 10 may request...a PIN to verify the payment instrument”), 12:64-13:51 (“...prompt the user to move a graphical element 180 to confirm the payment transaction”), FIGs. 5-8.

[19i]: displaying a summary of selectable payment account options on the display

240. *See supra*, [1f]-[1h].

[19j]: receiving a payment selection and approval authorization from a valid device user via the device input

241. The combination of Royyuru, Phillips, and Casey provides receiving a payment selection and approval authorization from a valid device user via the device input. *See supra*, [1f], [9a], [9c], [11]-[12].

[19k]: responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use in place of card issuer payment information

242. *See supra*, [1e] and [1i]. Additionally, Royyuru discloses generating a limited-use payment information for use in place of a card issuer supplied payment information in the form of both the DTC and dynamic PAN.

243. Phillips discloses that, in the predictable Royyuru-Phillips-Casey combination, the verification cryptograms (DTC and dynamic PAN) are generated in response to receiving an NFC transaction payment request. Similar to Royyuru, Phillips discloses that the device interacts with the POS terminal via NFC. EX1005, [0023]. Phillips discloses that, in the combination, the transaction is initiated when “the mobile device...receives 1302 a payment request.” EX1005, [0072]. The request can come in the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057]; *see also* EX1006, 8:52-9:8 (“receiving information through...the NFC device...may include a request for payment”); FIGs. 5-8. “The interrogation signal stimulates the mobile telephone 100 to exchange wireless RF communications with the merchant proximity reader,” thus initiating the transaction. EX1005, [0057].

244. Phillips goes on to disclose that, after receiving these interrogation signals and receiving a merchant identifier, the user device automatically selects a user payment card or allows the user to select a different payment method. EX1005, [0057]-[0058]. Phillips further discloses that the device “cryptographically generate[s] a dynamic security code (CVC3) for the transaction and transmit[s] the dynamic security code to the reader.” *Id.*, [0059]. Because the transaction is initiated in response to a request from the POS device, a POSITA would have recognized

that this cryptographic dynamic security code is generated responsive to receiving the NFC transaction payment request.

245. Therefore, because Royyuru discloses that the DTC and dynamic PAN are dynamically generated responsive to the device “detect[ing] initiation of the transaction” (EX1004, [0047], [0009]), a POSITA would have recognized that in the combination of Royyuru with Phillips and Casey, based on Phillips’ disclosure that the transaction is initiated responsive to receiving the payment request at the device (EX1005, [0072], [0023], [0027], [0057]-[0059]), the device generates the DTC and dynamic PAN responsive to receiving the NFC transaction payment request.

[19l]: wherein the NFC interface is operable to transmit said payment information from said electronic device to the NFC recipient of the transaction

246. Limitation [1j] recites: “transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface.” Hence *see supra*, [1j].

[19m]: wherein further the processor is operable to cause the display to visually convey a status of the transaction.

247. Limitation [1k] recites: “visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.” Hence *see supra*, [1k].

248. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 19 of the ’579 Patent as a whole obvious to a POSITA.

16. Claim 20

[20] The electronic device of claim 19, wherein the method further comprises: receiving the priming action of a valid user via the device input, wherein the device input comprises at least one of a set of device inputs comprising: a button; a touch ID button; a touch sensor array; a touch key-pad; a motion detection unit; an accelerometer; an optical sensor array; and identifying a valid device user through an input detection, selected from at least one of a set comprising: a correct passcode entry sequence; a touch ID recognition of a known user; a biometric recognition of a valid user; a biometric sensing of a valid users skin; a biometric detection that the electronic device continuously remains in contact with a valid user; and receiving a correct user response input, from a security challenge presented on the display.

249. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 19 of the '579 Patent as a whole obvious.

250. *See supra*, [1a], [1c], [7]-[8], [11], [12]. A POSITA would have recognized that a touchscreen provides or at least renders obvious a touch sensor array and a touch key-pad and that a valid PIN entry, as described above with respect to limitations [1a] and [9c] and claims [7]-[8] and [11]-[12] provides a correct passcode entry sequence and a correct user response input from a security challenge (“an ‘Enter PIN’ prompt”). EX1005, [0058]-[0059] (describing PIN entry using a “numeric keypad” of the touchscreen).

251. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 20 of the '579 Patent as a whole obvious to a POSITA.

17. Claim 21

[21] The electronic device of claim 19, wherein the memory is accessible to the processor, wherein said memory comprises a static device-specific device account number of limited-use that originates from a card issuing authority and is limited to use by the electronic device in place of a card issuer account information, wherein further said static device-specific device account number has an expiration date of limited duration of validity, and wherein the generating a limited-use payment information comprises the processor generating said limited-use payment information by combining said static device-specific device account number, said device account expiration date, when said issuer payment account method is selected.

252. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 19 of the '579 Patent as a whole obvious.

253. Royyuru discloses that the “memory [is] communicatively coupled with and readable by the processor.” EX1004, [0007]. As discussed with respect to claim [4], *supra*, Royyuru discloses a static device-specific device account number of limited-use in the form of the IKCV stored on the device. The IKCV is “generated when *each card (device) is being customized*” and is generated by the payment processor *or issuer* based on the PAN and “institution key of the issuer of the account.” EX1004, [0057], [0046], [0032]-[0033], [0054]-[0055]. Royyuru also expressly refers to the “IKCV *of the device*.” *Id.* A POSITA would have therefore recognized the IKCV as a device account number because it is specific to the device and is based on payment account information. A POSITA would have further

recognized that, because it can be generated by the issuer and provided to the device, it is static and originates from a card issuing authority. *Id.* The IKCV is of limited-use because it “customized” for the specific device and can only be used in performing transactions using the associated device (and not other devices or payment devices). EX1004, [0057].

254. Royyuru also explains that the “expiration date” of the payment account is also used in generating the IKCV. EX1004, [0091]-[0096]. As would have been recognized by a POSITA, the IKCV has a limited time-duration of valid use because after the expiration date has expired, a new IKCV would need to be generated based on the new expiration date to match the valid account information having the new expiration date. Alternatively, it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use tied to the payment account expiration date so that an IKCV generated using an expired PAN could not be used for transactions. This would help ensure that the user’s account is still valid. *Id.*

255. The DTC is generated using one of the CKs (such as the IKCV) and the dynamic PAN is generated using the IKCV. EX1004, [0057], [0005]-[0009]. Both the DTC and the dynamic PAN are limited-use payment information. *Supra*, Element [1i]. Furthermore, Royyuru discloses that the “dynamic PAN can also be based on an undeterminable number.” *Id.*, [0033]. Royyuru also discloses “generat[ing] a dynamic PAN 326 based on the real PAN 316, the **card-level key**

315, and one or more factors from the payment device or the POS reader such as **unpredictable numbers** or counters.” *Id.*, [0051]. The undeterminable number can be a “number generated by the presentation instrument 305 or *received by the presentation instrument* 305.” *Id.* Royyuru indicates that one number received by and stored at the presentation instrument is the “expiration date” which, as described above, is the expiration date for both the real PAN and the IKCV generated using the expiration date of the account. EX1004, [0057], [0091]-[0096]. Therefore, the dynamic PAN is limited-use payment information generated in part based on combining the IKCV (static device-specific device account number) and the device account expiration date.

256. Similarly, the DTC is generated by combining values including “expiration date” and “the CK.” EX1004, [0057]. As previously discussed, the card-level keys (CKs) include the IKCV. *Id.*, [0057], [0006]; Therefore, the DTC is another example of limited-use payment information generated in part based on combining the IKCV (static device-specific device account number) and the device account expiration date.

257. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 21 of the ’579 Patent as a whole obvious to a POSITA.

18. Claim 22

[22] The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates from a card issuing authority and is for limited-use by the specific electronic device only; and wherein said static device-specific device account information is valid for a limited duration, and wherein the generating a limited-use payment information comprises the processor generating a one-time limited-use cryptogram number and combining said limited-use static device account information and said one-time use cryptogram number to produce the limited-use payment information.

258. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 19 of the '579 Patent as a whole obvious.

259. As discussed with respect to claims [21] and [4], *supra*, the IKCV is a limited-use device account number stored in the memory accessible to the processor that is valid for a limited duration (expiration date) or alternatively it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use. EX1004, [0007], [0057], [0046], [0032]-[0033], [0054]-[0057], [0091]-[0096].

260. The IKCV is a key and Royyuru discloses that the device stores numerous other “unique card level key[s] *stored on the device.*” EX1004, [0005]-[0007], [0032] (describing “a unique encryption key per card or other device” and “a unique, card-level key” each stored on the device), [0051], [0057], FIG. 3.

261. The DTC is generated using one of the CKs (such as the IKCV) and the dynamic PAN is generated using the IKCV. EX1004, [0057], [0005]-[0009]. Both the DTC and the dynamic PAN are a one-time limited-use cryptogram number. *Supra*, Claim [3]. The IKCV makes up part of the dynamic PAN and is therefore combined with the limited-use cryptogram number (the DTC) (as part of the device generated payment information. EX1004, [0057], [0005]-[0009]. Alternatively, the IKCV makes up part of the DTC and is therefore combined with the limited-use cryptographic number (the dynamic PAN) as part of the device generated payment information. EX1004, [0057], [0005]-[0009].

262. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 22 of the '579 Patent as a whole obvious to a POSITA.

19. Claim 23

[23] The electronic device of claim 19 further comprising a cryptographic processor operable to dynamically generate a one-time limited-use cryptogram number by cryptographically combining of at least one information accessible on the electronic device, selected from a set comprising: a sequence counter; a device account number; a device secret; device keys; card issuer keys; a time; an amount; an expiration date; a card security code; a location; merchant information; NFC recipient information; payment reader information; an online location; transaction information; payment information; device information; user information; an email address; a user identification entry; a hash of transaction information; and a hashed record of transactions, and wherein said cryptogram number is operable to be used in place of at least a portion of a card issuer payment information, in a payment transaction.

263. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 19 of the '579 Patent as a whole obvious. It was well known even by 2005 to include a cryptographic processor in a mobile phone to perform computation-intensive cryptographic operations. *See, e.g., EX1015.*

264. Therefore, in my opinion, the combination of Royyuru, Phillips, and Casey would have rendered claim 23 of the '579 Patent as a whole obvious to a POSITA.

B. Ground 1B: Claim 3 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, and Spodak

1. Claim 3

[3] The method of claim 1, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the card issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count and at least one information of a set of information comprising: a device account number; device identifiers; device secrets; device keys; payment issuer secrets; payment issuer keys; user information; a time; and transaction information; and wherein further, said dynamically generating the cryptogram number results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction.

265. In my opinion, the combination of Royyuru, Phillips, Casey, and Spodak renders obvious as a whole claim 3 of the '579 Patent for at least the reasons discussed below.

266. Royyuru discloses generating a “Dynamic Transaction Cryptogram (DTC)” that is “valid for a single transaction.” EX1004, [0005], [0033], [0053], Abstract. This cryptogram is generated based on an Application Transaction Counter (ATC) and an “unpredictable number,” and then “encrypting them.” *Id.*, [0057], [0084]. The “unpredictable number” can be “a time of day.” *Id.*, [0047]. Therefore, in my opinion, Royyuru discloses dynamically generating the cryptogram by “cryptographically combining a device transaction sequence counter count and at least one [of] ... a time.”

267. Royyuru discloses that the ATC “increments for each transaction,” *Id.*, [0057], which, in my opinion, discloses that generating the cryptograms “results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction,” as claimed.

268. In my opinion, a POSITA would have been prompted to apply the teachings of Spodak to the Royyuru-Phillips-Casey combination. As Royyuru discloses, “a consumer can use the presentation instrument 305 to initiate a transaction at the POS device 330, for example by scanning or tapping the presentation instrument 305 on or near the POS device 330 at the time of payment for a purchase.” *Id.*, [0044]. The POS device 330 can be “any devices capable of reading a magnetic stripe, an RFID chip, NFC communications, or other information from a mobile device, contactless device, card, etc.” *Id.*, [0024].

269. In my opinion, having looked to Royyuru’s disclosure of scanning the presentation instrument at a POS device that is capable of reading a magnetic stripe (*Id.*, [0024], [0044]), a POSITA would have looked to Spodak for how to communicate with such POS devices. Similar to the Royyuru-Phillips-Casey combination, Spodak discloses a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002]. The universal card is similar to a mobile device such as a phone except that the universal card is shaped like a credit

card. *Id.*, [0027], [0034]. The universal card includes both a dynamic magnetic stripe and a short range transceiver. *Id.*, [0033], [0035]. The universal card can use the dynamic magnetic stripe to communicate with a traditional credit card magnetic stripe reader, and the short range transceiver to communicate with a contactless payment terminal such as via NFC. *Id.*, [0088]-[0089].

270. To emulate the magnetic stripe and “authenticate the transaction with the card issuer,” the universal card generates a “dynamic authentication value,” which discloses the claimed “cryptogram number.” *Id.*, [0094]. Spodak discloses that “the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value,” *id.*, which, in my opinion, discloses that this value is generated “for use by the electronic device in place of a card validation value originated from the card issuer” as claimed. The dynamic authentication value is generated based on “a random number” and “a transaction counter.” *Id.*, [0094]. Because the “dynamic authentication value is unique for every transaction,” *id.*, in my opinion, generating the dynamic authentication value “results in a one-time limited-use number” as claimed.

271. Therefore, in my opinion, for the Royyuru-Phillips-Casey combination to communicate with a magnetic stripe reader, a POSITA would have been motivated to incorporate the dynamic magnetic stripe from the universal card of

Spodak into the Royyuru-Phillips-Casey combination. *Id.*, [0035], [0088]-[0089]. The improved device would be compatible with a greater number of POS devices: those that communicate via a magnetic stripe reader and those that communicate via short range wireless communications such as NFC.

272. In my opinion, to the extent that the Royyuru-Phillips-Casey combination does not disclose generating a cryptogram distinctly from the limited-use payment information in claim 1, a POSITA would have applied Spodak to improve the device by generating the dynamic authentication value to enable the device to conduct transactions with both a magnetic stripe reader and a contactless payment terminal. *Id.*, [0088]-[0089], [0094]. The improved device would be compatible with a magnetic stripe reader by generating the dynamic authentication value for use in place of a card validation value (CVV) originating from the card issuer. *Id.*, [0094]. In my opinion, a POSITA would have been motivated to incorporate this feature of generating the dynamic authentication value so that “there would be no need to reconfigure the terminal with the magnetic stripe reader because it would already be configured to read a value from the static CVV field location.” *Id.*, [0094].

273. In my opinion, to the extent that Spodak does not disclose generating the dynamic authentication value cryptographically, a POSITA would have further been motivated to apply Royyuru’s disclosure about encrypting its dynamic

transaction cryptogram to Spodak to encrypt its dynamic authentication value. EX1004, [0058]-[0060], [0084]. A POSITA would have been motivated to encrypt Spodak's dynamic authentication value because like Royyuru's dynamic transaction cryptogram, Spodak's dynamic authentication value is used to securely conduct a transaction. *Id.*, [0047], [0057], [0084]; EX1009, [0094]. In my opinion, to the extent that Spodak does not disclose incrementing its transaction counter, a POSITA would have further been motivated to apply Royyuru's disclosure about incrementing its Application Transaction Counter (ATC) to Spodak to increment its transaction counter. In my opinion, a POSITA would have been motivated to increment Spodak's transaction counter by virtue of it being a counter, and because both Royyuru's dynamic transaction cryptogram and Spodak's dynamic authentication value are generated based on a transaction counter and a random/unpredictable number. *Id.*, [0047], [0057], [0084]; EX1009, [0094].

274. Furthermore, in my opinion, a POSITA would have recognized that application of Spodak's teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. In my opinion, a skilled person would have appreciated that the above-described combination would have merely involved a combination of known prior art technologies (e.g., known devices for conducting

transactions via both a magnetic stripe reader and a contactless payment terminal) according to known methods (e.g., known process for securing payment information during the transactions) to yield the predictable result of a device that could securely conduct transactions with both a magnetic stripe reader and a contactless terminal.

275. Therefore, in my opinion, the combination of Royyuru, Phillips, Casey, and Spodak would have rendered claim 3 of the '579 Patent as a whole obvious to a POSITA.

C. Ground 1C: Claim 5 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, Spodak, and Giordano

1. Claim 5

[5]: The method of claim 1, further comprising: generating a limited-use security number for use in place of a card issuer card security code by cryptographically combining information from at least one of a set of information comprising: user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; transaction information; and displaying the limited-use security number on the user-interface of the display.

276. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

277. Spodak’s generation of the dynamic authentication value in the Royyuru-Phillips-Casey-Spodak combination renders obvious “generating a limited-use security number” and the remaining features of this “generating” step for the reasons discussed in Ground 1B, *supra*, Element [3]. As for the “displaying” step, Spodak discloses that its universal card includes a display for displaying “an account number” or “any other information.” EX1009, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A. In my opinion, a POSITA would have understood that “information” can be the “authentication value” that satisfies the claimed “limited-use security number.” Having appreciated that the universal card includes a display, a POSITA would have further looked to Giordano to display the claimed number.

278. Giordano describes a mobile payment system for a person-to-merchant (P2M) payment service “to make payments...without having to share any confidential account information.” EX1010, [0028].

279. Similar to Royyuru and Spodak, Giordano describes a mobile payment device that generates an “alias” for each transaction based on information unique to the device and other information related to the transaction. *Id.*, [0028], [0029], [0033], [0080]. Giordano further discloses “prompt[ing] the user to approve a random or default static alias.” *Id.*, [0032]. The user can select, generate, or modify an alias “using the P2M application,” a “web-based module,” or a “banking

application.” *Id.*, [0032], [0038], [0066]. The “alias is only available for a limited time or limited number of transactions before it expires and must be changed.” *Id.*, [0032]. To manage the alias, the user can use a web browser or the P2M application on a device that displays graphical user interfaces on its display. *Id.*, [0033], [0059], [0066].

280. In my opinion, a POSITA would have been prompted to apply the teachings of Giordano to the Royyuru-Phillips-Casey-Spodak combination to provide a mobile payment system in which the generated limited-use security number (e.g., the combined dynamic authentication value and alias) is displayed on the device for the user to approve or modify the security number. *Id.*, [0032], [0038]. Displaying the security number on the device would allow the user to conveniently and quickly manage it because it is only available for a unique transaction (EX1009, [0094]) or a limited time or limited number of transactions (EX1010, [0032]), which increases the utility of the device and provide for more secure transactions by allowing the user to know when the security number is expected to expire and require modification. In my opinion, a POSITA would have recognized that the application of Giordano’s teachings to the Royyuru-Phillips-Casey-Spodak device is merely the application of known techniques to known devices ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification.

281. Therefore, in my opinion, the combination of Royyuru, Phillips, Casey, Spodak, and Giordano would have rendered claim 5 of the '579 Patent as a whole obvious to a POSITA.

D. Ground 1D: Claims 10 and 14 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, and Deibert

282. In my opinion, the combination of Royyuru, Phillips, Casey, and Deibert renders obvious as a whole claims 10 and 14 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Deibert with the Combination of Royyuru, Phillips, and Casey

283. All four references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS terminals. Deibert describes a mobile payment system with a disabling feature. EX1012, Abstract. The user can set “a predetermined timeout time such that the mobile payment application is disabled after the predetermined timeout time has elapsed” to “help prevent the accidental transmittal of [payment] information.” *Id.*, [0009], [0023]. Deibert discusses manual activation of a mobile payment application and multiple techniques for disabling the mobile application to prevent unintentional transmittal of payment information, including completion of a transaction, manual disabling based on user input, and expiration of a predetermined timeout time. *Id.*, [0023]-[0025], [0058]-[0059].

284. A POSITA would have been prompted to apply the teachings of Deibert to the Royyuru-Philips-Casey combination to include multiple techniques for disabling a payment priming operation (including through completion of a transaction, manual user input, and expiration of a timeout period) to “help prevent the accidental transmittal of information,” provide increased functionality of allowing the user to intentionally return the device to an idle state, and to “allow[] the phone to have full contactless card functionality, while removing limitations.” EX1012, [0023]-[0025], [0061]. This modification also “minimize[s]” user concern and hesitancy regarding mobile payment transactions, thus increasing user satisfaction. *Id.*, [0061]; Such a modification could also save power by decreasing the amount of time that the NFC circuit is actively transmitting payment information and increase ease of use by providing mechanisms for disabling payment priming that don’t require user interaction. Furthermore, a POSITA would have recognized that application of Deibert’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification.

2. Claim 10

[10]: The method of claim 1, further comprising: activating an NFC communication for a limited duration of time responsive to the electronic device priming; and responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction.

285. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

286. Like Royyuru, Deibert similarly discloses using NFC to facilitate communications between the user device and merchant terminal during mobile payment transactions. EX1012, [0019], [0040]; EX1004, [0022], [0044], [0047]. Deibert describes manually activating an application and in response “the mobile phone will transmit payment information.” EX1012, [0023]. A POSITA would have recognized this activation of the application to transmit payment information as a priming action. The communication of the transaction information is limited to “a predetermined timeout time” such that “[i]f no payment transaction occurs within the predetermined timeout time, then after the predetermined timeout time, the mobile payment application on the phone will automatically disable so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]. The manual activation can include “entering a password.” *Id.*, [0057]. A POSITA would have understood that terminating the mobile payment application provides, or at least renders obvious, terminating the NFC communication and aborting the transaction.

287. Therefore, in my opinion, the combination of Royyuru, Phillips, Casey, and Deibert would have rendered claim 10 of the '579 Patent as a whole obvious to a POSITA.

3. Claim 14

[14]: A method of claim 1, wherein the priming operation is input after at least one of: a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device, and validating a user passcode entry on the touch-screen display of the electronic device; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.

288. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

289. Both Phillips and Casey disclose requiring a PIN to access the payment application/functionality or prior to selecting a specific payment method. EX1005, [0035], [0038]-[0039], [0066]; EX1006, 9:9-36. A POSITA would have recognized that a user PIN is a type of passcode and therefore entry of the PIN is a "passcode entry" and thus discloses validating a user passcode entry on the touch-screen display of the electronic device. A POSITA would have further recognized that user selection of a payment method provides a priming operation after entry of the PIN/passcode. Deibert similarly describes requiring "entering a password into the mobile phone application, in order to authenticate the consumer **30** and prevent

fraud.” EX1012, [0057], [0049] (“user is prompted to enter a password”). Deibert describes further priming operations after entry of the password, including manual activation of the payment application after expiration of a timeout period without requiring additional password entry “because the consumer has already been authenticated by entering the password the first time.” EX1012, [0058], [0023] (describing that the user “*manually* select[s] the mobile phone application *each time* before making a purchase). In another example, Deibert describes that after the payment application is opened (which can require entry of a password), the device requires a further priming operation of selecting the “pay functionality of the mobile payment application” to prime the device “to engage in a payment transaction.” EX1012, [0060], [0057].

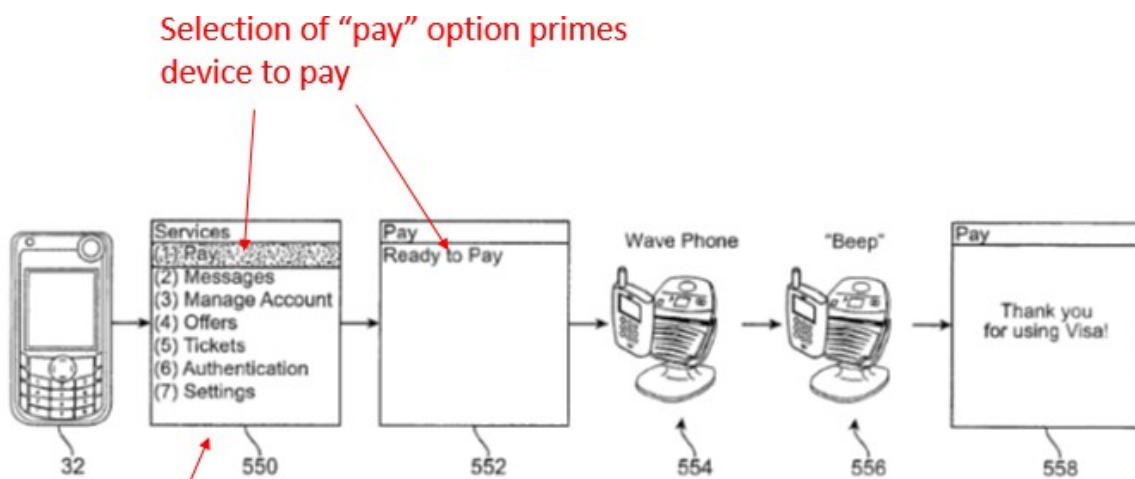


FIG. 7

Mobile payment application open (after entry of password)
Id., FIG. 7, [0057], [0060].

290. Furthermore, a POSITA would have recognized that payment priming is a type of device priming. Deibert discloses disabling a device priming on further button pressing, stating that “the consumer can manually disable the mobile phone application, thereby returning the mobile phone to the idle state.” EX1012, [0024]. Deibert further teaches that “[i]f no payment transaction occurs within the predetermined timeout time, then *after the predetermined timeout time, the mobile payment application on the phone will automatically disable* so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]. Additionally, [o]nce a transaction has occurred, the mobile phone can go back to the idle state.” *Id.*, [0024], [0059]-[0060].

291. Therefore, in my opinion, the combination of Royyuru, Phillips, Casey, and Deibert would have rendered claim 14 of the '579 Patent as a whole obvious to a POSITA.

E. Ground 1E: Claim 13 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey, Deibert, and Power

292. In my opinion, the combination of Royyuru, Phillips, Casey, Deibert, and Power renders obvious as a whole claim 13 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Power with the Combination of Royyuru, Phillips, Casey, and Deibert

293. All five references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS terminals. Further, all five references are concerned with security of wireless payment transactions. EX1004, [0004]; EX1005, [0035], [0038], [0062]; EX1006; 12:66-13:15; EX1012, [0004]; EX1016, 1:7-28. In particular, Deibert at [0004] addresses the problem of unauthorized “sniffing” of data from contactless payment devices.

294. A POSITA would have been motivated to adopt a selection of security mechanisms to enhance the security of the combination of Royyuru, Phillips, Casey, and Deibert based on the teachings of Power. As discussed above, Power teaches a number of techniques for activating the wireless payment device only for an imminent transaction when the payment device is in physical contact with the user. EX1016, 1:58-67. This can be done using one or more of a resistive sensor, a capacitive sensor, or a pressure sensor for sensing that the user is holding the payment device. *Id.*

295. A POSITA would have applied these teachings regarding only activating the device for a wireless payment transaction based on the teachings of Power to the combination of Royyuru, Phillips, Casey, and Deibert to “protect” transaction information from being inadvertently transmitted when the user does not

intend to conduct a financial transaction. EX1016, 2:47-3:5. This additionally level of security would have further helped to prevent unintended or fraudulent charges to the user's payment cards while "increas[e/ing] security." *Id.* Furthermore, such protections are not overly burdensome and provide "ease of use" because the user only needs to make physical contact with the card to maintain the priming state. *Id.*

2. Claim 13

[13]: A method of claim 1, wherein the priming operation comprises: a button double press; and a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation; and further comprising: denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user, until after successfully re-validating a user; and wherein re-validating a user requires a correct user passcode re-entry; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.

296. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

297. Regarding the additional limitations of claim 13, Phillips discloses priming (preparing the device to transmit payment information) through selection of a "card accounts" option from menu 700 followed by selection of a displayed payment option. EX1005, [0036]-[0037], FIGs. 7-8. These menu button selections would have been conducted via the "select button" disclosed by Phillips in at least

some embodiments. EX1005, [0033]. This sequence of menu selections using a button falls within the disclosure of a button double press in the '579 Patent. EX1001, 9:64-10:3, 17:19-23. The '579 Patent does not disclose pressing the same button twice, so I understand a “button double press” could involve pressing the same button twice, or a sequence of two different buttons.

298. Furthermore, a POSITA would have applied the teachings of Power to Royyuru-Phillips-Casey-Deibert to require biometric sensing of the device continuously remaining in contact of the valid user (e.g., using Power’s capacitive sensor) and disabling the priming operation when the device is not continuously in contact with the user. Power teaches that the device “detects a presence or an absence of a gating signal.” EX1016, 2:1-3. In some embodiments, presence of the gating signal (to allow use of a smart payment device) requires continued contact with “the customer’s body.” *Id.*, 4:37-43. The device includes a transducer to “monitor[] the one or more physical phenomena” and enables/disables the wireless-communication circuit in response to detection or absence of the physical phenomena. *Id.*, 2:52-60, 3:51-67. The transducer(s) can detect a temperature, resistance, capacitance, or pressure change “when the user is holding the payment card” such that the device “is only active (and able to communicate the financial information) when it is being used by customer.” *Id.*, 1:55-62, 3:65-4:19. A POSITA would have applied these teachings of Power to Royyuru-Phillips-Casey-Deibert to protect transaction information from

being inadvertently transmitted when the user does not intend to conduct a financial transaction, thereby preventing unintended or fraudulent charges to the user's payment cards and "increase[ing] security." EX1016, 2:47-3:5.

299. Both Phillips and Casey discuss requiring the user to enter a PIN (i.e., a passcode) to re-validate a user, which a POSITA would have recognized as adding an extra layer of security when combined with Power's physical contact detection requirement. EX1005, [0035], [0038]-[0039], [0066]; EX1006, 9:9-36.

300. Deibert discloses that the Royyuru-Phillips-Casey-Deibert-Power combination provides the last three elements of claim 13 for the reasons discussed in Ground 1D, *supra*. Specifically, Deibert discloses disabling a device priming on further button pressing, stating that "the consumer can manually disable the mobile phone application, thereby returning the mobile phone to the idle state." EX1012, [0024]. Deibert further teaches that "[i]f no payment transaction occurs within the predetermined timeout time, then ***after the predetermined timeout time, the mobile payment application on the phone will automatically disable*** so that contactless payments cannot be made." *Id.*, [0025]-[0026], [0058]. Additionally, [o]nce a transaction has occurred, the mobile phone can go back to the idle state." *Id.*, [0024], [0059]-[0060].

301. Therefore, in my opinion, the combination of Royyuru, Phillips, Casey, Deibert, and Power would have rendered claim 13 of the '579 Patent as a whole obvious to a POSITA.

F. Ground 1F: Claims 4, 21 and 22 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Royyuru in view of Phillips, Casey and Carlson

302. In my opinion, the combination of Royyuru, Phillips, Casey and Carlson renders obvious as a whole claims 4, 21 and 22 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Carlson with the Combination of Royyuru, Phillips, and Casey

303. All four references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS terminals. Similar to Royyuru, Carlson describes a device for “conducting transactions using pseudo primary account identifiers.” EX1013, [0012], [0029]. The pseudo account identifier can be “similar in format to a consumer’s real account identifier” without revealing the true sequence of numbers or characters in the real account identifier. *Id.*, [0030]. The pseudo account identifier is generated by the payment processor and provided to the device for use in place of the primary account identifier. *Id.*, [0035], [0017]-[0018]. “[T]he pseudo primary account number may be *set to expire* after a certain number of transactions or after a certain time period” to avoid “illicit use.” EX1013, [0036], [0044], [0086].

304. A POSITA would have been prompted to apply the teachings of Carlson to the Royyuru-Philips-Casey combination such that the IKCV is “set to expire...after a certain time period” because “[d]oing so can help to ensure that if for some reason a pseudo primary account number is revealed to anyone other than an authorized user, the amount of damage that can be done is limited due to the limited lifetime of the pseudo primary account number.” EX1013, [0036]. Implementing the IKCV to “have a limited lifetime... provides a level of protection to the consumer's account” because it would likely “expire[] before any illicit use could be made.” EX1013, [0044]. Therefore, setting an expiration for the IKCV can prevent fraudulent use of the IKCV to generate DTCs and dynamic PANs by unauthorized devices. A POSITA would have found it beneficial to apply such an expiration date/time limitation to other account and device related information in the combination to achieve similar benefits.

305. Furthermore, a POSITA would have recognized that application of Carlson’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification.

2. Claims 4, 21, and 22

[4]: The method of claim 1, wherein a limited-use number comprises a device account number, and wherein the device account number is of a limited time-duration of valid use, and wherein further a card issuing authority provides said device account number for use only by the electronic device, in place of card issuer information in performing payment transactions by the electronic device, and further comprising: performing payment transactions by the electronic device including the limited-use number; combining the limited-use number and said device account number within a device generated payment information; and conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.

[21] The electronic device of claim 19, wherein the memory is accessible to the processor, wherein said memory comprises a static device-specific device account number of limited-use that originates from a card issuing authority and is limited to use by the electronic device in place of a card issuer account information, wherein further said static device-specific device account number has an expiration date of limited duration of validity, and wherein the generating a limited-use payment information comprises the processor generating said limited-use payment information by combining said static device-specific device account number, said device account expiration date, when said issuer payment account method is selected.

[22] The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates from a card issuing authority and is for limited-use by the specific electronic device only; and wherein said static device-specific device account information is valid for a limited duration, and wherein the generating a limited-use payment information comprises the processor generating a one-time limited-use cryptogram number and combining said limited-use static device account information and said one-time use cryptogram number to produce the limited-use payment information.

306. As shown above, the combination of Royyuru, Phillips, and Casey would have rendered parent claim 1 of the '579 Patent as a whole obvious.

307. With respect to claims [4], [21], and [22], as discussed above, in the Royyuru-Phillips-Casey-Carlson system, the IKCV is “set to expire...after a certain time period” by the payment processor or issuer. EX1013, [0036], [0044], [0086]. The IKCV therefore has an expiration date of limited duration of validity and is therefore of limited time-duration of valid use. Furthermore, the DTC and dynamic PAN can be generated using both the IKCV and any “unpredictable number” including any “number...*received by the presentation instrument.*” EX1004, [0051], [0057], [0006]. A POSITA would have recognized that the device would have received the expiration date for the IKCV to allow the device to determine when the IKCV was no longer valid and should therefore not be used for generating the

DTC and dynamic PAN for future transactions. Therefore the DTC and dynamic PAN are generated using the IKCV and the expiration date of the IKCV in the combination of Royyuru with Phillips, Casey , and Carlson, thus providing claim [21].

308. All other elements of claims [4], [21], and [22] are disclosed by the Royyuru-Phillips-Casey-Carlson combination for the reasons discussed in Ground 1A, *supra*.

309. Therefore, in my opinion, the combination of Royyuru, Phillips, Casey and Carlson would have rendered claims 4, 21 and 22 of the '579 Patent as a whole obvious to a POSITA.

G. Ground 2A: Claims 1-9, 11-12, 15-20, and 22-23 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker and Spodak

310. In my opinion, the combination of Gomez, Amacker, and Spodak renders obvious as a whole claims 1-9, 11-12 and 15-23 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Gomez, Amacker, and Spodak

311. All three references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS.

312. A POSITA would have beneficially applied the teachings of Amacker, and Spodak to modify Gomez's mobile payment system to include multiple improvements. First, a POSITA would have modified Gomez such that the EPIC

payment card of Gomez would include a larger touch screen display, as taught by Amacker. EX1007, 5:48-57, 10:34-42; EX1008, 4:51-60, 2:13-25, 6:21-30. A POSITA would have recognized that including a larger touch screen display would have allowed the device to display additional information regarding payment cards, details of the transaction, and transaction status on the device while allowing for easier, intuitive user manipulation via the touchscreen. For example, Amacker describes displaying information about the transaction with various user selection options all as one display, which a user can easily choose between via the touchscreen. EX1008, 5:1-17, FIG. 2. A POSITA would have recognized that a larger display for displaying such information, and easier touchscreen navigation, would have improved the user experience.

313. Second, a POSITA would have modified Gomez based on Amacker to receive a payment request for a transaction and display payment options for conducting the transaction at the device. EX1008, 2:37-3:3, 3:42-57, 4:37-5:17. Gomez already discloses NFC communication with the merchant and Amacker beneficially discloses that such NFC communications can include a payment request. EX1007, 8:53-57, 7:49-54; EX1008, 3:27-57, 2:37-3:3, 4:37-5:17. As shown by Amacker, the request can include useful information about the transaction displayed on the device:

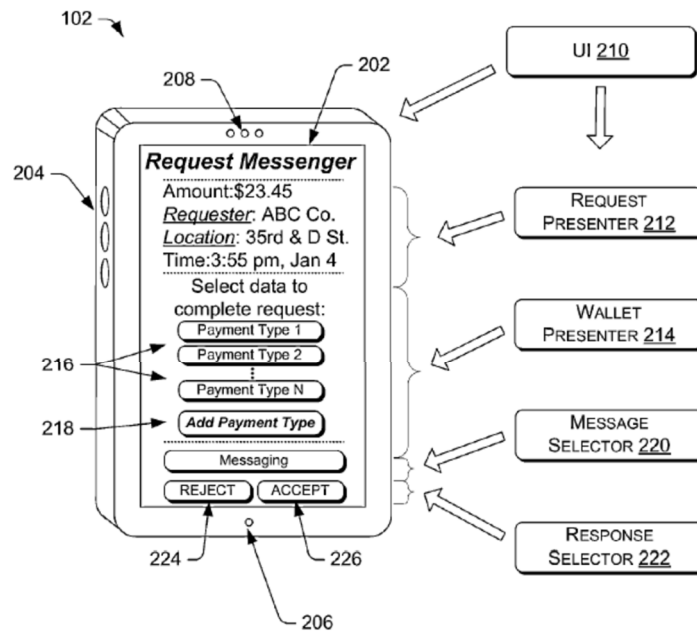


Fig. 2

EX1008, FIG. 2.

314. Modifying Gomez's system such that the user device receives a payment request from a merchant device would have improved the system by allowing the user to better ensure that they are approving a payment transaction and transmitting payment information to a correct merchant terminal, which can prevent fraudulent transmittal of payment information to an incorrect terminal. Such a modification would also allow the user to visually review transaction data before approving (or denying) the transaction. EX1008, 3:27-57, 2:37-3:3, 4:37-5:41, 6:2-15. Requiring the user to authorize the transaction (as taught by Amacker) would have allowed the user to review transaction information (e.g., price, purchase items) prior to completing the transaction, allowed the user extra opportunity to change

their mind regarding a transaction, and provide extra assurance that the user intends to initiate a payment transaction rather than having inadvertently opened a payment application.

315. Third, a POSITA would have modified Gomez based on Amacker and Spodak to display additional information when allowing a user to select a payment method. Gomez discloses that the user can “manually select the actual credit card that he/she wishes to use during a purchase transaction.” EX1007, 20:30-42, 21:5-20. Amacker provides additional details on how a user can use a touchscreen display to view additional information about payment methods before selecting. For example, Amacker allows the user to view the payment request and select from “relevant payment options that may be used to respond to the payment request.” EX1008, 5:18-41, Cl. 1

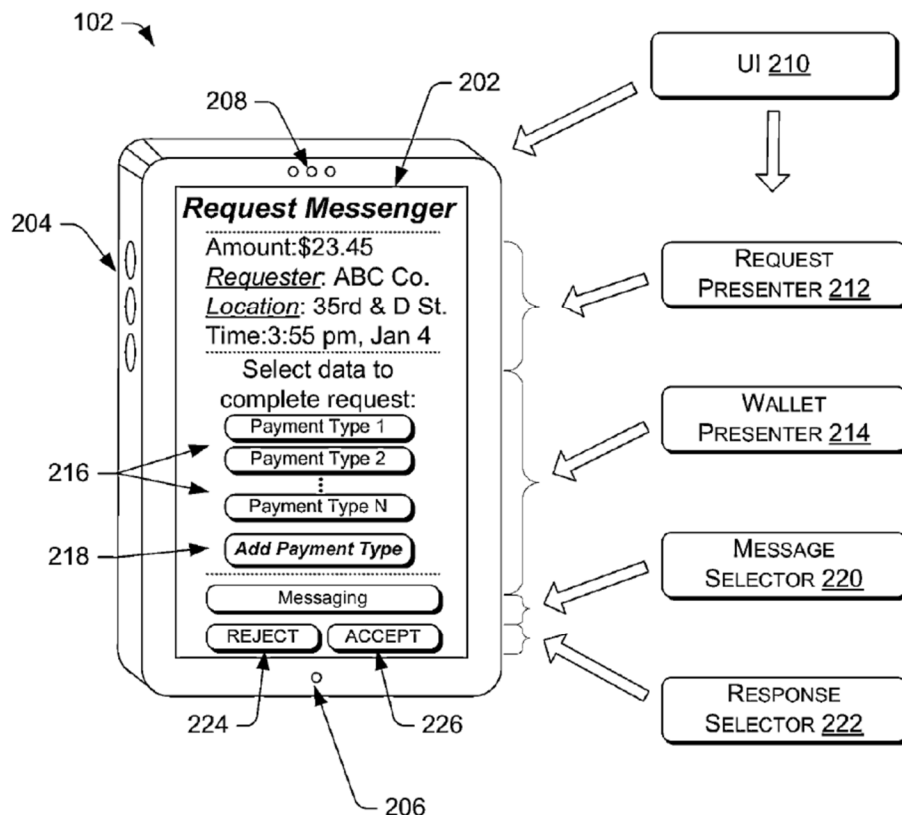


Fig. 2

EX1008, FIG. 2.

316. Spodak further discloses that its universal card includes a display for displaying payment information. EX1009, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A. A POSITA would have recognized that including such additional information in the card selection process would have allowed the user to more easily identify a desired card for a particular transaction.

317. Fourth, a POSITA would have modified Gomez based on Spodak to only display the last four digits of the account number. EX1009, [0068] (displaying

account number), [0089] (displaying last four digits of an account number). A POSITA would have recognized that only displaying the last four digits of the payment number for each card would have allowed the user to more readily recognize and identify a desired payment method from among the multiple payment methods stored on the device while obscuring the full payment number to prevent fraud due to nearby third parties observing the displayed payment numbers, thereby increasing overall utility of the device while increasing security. Furthermore, as discussed above, credit card masking was required by the Payment Card Industry. EX1026.

318. Fifth, a POSITA would have modified Gomez based on the teachings of Amacker to generate the authentication cryptogram in response to receiving the request to ensure that the limited-duration cryptogram is valid for the intended transaction. EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61. Such a modification would have saved processing resources by only utilizing the processor to generate the authentication cryptogram when a valid payment request has been received.

319. Sixth, when Amacker's screen displays the payment request, a POSITA would have understood that it visually conveys that the status of the transaction is incomplete. EX1008, FIG. 2; *see also generally* EX1001 (specification does not define "status").

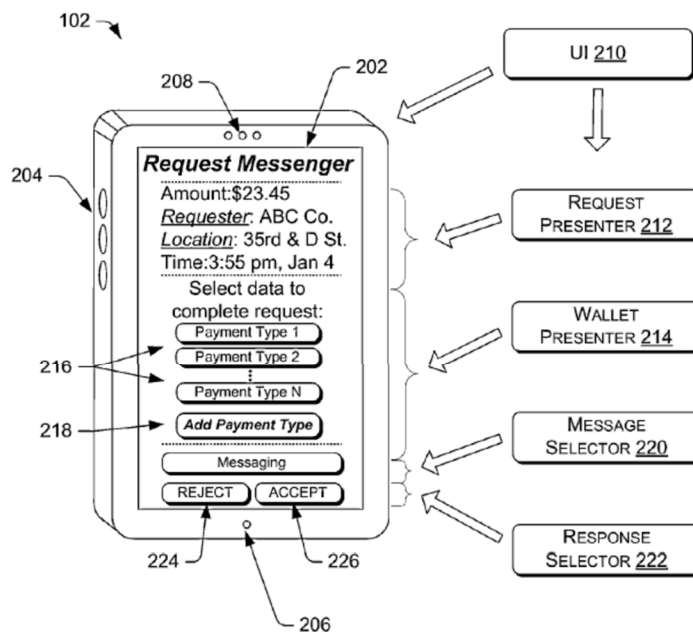


Fig. 2

Id., FIG. 2.

320. As shown in FIG. 2, the user interface visually conveys to the user that the transaction is incomplete by displaying “request” in the heading, the name of the requester, payment types to “**complete**” the request, and the option to reject or accept the payment request. *Id.* In my opinion, to the extent that this user interface does not explicitly display that the transaction is incomplete, Amacker’s disclosure would have motivated a POSITA to explicitly display that the status of the transaction is incomplete until the user selects a “payment type” and “accept.” EX1008, 6:3-15, 11:25-35, FIG. 2.

321. Finally, a POSITA would have recognized that application the teachings of Amacker and Spodak to Gomez is merely the application of known

techniques to a known system ready for improvement to yield predictable results. Here, all three references describe aspects of conducting contactless payment transactions using payment information stored on or generated by a device and Amacker and Spodak describe improvements that would have been beneficially applied to Gomez's system to improve the overall user experience and transaction security.

322. A POSITA would have furthermore had a reasonable expectation of success in modifying the mobile payment system of Gomez based on Amacker and Spodak as they all are directed toward similar mobile payment systems and all rely on common capabilities of devices. Specifically, as described above and in greater detail below, the disclosures of Amacker and Spodak complement the teachings of Gomez. Gomez's disclosure focuses on generation of the secure payment information, including the generation of an authentication cryptogram for validating the transaction. Amacker and Spodak provide teachings that a POSITA would have recognized as readily applicable to Gomez including by implementing Gomez's authentication cryptogram-focused teachings in a smart device having a larger touchscreen interface, and additional user interface and user authentication details that would have readily integrated with the dynamic cryptogram generation disclosures of Gomez, thus giving the POSITA a reasonable expectation of success combining the teachings of these references into a single system.

2. Claim 1

[1pre]: A method of performing a transaction, the method comprising:

323. Whether or not the preamble is limiting, Gomez, Amacker, and Spodak each disclose it. Gomez describes “purchase transaction approval at a retail merchant.” EX1007, 3:65-67, 5:65-6:4, 2:45-54. Amacker discloses:

In this way, the person may complete a complicated transaction, such as a purchase and delivery setup of a home appliance, by transmitting payment and personal information (e.g., address, contact information, etc.) to the retailer via a real-time mobile wallet server while avoiding timely manual entry of the information and while reducing dissemination of the personal information to additional storage locations (e.g., an entity server used to store personal account information)

EX1008, 2:49-58.

324. Spodak discloses a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002], [0027], [0033]-[0035].

[1a]: receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises:

325. Gomez describes “generat[ing] an authentication cryptogram” “upon verification of a valid credential” with an input such as “*the cardholder successfully present[ing] a credential, such as a fingerprint or PIN number, into the payment card.*” EX1007, 2:59-64, 5:13-18, 7:9-16 (“the card confirms the presentation of a

valid credential for the payment card user”), 9:12-33, 13:40-44. Thus, the user is an “identified user” who provides an input corresponding to a priming operation of authorizing the payment card to perform the transaction. Gomez discloses performing the described functions using an “EPIC payment card.” EX1007, 11:19-38, 2:55-3:3, FIG. 9. Spodak further discloses an input because, to activate the universal card, a user taps or bends the universal card itself, which corresponds to a priming action of activating the universal card. EX1009, [0045], [0084]; *see also* EX1001, 11:34-42, 13:25-32 (the ’579 patent’s examples of priming).

[1b]: a processor

326. All three of Gomez, Amacker, and Spodak disclose user devices having processors, e.g. processor 342 of Gomez, processor(s) 402 of Amacker, processors of Spodak. EX1007, 10:34-38, 2:59-64; EX1008, 7:42-52; EX1009, [0027], [0028], [0059], [0086], [0111].

[1c]: a touch screen display coupled to the processor

327. Gomez discloses “a display” and “an activation input device” that are “coupled to” the processor. EX1007, 12:49-61; 10:34-38. Amacker discloses that the display of the predictable Gomez-Amacker-Spodak combination “may be a touch screen display.” EX1008, 4:51-60.

[1d]: a near field communications (NFC) interface coupled to the processor

328. This element is disclosed in all three of Gomez, Amacker, and Spodak. For example, Gomez discloses that the device's "processor ... may include more than one IC operating together," such as "NFC circuits for implementing a near-field communications transceiver." EX1007, 10:53-57, 7:49-54, 2:40-3:3. Spodak discloses near field communication (NFC) coupled to the processor of the universal card. EX1009, [0004], [0027], [0032], [0033].

[1e]: receiving a request for a transaction payment at said electronic device via the NFC interface

329. Amacker discloses that in the combination the retailer can "transmit a request to the person's mobile device using the identifier." EX1008, 2:37-3:3. Amacker goes on to describe "provid[ing] the recipient 104 with payment in response to an information request." *Id.* In another example disclosed by Amacker, "[u]pon receipt of a request (via the MWS 102) from the recipient 104, the user 110 may make one or more selections using the MWS to determine a response to the request." EX1008, 3:42-57. Amacker further describes "generat[ing] a request for personal information (e.g., payment information) from the wallet 108." *Id.*, 4:37-50. For example, "the recipient server(s) **114** may generate a request for information, such as personal information that the user **110** may have stored in the wallet 108...such as payment information" for completing "in person" transactions, among

others. *Id.*, 6:37-61. The communication is sent via the NFC interface. EX1007, 8:53-57, 7:49-54; EX1008, 3:27-34.

[1f]: displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card

330. The Gomez-Amacker-Spodak device includes “a display and a selection capability” to allow the user “to manually select the actual credit card that he/she wishes to use during a purchase transaction.” EX1007, 20:30-59, FIG. 9. For example, “a customer may select the desired account using a mobile phone.” *Id.* The user can “scroll through available card accounts sequentially displayed on the card, and select one of the accounts.” *Id.*, see also 21:5-20 (“The customer may optionally select the desired credit card to use for the current transaction”). FIG. 9 of Gomez shows an example display:

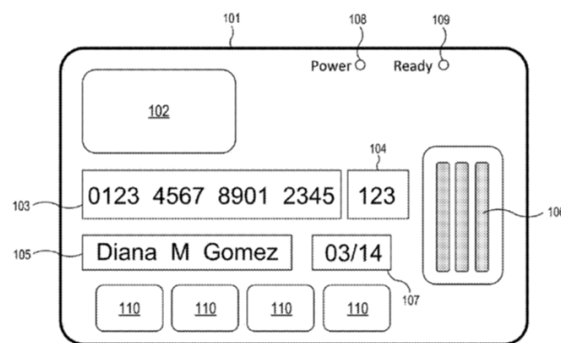


FIG. 9

331. Amacker confirms that, in the combination, “when the MWS **102** receives a payment request, the wallet presenter **214** may present relevant payment options that may be used to respond to the payment request (e.g., payment card

selections, etc.).” EX1008, 5:18-41, Cl. 1. FIG. 2 of Amacker shows an example display including multiple selectable payment types:

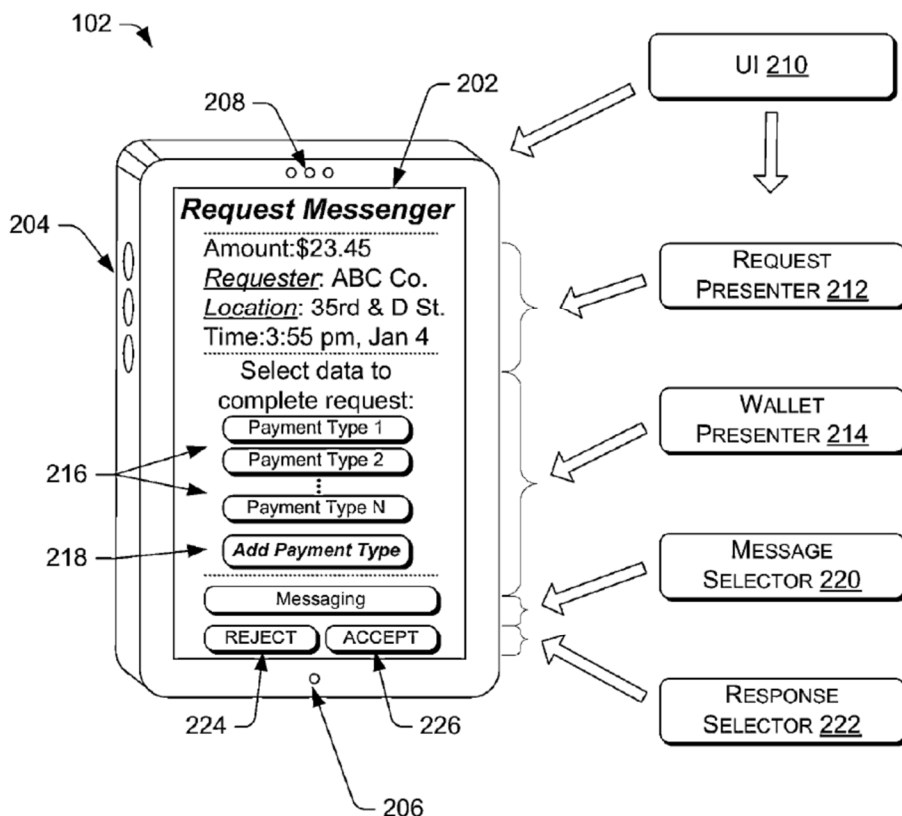


Fig. 2

EX1008, FIG. 2.

332. Spodak further discloses that its universal card includes a display for displaying payment information. EX1009, [0034], [0068] (displaying account number), [0069], [0074], [0076], [0079], [0089] (displaying last four digits of an account number), FIGs. 8A, 8B, 8D, 10A, 11A, 12A.

[1g]: a card logo

332. It is of course obvious to display an image of a payment card when presenting the user with a choice of payment cards, and it was well-known that payment cards typically bore the logo of the issuing bank.

333. Gomez discloses that as part of the process for “select[ing] the desired account using a mobile phone” the device displays “all credit cards in their EPIC account by their description name (or nickname) and *card logo*.” EX1007, 20:43-59; *see also* EX1008, 5:18-41. Spodak also discloses displaying a card issuer logo. EX1009, [0068].

[1h]: other iconography of the payment card

334. It is of course obvious to display an image of a payment card when presenting the user with a choice of payment cards, and such an image would also contain any accompanying iconography.

335. As disclosed by Gomez and Spodak, the device of the combination displays additional iconography of the payment card such as “name (or nickname)” and “graphical information, such as logos and barcodes.” EX1007, 20:43-59; EX1009, [0068] (displaying card issuer logo).

[1i]: generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information

336. Gomez describes “a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card, and which expires within a short period of time thereafter.” EX1007, 1:58-2:4. “The authentication cryptogram is generated based upon a seed value stored within the payment card, and further based upon a temporal signal value which changes for each attempted use of the payment card.” *Id.* The device generates the “authentication cryptogram for each attempted transaction only after the cardholder successfully presents a credential.” *Id.*, 5:13-18; *see also* 7:26-8:9.

337. As would have been recognized by a POSITA, the authentication cryptogram (the limited-use payment information) is used in place of the card issuer supplied payment information (the “actual credit card account number” disclosed by Gomez) in that the authentication cryptogram is combined with the static EPIC account number and provided to the merchant rather than the issuer supplied payment information. EX1007, 1:55-2:39, 5:19-24, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3.

[1j]: transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface

338. Gomez discloses “communicating a payment card identifying number to a payment processing system, and communicating *the authentication cryptogram* in a payment card account name field to the payment processing system.” EX1007, 2:50-54. For example, “the card communicates the payment card identifying number to the payment system...using near field communication (NFC).” *Id.*, 7:49-54, 8:16-23 (“the card communicates the payment card identifying number, the authentication cryptogram”). As discussed above, in some embodiments the “payment card identifying number” is “an EPIC account which is not itself a live payment card account, but to which are linked one or more live payment card accounts.” EX1007, 5:19-24, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; 1:55-2:39.

[1k]: visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.

339. It is universal in payment transactions to provide a receipt indicating that the transaction is complete.

340. Gomez describes that “a great variety of useful information may be displayed, including...secure messages, alarms, and other notifications.” EX1007, 12:58-67. The device also provides various notifications. *Id.*, 10:18-26, 11:53-62. Gomez also teaches that a transaction status is provided “back to the merchant 406 to indicate either approval or denial of the transaction.” *Id.*, 6:56-64.

341. In my opinion, having looked to Gomez, a POSITA would have applied the teachings of Amacker, which, as discussed above, visually conveys that the status of the transaction is incomplete. EX1008, FIG. 2.

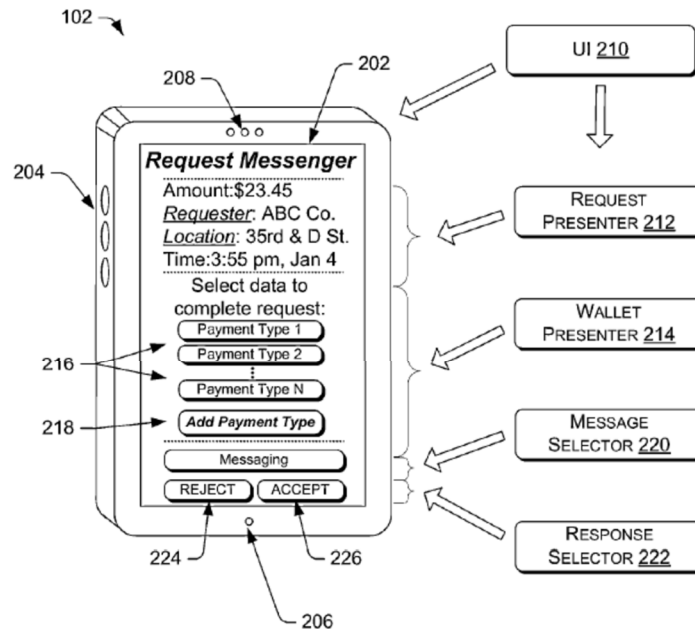


Fig. 2

Id., FIG. 2.

342. To the extent that the user interface does not explicitly display that the transaction is incomplete, a POSITA would have modified Gomez based on Amacker to explicitly display that the status of the transaction is incomplete until the user selects a “payment type” and “accept.” *Id.*, 6:3-15, 11:25-35, FIG. 2. In my opinion, because Amacker requires the user to accept or reject the payment request before accepting or rejecting the payment request from the mobile wallet server (MWS), such a modification would have explicitly provided additional assurance to

the user that they are in control of their financial transactions because the transaction would not proceed until they accepted or rejected the payment request. Furthermore, Amacker discloses initiating communications between the user and the MWS, which provides the payment request, if the user rejects the payment request. *Id.*, 7:30-33, 11:10-35. In my opinion, POSITA would also have been motivated to initiate communications if the user accepted the request, and to modify these communications to include the status of the transaction. Such a modification would have provided even more assurance to the user that they are in control of their financial transactions by displaying confirmation over whether the transaction was accepted or rejected as the user intended in making their selection.

343. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 1 of the '579 Patent as a whole obvious to a POSITA.

3. Claim 2

[2]: The method of claim 1, wherein the generating the limited-use payment information utilizes at least one information from a set of information comprising: a device transaction sequence counter; a device account number; device secret keys; card issuer keys; merchant information; NFC recipient information; payment reader information; a time; a timestamp; an amount; a location; an online location; transaction information; payment information; device information; user information; an email address; and a user identification entry.

344. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

345. Gomez discloses that “[t]he authentication cryptogram is generated based upon a seed value stored within the payment card, and further based upon a temporal signal value which changes for each attempted use of the payment card.” EX1007, 1:58-2:4. The temporal value can be “the date/time of the transaction” or “the sequence value (or sequential number) of the attempted use.” *Id.*, 5:25-32, 6:27-33, 7:17-48, 10:66-11:6. The “seed value is unique for each payment card, [] corresponds to the payment card identifying number,” and “may include certain non-random customer specific information, such as a unique customer key.” *Id.*, 7:17-48.

346. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 2 of the '579 Patent as a whole obvious to a POSITA.

4. Claim 3

[3]: The method of claim 1, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the card issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count and at least one information of a set of information comprising: a device account number; device identifiers; device secrets; device keys; payment issuer secrets; payment issuer keys; user information; a time; and transaction information; and wherein further, said dynamically generating the cryptogram number results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction.

347. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

348. Gomez's "authentication cryptogram" is dynamically generated on the device by combining "a seed value" and "a temporal signal." EX1007, 1:58-2:4, 7:41-43, 21:37-48. The temporal signal can be "the sequence value (or sequential number) of the attempted use." *Id.*, 7:17-26, 8:36-41, 10:58-11:6. This sequential parameter is generated by "a sequential instance circuit" when the user attempts to use the device for a transaction. *Id.*, 10:64-11:6, FIG. 7 (348). The "seed value is *unique for each payment card*, [] corresponds to the payment card identifying number," and "may include certain non-random customer specific information, such as a *unique customer key*." *Id.*, 7:17-48, *see also id.*, 12:30-34, 16:31-34, 16:64-17:13. Therefore the seed value provides at least the claimed device account number,

device identifier, device secrets, device key, and payment issuer key. Alternatively, Gomez discloses that the temporal value can be a sequence counter or time and it would have been obvious to a POSITA to use **both** a sequence counter and time when generating the cryptogram to increase the security of the cryptogram by incorporating multiple temporal values, making the values more difficult to guess or derive. *Id.*, 5:25-32, 6:27-33, 7:17-48, 10:66-11:6.

349. Gomez discloses that the authentication cryptogram is provided in place of “the 3-digit security code” provided by the issuer. *Id.*, 9:65-10:17, 2:4-12, 14:37-63. The authentication server uses the authentication cryptogram to validate the transaction. *Id.*, 6:23-38.

350. Gomez further discloses that the authentication cryptogram is a one-time limited-use number in that it “is **generated uniquely for each attempted use of the payment card.**” *Id.*, 1:58-63. Gomez further discloses that “any newly-generated authentication cryptogram is only good for a finite amount of time, preferably measured in seconds” after which the cryptogram “become[s] obsolete” and “rendered useless.” *Id.*, 21:37-48. Because the authentication cryptogram is generated “based upon a temporal signal value which changes for each attempted use of the payment card,” the cryptogram can only be used once and constitutes a one-time limited use number. *Id.*, 1:64-2:1; *see also id.*, 5:15-16 (“generates an authentication cryptogram for each attempted transaction”), 8:36-39, 14:3-4. In

embodiments in which the temporal signal is a sequential counter, the value is “increment[ed] for each attempted use” such that each cryptogram is unique for each attempted use. *Id.*, 8:36-39.

351. Amacker also discloses a one-time payment number. EX1008, 4:26-30 (“limited-use payment information (e.g., one-time payment number, etc.)”), 8:28-33, 11:38-51.

352. To the extent Gomez and Amacker do not render obvious generating a cryptogram number separately from generating payment information in claim 1, this would have been obvious in view of Spodak. Similar to Gomez and Amacker, Spodak discloses a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002]. The universal card is similar to a mobile device such as a phone except that the universal card is shaped like a credit card. *Id.*, [0027], [0034]. The universal card includes both a dynamic magnetic stripe and a short range transceiver. *Id.*, [0033], [0035]. The universal card can use the dynamic magnetic stripe to communicate with a traditional credit card magnetic stripe reader, and the short range transceiver to communicate with a contactless payment terminal such as via NFC. *Id.*, [0088]-[0089].

353. To emulate the magnetic stripe and “authenticate the transaction with the card issuer,” the universal card generates a “dynamic authentication value,”

which discloses the claimed “cryptogram number.” *Id.*, [0094]. Spodak discloses that “the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value,” *id.*, which discloses that this value is generated “for use by the electronic device in place of a card validation value originated from the card issuer” as claimed. The dynamic authentication value is generated based on “a random number” and “a transaction counter.” *Id.*, [0094]. Because the “dynamic authentication value is unique for every transaction,” *id.*, generating the dynamic authentication value “results in a one-time limited-use number” as claimed.

354. In my opinion, a POSITA would have been prompted to apply the teachings of Spodak to Gomez and Amacker. Gomez discloses that its payment card “may use a programmable magnetic stripe or contactless technology to provide total compatibility with existing POS equipment” (EX1007, 2:42-44) and that it the card “includes a re-writable magnetic stripe on which the payment card” (*Id.*, 5:50-51). In my opinion, a POSITA would have been motivated to combine Spodak’s dynamic authentication value and Gomez’s cryptogram encryption techniques in the Gomez-Amacker-Spodak combination to generate the claimed cryptogram number to improve the security and compatibility of the device with existing POS equipment that use magnetic stripes. *Id.*, [0088]-[0089], [0094]; EX1008, 4:26-30, 8:28-33,

11:38-51; EX1007, 1:58-2:4, 2:42-44, 5:15-16, 5:50-51, 7:17-26, 7:41-43, 8:36-41, 10:58-11:6, 21:37-48.

355. A POSITA would have incorporated Spodak's generation of the dynamic authentication value so that "there would be no need to reconfigure the terminal with the magnetic stripe reader because it would already be configured to read a value from the static CVV field location." EX1009, [0094]. The improved device would be compatible with additional magnetic stripe readers by generating the dynamic authentication value for use in place of a card validation value (CVV) originating from the card issuer. EX1009, [0088]-[0089], [0094].

356. To the extent that Spodak does not disclose generating the dynamic authentication value cryptographically, a POSITA would have further been motivated to apply Gomez's disclosure of encrypting its authentication cryptogram for Spodak to encrypt its dynamic authentication value. EX1007, 1:58-2:4, 7:41-43, 21:37-48, 7:17-26, 8:36-41, 10:58-11:6. A POSITA would have been motivated to encrypt Spodak's dynamic authentication value because, like Gomez's authentication cryptogram, Spodak's dynamic authentication value is used to securely conduct a transaction. EX1007, 1:58-2:1, 21:37-48; 5:15-16, 8:36-39, 14:3-4; EX1008, 4:26-30, 8:28-33, 11:38-51.

357. To the extent that Spodak does not disclose incrementing its transaction counter, a POSITA would have further been motivated to apply Gomez's

disclosure about incrementing its sequential counter to Spodak to increment its transaction counter. A POSITA would have further been motivated to increment Spodak's transaction counter by virtue of it being a counter, and because both Gomez's authentication cryptogram and Spodak's dynamic authentication value are generated based on counters and numbers. EX1007, 7:17-48, 12:30-34, 16:31-34, 16:64-17:13; EX1009, [0094].

358. In my opinion, a POSITA would have recognized that application of Spodak's teachings to Gomez is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. A skilled person would have reasonable expectation of success in making the above-described combination of known prior art technologies (e.g., known devices for conducting transactions via both a magnetic stripe reader and a contactless payment terminal) according to known methods (e.g., known process for securing payment information during the transactions) to yield the predictable result of a device that could securely conduct transactions with both a magnetic stripe reader and a contactless terminal.

359. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 3 of the '579 Patent as a whole obvious to a POSITA.

5. Claim 4

[4]: The method of claim 1, wherein a limited-use number comprises a device account number, and wherein the device account number is of a limited time-duration of valid use, and wherein further a card issuing authority provides said device account number for use only by the electronic device, in place of card issuer information in performing payment transactions by the electronic device, and further comprising: performing payment transactions by the electronic device including the limited-use number; combining the limited-use number and said device account number within a device generated payment information; and conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.

360. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

361. The device account number is disclosed by Gomez's seed value, which is used to generate the authentication cryptogram, "is *unique for each payment card*, and *corresponds to the payment card identifying number*."

EX1007, 1:44-47, 7:17-48, *see also id.*, 12:30-34, 13:45-14:2, 16:31-34, 16:64-17:13.

The seed value therefore provides a device account number that can be the 16-digit card number that a POSITA would understand is provided by a card issuing authority. The payment card number has an "expiration date" and, therefore, a POSITA would have recognized that, because the seed value "corresponds to the payment card identifying number," the expiration date for the payment card number is also the expiration date for the seed value, meaning that the seed value has a

limited time-duration of valid use. EX1007, 3:67-4:4, 5:50-57, 11:23-27, 7:17-48. Alternatively, it would have been obvious to a POSITA to make the seed value of a limited time-duration of valid use tied to the payment account expiration date so that a seed value generated using an expired account number could not be used for transactions. This would help ensure that the user's account is still valid. *Id.*

362. Gomez further discloses that the device combines the “payment card identifying number” and the “authentication cryptogram” together to form complete payment information and communicates this payment information to the payment processing system. EX1007, 2:50-3:3, 5:48-60. In my opinion, because the specification does not define “combine,” the claimed device generated payment information is disclosed by Gomez transmitting the “authentication cryptogram” and the “payment card identifying number” together. This combined payment information is used to perform a payment transaction. *Id.*, 6:23-38, 7:57-65, 8:16-23. The payment card identifying number can be “an EPIC account number” “which is not itself a live payment card account, but to which are linked one or more live payment card accounts.” EX1007, 6:7-22, 5:19-24. Therefore, the combined payment information is conveyed in place of card issuer information during a payment transaction.

363. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 4 of the '579 Patent as a whole obvious to a POSITA.

6. Claim 5

[5] The method of claim 1, further comprising: generating a limited-use security number for use in place of a card issuer card security code by cryptographically combining information from at least one of a set of information comprising: user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; transaction information; and displaying the limited-use security number on the user-interface of the display.

364. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

365. The Gomez-Amacker-Spodak combination describes generating a limited-use number based on the dynamic authentication value and the authentication cryptogram and therefore provides combining at least one of a device transaction sequence counter, a device account number, device identifiers, device secrets, device keys, issuer secrets, a payment card account number, a time, and an expiration date. *See supra*, Claims [2]-[4]; EX1007, 5:25-32, 6:27-33, 7:17-48, 8:36-41, 10:58-11:6; 10:64-11:6, 12:30-34, 16:31-34, 16:64-17:13, 1:58-63, FIG. 7; EX1009, [0002], [0027], [0033]-[0035], [0088]-[0089], [0094]. The

authentication cryptogram is provided in place of the card issuer card security code. *See supra*, Claims [3]-[4]; EX1007, 9:65-10:17, 2:4-12, 14:37-63.

366. Gomez further describes “a great variety of useful information may be displayed” on the display of the payment device, for example “***the generated authentication cryptogram may be displayed***, which may be beneficial in facilitating an online transaction.” EX1007, 12:64-13:4, 13:22-33, 21:5-20. Spodak further discloses that its universal card includes a display for displaying payment information. EX1009, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A. In my opinion, having appreciated displaying the payment information and the generated authentication cryptogram, a POSITA would have looked to the Gomez-Amacker-Spodak combination for the displaying step of claim 5. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 5 of the ’579 Patent as a whole obvious to a POSITA.

7. Claim 6

[6] The method of claim 1, wherein a payment processing authority verifies a limited-use number based on at least one information of the set of information comprising: a transaction sequence count information; a device account number; user account information; issuer secrets; issuer keys; issuer-provided device keys; transaction information; and a time of use, and further comprising: authorizing said transaction, by the payment processing authority, responsive to verifying a valid limited-use number appearing in place of card issuer information; and rejecting a limited-use number, by the payment processing authority, on at least one unverifiable condition, of a set of unverifiable conditions comprising: an invalid number generation; an invalid device account number; a use outside of a valid time window; an invalid re-use of a limited-use number; and an invalid use of an expired limited-duration number.

367. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

368. Gomez discloses that the acquirer sends an account authentication request that “includes at least the EPIC account number, the date and time of the transaction, and the authentication cryptogram” to an EPIC authentication server. EX1007, 6:12-38, 14:21-27, 17:40-62. The authentication server determines if the authentication cryptogram is valid “by independently generating a ‘reference’ authentication cryptogram based upon the seed value corresponding to the EPIC account number, and based upon the *date/time of the transaction* (or other temporal signal value, as described below).” *Id.* As discussed above (*supra*, Claims [2]-[4]), the “other temporal signal values” include a transaction sequence counter and the

seed value provides at least a device account number, user account information, issuer secrets, issuer keys, and issuer-provided device keys. EX1007, 7:17-48, 8:36-41, 10:58-11:6, 12:30-34, 16:31-34, 16:64-17:13. The authentication cryptogram is provided in place of the card issuer card security code. *See supra*, Claims [3]-[4]; EX1007, 9:65-10:17, 2:4-12, 14:37-63.

369. The authentication server authorizes the transaction “[i]f the server-calculated reference authentication cryptogram matches the received authentication cryptogram generated by the EPIC card and provided to the merchant 406.” EX1007, 6:23-38, 18:20-25. Specifically, if the authentication cryptogram is valid, the payment card information is transmitted to a card association and then the issuer “to either approve or deny the particular transaction.” *Id.*, 6:23-64. The transaction is rejected if a previously used authentication cryptogram is reused. EX1007, 5:34-47, 21:37-48.

370. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 6 of the ’579 Patent as a whole obvious to a POSITA.

8. Claim 7

[7] The method of claim 1, wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: a device button; a device touch-screen interface; a device touch ID button interface; a device optical sensor array; a device skin touch sensor; a skin-contact sensor; a device motion detection interface; a device biometric sensor interface; and a device user-interface selection.

371. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

372. Further, Gomez, Amacker, and Spodak each disclose receiving input at a touch screen interface. *See supra*, [1a], [1c].

373. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 7 of the '579 Patent as a whole obvious to a POSITA.

9. Claim 8

[8] The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising: a button press; a touch ID button press; a button double-press; a touch ID sensor touch; a touch-screen touch; a touch-input sequence; a gesture or swipe over a sensor-array; a skin-contact sense; an optical-sensor array sense; an electronic device tap; a sequence of motions of the electronic device; a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation; and, further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a touching from an identified valid user; a user entry of a valid passcode; a user entry of a valid PIN; swiping of a recognized user skin over a device sensor array; a correct user swiping or gesturing on the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motioning of the electronic device; a skin-contact sensing of an identified user; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.

374. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

375. Gomez discloses that the device can be primed when “the cardholder successfully presents a credential, such as a fingerprint or PIN number, into the payment card.” EX1007, 5:13-18, 13:40-44. Amacker confirms that the device in the combination can “require the user **110** to provide text, audio, biometric, or other information before accessing the wallet” and that the device includes a touch screen for receiving such text or other input. EX1008, 8:16-20; 4:51-60.

376. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 8 of the '579 Patent as a whole obvious to a POSITA.

10. Claim 9

[9a]: The method of claim 1, further comprising: obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user

377. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

378. Amacker discloses obtaining a user payment approval through a device touch interface (and also a device touch-screen display interface).

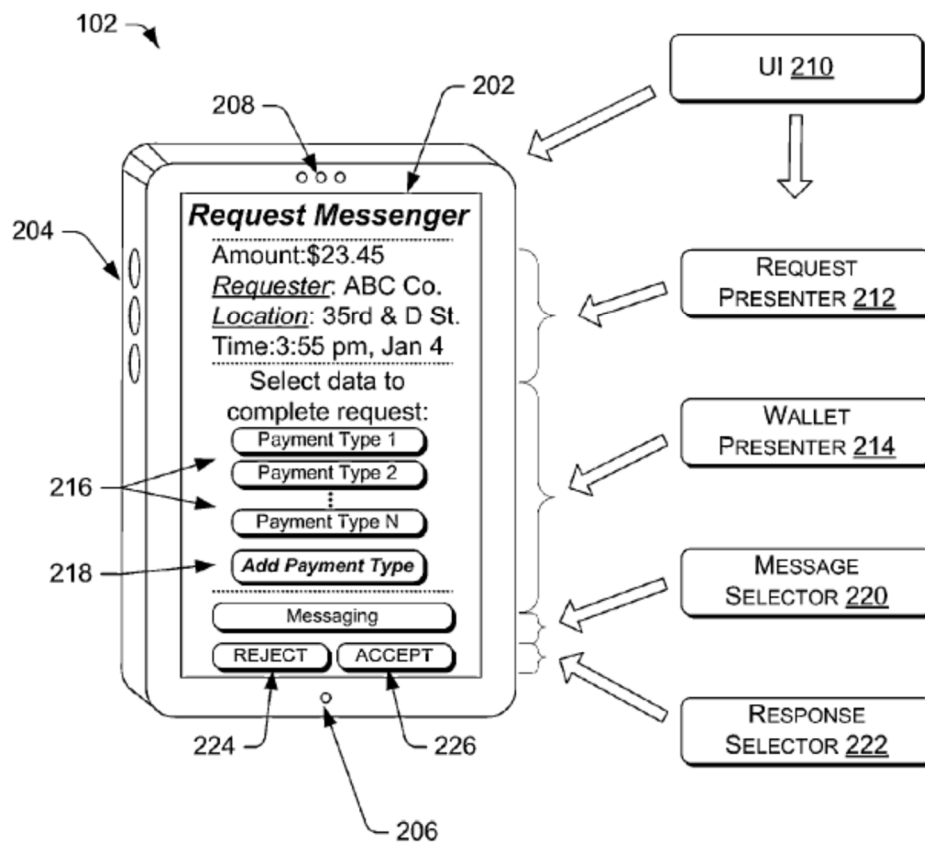


Fig. 2

EX1008, FIG. 2.

[9b]: displaying, on the display, at least one information of a set of information comprising: a priming status of the electronic device for payment; a default payment method; a plurality of selectable payment accounts; a payment request; transaction information; a payment amount; a merchant identification; a time; an expiration date; a location; an account balance; a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography

379. Amacker discloses displaying a plurality of selectable payment accounts. EX1008, FIG. 2. Amacker further discloses that in the combination, the

touchscreen can display “**a type of request** (payment, contact information, username, etc.), **a requester’s identity/location**, a time of the request, **an amount (if applicable)** and/or **other relevant information.**” EX1008, 5:1-17. As shown in FIG. 2, the display includes “a reject option 224 and an accept option 226.” *Id.*, 6:2-15. As shown in FIG. 2, the display also includes a plurality of selectable payment accounts and the device of the combination receives a user payment method selection. *Supra*, Element [1f]; EX1008, 5:18-41; *see also* 4:40-46, 6:3-15; EX1007, 20:30-21:20.

[9c]: receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.

380. Amacker discloses receiving a user input of a payment method selection. Amacker also discloses receiving a payment approval authorization. EX1008, FIG. 2.

381. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 9 of the ’579 Patent as a whole obvious to a POSITA.

11. Claim 11

[11] The method of claim 1, further comprising completing the transaction on the electronic device, wherein the completing further comprises: receiving an authorization input on the electronic device from a valid device user, in response to at least one of a set of exceptional conditions comprising: the electronic device leaving the proximity of the NFC recipient; the incomplete identifying of a valid device user; the electronic device leaving the user's possession; the electronic device leaving the proximity contact of the user; the electronic device leaving the grasp of the user; a biometric sensing the electronic device leaving the possession of a user since a last user validation; the transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration; a card issuing authority requesting a security check; and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; continuing with the default payment method; selecting an alternate payment account; inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.

382. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

383. Amacker discloses that in the combination, the device allows for “selectively approving or rejecting requests for personal information using the mobile wallet server.” EX1008, 2:32-49 (“The person may respond to the request by interacting with the mobile wallet server (e.g., select ‘accept’ or ‘reject’ button, etc.)”), 6:2-15, 12:34-46, 12:47-57 (time range for handling transactions), 12:58-67 (transaction restrictions based on fund availability and request limit), 13:1-6, FIG. 2 (see above).

384. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 11 of the '579 Patent as a whole obvious to a POSITA.

12. Claim 12

[12] The method of claim 1, further comprising: subsequent to the priming operation, offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display, including at least one of: a last four digits of a payment account number portion; a last four digits of a device account number portion; an expiration date; a card issuer icon; a bank logo; a card processing network logo; a card image; a card payment network icon; graphical images associated with the payment account; accepting a user input selection of a payment option, from said payment options, via said touch-screen display; and proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options.

385. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

386. Gomez discloses that “*after entering a customer-established PIN authorization code*, a customer may then view all credit cards in their EPIC account by their description name (or nickname) and *card logo*, and *select the card* they wish to use on their next transaction.” EX1007, 20:43-21:20, 20:12-23. Gomez further discloses that “[t]he customer may optionally select the desired credit card to use for the current transaction, but otherwise the EPIC card defaults to the pre-established

credit card account selection order.” *Id.* The entering of a customer-established PIN authorization code is the claimed “priming operation.”

387. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 12 of the ’579 Patent as a whole obvious to a POSITA.

13. Claim 15

388. Claim 15 contains limitations similar to those of claim 1, and would have been obvious in view of the combination of Gomez, Amacker, and Spodak, for the same reasons as articulated with respect to claim 1, and as supplemented below.

[15pre]: A method of performing a transaction, the method comprising:

389. The preamble of claim 15 is identical to the preamble of claim 1. Hence, *see supra*, [1pre].

[15a]: receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device:

390. Limitations [1a], [1d], and [1e] recite:

[1a] **receiving an input at an electronic device**, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises:

[1d] **a near field communications (NFC) interface** coupled to the processor;

[1e] **receiving a request for a transaction payment at said electronic device via the NFC interface**

391. Hence, *see supra*, [1a], [1d], [1e].

[15b]: displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device

392. Limitations [1c], [1f], and [9b] recite:

[1c] **a touch screen display** coupled to the processor

[1f] **displaying, on the touch-screen display**, images of: a **card issuer payment method selection**, including a last 4-digit partial number of a card issuer supplied account number of a payment card

[9b] (abridged) displaying, on the display, at least one information of a set of information comprising: . . . **a plurality of selectable payment accounts**; a payment request; transaction information; a payment amount . . .

393. Hence, *see supra*, [1c], [1f], [9b].

[15c]: receiving, from a valid device user, a payment selection and approval authorization input on the electronic device

394. Limitations [1f], [9a], [9c], and claims [11]-[12] recite:

[1f] displaying, on the touch-screen display, images of: a **card issuer payment method selection**, including a last 4-digit partial

number of a card issuer supplied account number of a payment card

[9a] (abridged) The method of claim 1, further comprising:
obtaining, by the electronic device, **a user payment approval** .
..

[9c] **receiving a user input of** at least one user action, from a set of actions comprising: **a payment method selection**; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.

[11] (abridged) completing the transaction on the electronic device, wherein the completing further comprises: **receiving an authorization input on the electronic device from a valid device user**, . . . **inputting an approval authorization**; inputting a transaction denial; and inputting an adjustment of the transaction payment . . .

[12] (abridged) subsequent to the priming operation, **offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display** . . .

395. A “user payment approval” can only be obtained from a valid device user. Hence, *see supra*, [1f], [9a], [9c], [11], [12].

[15d]: generating a limited-use number at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information

396. Limitation [1i] recites:

[1i] generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information

397. Hence, *see supra*, [1i].

[15e]: transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface

398. Limitation [1j] recites:

[1j] transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface

399. Limitation [15e] is nearly identical to [1j]. Hence, *see supra*, [1j].

[15f]: obtaining a user payment approval through at least one user-interface of the electronic device, of a set of user-interfaces comprising: a touch-screen interface of the touch-screen display user-interface; a touch ID button; input buttons; a touch key-pad; an optical sensor array; a sensor array operable to recognize a swiping of a recognized user skin over the sensor array; a motion detection unit; an accelerometer; a biometric user-sensor; a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient

400. Limitation [9a] recites:

[9a] obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user

401. Limitation [15f] is nearly identical to [9a]. Hence, *see supra*, [9a].

[15g]: displaying on said display at least one of a set of information comprising: transaction information; merchant information; a time; a location of the transaction; a payment bank logo; a card issuer icon; a payment card image; an amount

402. Limitations [1g], [1h], and [9b] recite:

[1g] a card logo

[1h] other iconography of the payment card

[9b] (abridged) **displaying, on the display, at least one information comprising: . . . transaction information, a payment amount. a time; a location; . . . a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography**

403. Limitation [1g] is a subset of limitations [1g], [1h], and [9b]. Hence, *see supra*, [1g], [1h], and [9b].

[15h]: receiving a user input providing for at least one transaction action, from a set of actions comprising: approving a transaction; denying a transaction; and adjusting a transaction.

404. Limitations [9a], [9c], and claim [11] recite:

[9a] (abridged) obtaining, by the electronic device, a user payment approval . . .

[9c] (abridged) **receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.**

[11] (abridged) completing the transaction on the electronic device, wherein the completing further comprises: **receiving an authorization input on the electronic device** from a valid device user, ... and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; . . . **inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.**

405. Limitation [15h] is a subset of limitations [9a], [9c] and claim [11].

Hence, *see supra*, [9a], [9c], and claim [11].

406. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 15 of the '579 Patent as a whole obvious to a POSITA.

14. Claim 16

[16] The method of claim 15, further comprising: **visually conveying on the touch-screen display user-interface, information regarding the transaction, including at least one of: a payment amount requested; an indication requesting an authorization input; an indication of an authorization success; an indication of an authorization failure; an option to retry a transaction; an option to retry a user authorization; an option to retry validating a user identity; an indication of a payment successfully completed; an indication of a payment failure; and an indication of a payment retry option.**

407. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 15 of the '579 Patent as a whole obvious.

408. The device of the Gomez-Amacker-Spodak combination has a touchscreen. *Supra*, [1c]; EX1008, 4:51-60. As described by Amacker, the device presents a confirmation screen displaying “a type of request” including “**a requester's identity/location**, a time of the request, **an amount (if applicable)** and/or **other relevant information** that may assist the user to understand the request.” EX1008, 5:1-17. As shown in FIG. 2, the display includes “a reject option 224 and an accept option 226.” *Id.*, 6:2-15. *See* FIG. 2, reproduced above.

409. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 16 of the '579 Patent as a whole obvious to a POSITA.

15. Claim 17

[17] The method of claim 15, further comprising: visually presenting on the touch-screen display user-interface, a plurality of payment options, including at least one of a set of payment method information for each payment option, the set comprising: a card image; a payment issuer logo; partial payment account numbers; a card payment network icon; a graphical image-encoding of a users payment account information; an amount of currency; an account balance; a credit limit; an amount of remaining credit; an amount of cryptocurrency; a cryptocurrency server network; and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface.

410. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 15 of the '579 Patent as a whole obvious. *See supra*, [1f] (users [sic] payment account information), [1g]-[1h] (payment issuer

logo), [9c] (receiving a user-selection of a payment method), [11] (a plurality of payment options), [12] (payment issuer logo).

411. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 17 of the '579 Patent as a whole obvious to a POSITA.

16. Claim 18

[18] The method of claim 15, further comprising: receiving a priming operation at the electronic device for priming the electronic device for imminent payment, wherein the priming operation causes the electronic device to successfully identify the user through completing at least one user-validation, of a set of user validations comprising: a touching of the device by an identified user; a user entry of a valid passcode; a user entry of a valid PIN; a swiping of a recognized user skin over a sensor array of the electronic device; a correct user swiping or gesturing on a touch sensor array of the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motions of the electronic device; a skin-contact sense of a valid user; and a device biometric recognition of a valid user.

412. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 15 of the '579 Patent as a whole obvious. *See supra*, [1a] (priming operation), [8] (device biometric recognition of a valid user).

413. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 18 of the '579 Patent as a whole obvious to a POSITA.

17. Claim 19

414. Claim 19 contains limitations similar to those of claim 1, and would have been obvious in view of the combination of Gomez, Amacker, and Spodak, for the same reasons as articulated above with respect to claim 1, and as supplemented below.

[19pre]: An electronic device comprising:

415. Each of Gomez, Amacker, and Spodak discloses an “electronic device” such as the card of Gomez (EX1007, FIG. 11), the mobile wallet server 102 of Amacker (EX1008) and the “universal card” of Spodak (EX1009, [0002]). Gomez discloses performing the described functions using an “EPIC payment card” having a processor coupled to memory. EX1007, 10:34-38, 11:19-38, 2:55-3:3, FIG. 9.

[19a]: at least one processor

[19b]: a memory coupled to the at least one processor

416. The device of the combination “includes a processor 342 coupled to a memory 344.” EX1007, 10:34-38, 2:55-3:3; EX1008, Cl. 9; EX1009, [0027], [0028], [0059], [0086], [0111].

[19c]: a display operable to present a visual user-interface comprising device inputs; display output

417. *See supra*, Element [1c].

[19d]: a device input

418. It is unclear what is meant by “a device input,” as the act of inputting information to a device is not an apparatus element. I believe a POSITA would understand “a device input” to mean “an input device,” such as the “device input button” of claim 9.

419. With that understanding, Gomez discloses “an activation input device” including “a fingerprint reader.” EX1007, 10:34-38, 11:14-31, 2:55-59. Amacker discloses that the display of the predictable Gomez-Amacker-Spodak combination “may be a touch screen display” and the device includes “an input button.” EX1008, 4:51-60, 5:42-49, 8:49-53; EX1007, 13:22-33.

[19e]: an NFC interface operable to receive a transaction request when in proximity to an NFC recipient

420. Limitation [1c] recites “a near field communications (NFC) interface coupled to the processor.” Limitation [1e] recites “receiving a request for a transaction payment at said electronic device via the NFC interface.” Hence *see supra*, [1c], [1e].

[19f]: wherein the processor is operable to execute a program to implement a method comprising

421. Gomez describes “a processor operable to verify the credential for the payment card user and, upon verification of a valid credential, to generate an authentication cryptogram based at least in part on the seed value and the temporal signal value.” EX1007, 2:59-64. Amacker confirms that in the combination, the

device memory stores “computer-executable instructions that, when executed by one or more processors, cause the one or more processors to perform the recited operations.” EX1008, 6:21-30.

[19g]: accepting a priming action of the electronic device by an identified device user, from the device input

422. *See supra*, [1a], [7]-[8].

[19h]: enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user

423. Gomez describes that “upon verification of a valid credential” (e.g., a priming operation that authorizes the payment card to perform a transaction), the device “generate[s] an authentication cryptogram based at least in part on the seed value and the temporal signal value.” EX1007, 2:59-64, 5:13-18 (“...generates an authentication cryptogram for each attempted transaction only after the cardholder successfully presents a credential.”), 7:17-20; At this point “the card is considered ready to communicate with the payment processing system.” EX1007, 8:11-15, 9:30-41, 11:53-62; *see also* EX1008, 2:32-57, 6:2-15.

[19i]: displaying a summary of selectable payment account options on the display

424. *See supra*, [1f]-[1h].

[19j]: receiving a payment selection and approval authorization from a valid device user via the device input

425. *See supra*, [1f], [9a], [9c], [11]-[12].

[19k]: responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use in place of card issuer payment information

426. *See supra*, [1e] and [1i]. Gomez discloses that the combination provides generating a limited-use payment information for use in place of card issuer payment information in the form of the authentication cryptogram. *Supra*, Element [1i]; EX1007, 1:58-2:4, 5:13-24, 7:26-8:9, 1:55-2:39, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3.

427. Amacker discloses that, in the combination, the authentication cryptogram (the limited-use payment information) is generated in response to receiving the NFC transaction payment request. Amacker discloses that in the combination, the retailer can “transmit a request to the person's mobile device.” EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; *supra*, [1e]. The “approval request may provide information to the request presenter 212 to enable the user to make an informed decision regarding the request.” EX1008, 10:66-11:11. Upon viewing the request information displayed as a result of receiving the request, the user “may accept the request” by “selecting an approve button.” *Id.*, 11:25-30. In some embodiments the device “generate[s] the limited use number following the ‘yes’ route” of the user accepting the request. *Id.*, 12:9-17, 11:42-64. In another example, Amacker discloses that the limited use number is generated and provided to the

merchant “[u]pon a selection of ‘accept’” in response to the payment request.

EX1008, 2:46-49.

[19l]: wherein the NFC interface is operable to transmit said payment information from said electronic device to the NFC recipient of the transaction

428. Limitation [1j] recites: “transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface.” Hence *see supra*, [1j].

[19m]: wherein further the processor is operable to cause the display to visually convey a status of the transaction.

429. Limitation [1k] recites: “visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.” Hence *see supra*, [1k].

430. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 19 of the ’579 Patent as a whole obvious to a POSITA.

18. Claim 20

[20]: The electronic device of claim 19, wherein the method further comprises: receiving the priming action of a valid user via the device input, wherein the device input comprises at least one of a set of device inputs comprising: a button; a touch ID button; a touch sensor array; a touch key-pad; a motion detection unit; an accelerometer; an optical sensor array; and identifying a valid device user through an input detection, selected from at least one of a set comprising: a correct passcode entry sequence; a touch ID recognition of a known user; a biometric recognition of a valid user; a biometric sensing of a valid users skin; a biometric detection that the electronic device continuously remains in contact with a valid user; and receiving a correct user response input, from a security challenge presented on the display.

431. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 19 of the '579 Patent as a whole obvious. *See supra*, [1a], [1c], [7], [8], [11], [12].

432. A POSITA would have recognized that a valid PIN entry, as described above with respect to limitation [1a] and claim [8] and [12], provides a correct passcode entry sequence and a correct user response input from a security challenge. EX1007, 2:59-64, 5:13-18, 7:9-16, 20:43-21:20, 20:12-23. Gomez further discloses “a fingerprint reader” for detecting entry of “a fingerprint” which a POSITA would have recognized provides or at least renders obvious a touch ID button, touch sensor array, a biometric recognition of a known user, and a biometric recognition of a valid user. EX1007, 11: 15-18, 11:30-38, 5:13-18.

433. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 20 of the '579 Patent as a whole obvious to a POSITA.

19. Claim 22

[22] The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates from a card issuing authority and is for limited-use by the specific electronic device only; and wherein said static device-specific device account information is valid for a limited duration, and wherein the generating a limited-use payment information comprises the processor generating a one-time limited-use cryptogram number and combining said limited-use static device account information and said one-time use cryptogram number to produce the limited-use payment information.

434. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 19 of the '579 Patent as a whole obvious.

435. Gomez discloses that the memory is coupled to the processor. EX1007, 10:34-38. As discussed with respect to Claim [4], *supra* Gomez's seed value, which is used to generate the authentication cryptogram, "is *unique for each payment card*, and *corresponds to the payment card identifying number*," which can be the 16-digit number that is provided by a card issuing authority and provides static device-specific account information including a device account number of limited-use (i.e., limited in use to the specific card). EX1007, 1:44-47,

7:17-48, *see also id.*, 12:30-34, 13:45-14:2, 16:31-34, 16:64-17:13. The seed value is stored on the device. EX1007, 5:25-28. The seed value includes “a unique customer key.” EX1007, 7:31-41, 14:30-36 (describing using “an RSA key generated value” in place of the temporal value), 9:23-29. Amacker reveals that in the combination, the seed value (Amacker’s limited-use number) can be provided by the issuer. EX1008, 4:21-23, 11:58-12:8. Because Gomez discloses a number issued by a card issuer and Amacker discloses a data provider that may be a financial institution that generates the limited use number, in my opinion, the limited use number is provided by the issuer. Having the issuer provide the seed value would beneficially improve the system by ensuring that the seed value is known to the issuer (and payment processor) for purposes of verifying the authentication cryptogram.

436. As discussed with respect to Claim [4], *supra*, the payment card number has an “expiration date” and therefore, a POSITA would have recognized that, because the seed value “corresponds to the payment card identifying number,” the expiration date for the payment card number is also the expiration date for the seed value, meaning that the seed value has a limited time-duration of valid use. EX1007, 3:67-4:4, 5:50-57, 11:23-27, 7:17-48. Alternatively, it would have been obvious to a POSITA to make the seed value of a limited time-duration of valid use tied to the payment account expiration date so that a seed value generated using an

expired account number could not be used for transactions. This would help ensure that the user's account is still valid.

437. In my opinion, because the specification does not define “combine,” the claimed generated payment information is disclosed by generation of the “authentication cryptogram” based on the “seed value” and the “cryptographic hash” (one-time limited-use cryptogram number). *See* EX1007, 8:3-9:11.

438. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 22 of the '579 Patent as a whole obvious to a POSITA.

20. Claim 23

[23] The electronic device of claim 19 further comprising a cryptographic processor operable to dynamically generate a one-time limited-use cryptogram number by cryptographically combining of at least one information accessible on the electronic device, selected from a set comprising: a sequence counter; a device account number; a device secret; device keys; card issuer keys; a time; an amount; an expiration date; a card security code; a location; merchant information; NFC recipient information; payment reader information; an online location; transaction information; payment information; device information; user information; an email address; a user identification entry; a hash of transaction information; and a hashed record of transactions, and wherein said cryptogram number is operable to be used in place of at least a portion of a card issuer payment information, in a payment transaction.

439. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 19 of the '579 Patent as a whole obvious. It was

well known even by 2005 to include a cryptographic processor in a mobile phone to perform computation-intensive cryptographic operations. *See, e.g.,* EX1015.

440. Therefore, in my opinion, the combination of Gomez, Amacker, and Spodak would have rendered claim 23 of the '579 Patent as a whole obvious to a POSITA.

H. Ground 2B: Claims 10 and 14 of the '579 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Spodak, and Deibert

441. In my opinion, the combination of Gomez, Amacker, Spodak, and Deibert renders obvious claims 10 and 14 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Gomez, Amacker, Spodak, and Deibert

442. All four references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS. A POSITA would have applied the teachings of Deibert to the Gomez-Amacker-Spodak combination in the same manner, for the same reasons, and to achieve the same benefits discussed in Ground 1D, *supra*. For similar reasons, a POSITA would have had a reasonable expectation of success in making such a modification.

443. Specifically, a POSITA would have been prompted to apply the teachings of Deibert to the Gomez-Amacker-Spodak combination to include multiple techniques for disabling a payment priming operation (including through

completion of a transaction, manual user input, and expiration of a timeout period) to “help prevent the accidental transmittal of information,” provide increased functionality of allowing the user to intentionally return the device to an idle state, and to “allow[] the phone to have full contactless card functionality, while removing limitations.” EX1012, [0023]-[0025], [0061].

444. This modification also “minimize[s]” user concern and hesitancy regarding mobile payment transactions, thus increasing user satisfaction. EX1012, [0061]. Such a modification could also save power by decreasing the amount of time that the NFC circuit is actively transmitting payment information and increase ease of use by providing mechanisms for disabling payment priming that don’t require user interaction. Furthermore, a POSITA would have recognized that application of Deibert’s teachings to the Gomez-Amacker-Spodak is merely the application of known techniques to a known system ready for improvement to yield predictable results.

2. Claim 10

[10] The method of claim 1, further comprising: activating an NFC communication for a limited duration of time responsive to the electronic device priming; and responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction.

445. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the ’579 Patent as a whole obvious.

446. Deibert provides the additional limitation of claim [10] to the Gomez-Amacker-Spodak-Deibert combination for the same reasons discussed in Ground 1D, *supra*. See also *supra*, [1d]-[1e] (transactions conducted using NFC). Specifically, as with Gomez, Deibert similarly discloses using NFC to facilitate communications between the user device and merchant terminal during mobile payment transactions. EX1012, [0019], [0040]; EX1004, [0022], [0044], [0047]. Deibert describes manually activating a mobile application and, in response, “the mobile phone will transmit payment information.” EX1012, [0023].

447. A POSITA would have recognized this activation of the application to transmit payment information as a priming action. The communication of the transaction information is limited to “a predetermined timeout time” such that “[i]f no payment transaction occurs within the predetermined timeout time, then after the predetermined timeout time, the mobile payment application on the phone will automatically disable so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]. The manual activation can include “entering a password.” *Id.*, [0057]. A POSITA would have understood that terminating the mobile payment application provides, or at least renders obvious, terminating the NFC communication and aborting the transaction.

448. Therefore, in my opinion, the combination of Gomez, Amacker, Spodak, and Deibert would have rendered claim 10 of the '579 Patent as a whole obvious to a POSITA.

3. Claim 14

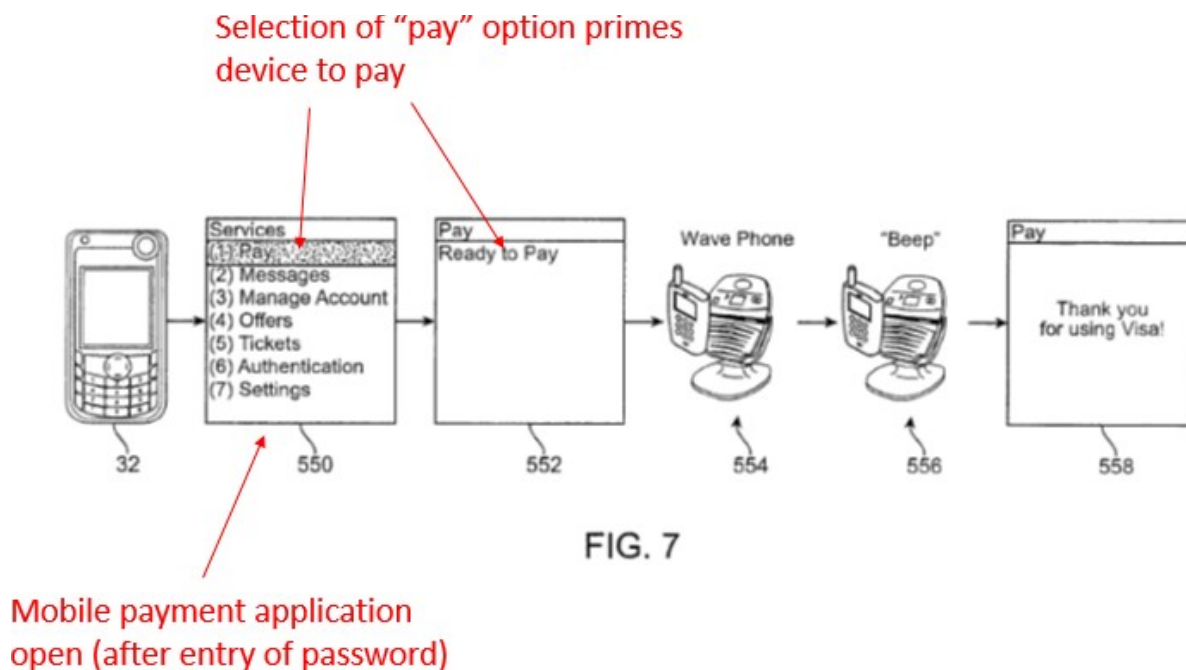
[14]: A method of claim 1, wherein the priming operation is input after at least one of: a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device, and validating a user passcode entry on the touch-screen display of the electronic device; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.

449. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

450. Gomez discloses requiring a PIN (a passcode) to access the payment application/functionality or prior to selecting a specific payment method. *Supra* Ground 2A, Claim [12]; EX1007, 20:43-21:20, 20:12-23. A POSITA would have recognized that a user PIN is a type of passcode and therefore entry of the PIN provides validating a user passcode entry on the touch-screen display of the electronic device. A POSITA would further have recognized that user selection of a payment method provides a priming operation after entry of the PIN/passcode.

451. Deibert similarly describes requiring “entering a password into the mobile phone application, in order to authenticate the consumer **30** and prevent

fraud.” EX1012, [0057], [0049] (“user is prompted to enter a password”). Deibert in the Gomez-Amacker-Spodak-Deibert combination discloses the additional recitations of Claim [14] for the same reasons discussed in Ground 1D, *supra*. For example, Deibert describes further priming operations after entry of the password, including manual activation of the payment application after expiration of a timeout period without requiring additional password entry “because the consumer has already been authenticated by entering the password the first time.” *Id.*, [0058], [0023] (describing that the user “***manually*** select[s] the mobile phone application ***each time*** before making a purchase). In another example, Deibert describes that after the payment application is opened (which can require entry of a password), the device requires a further priming operation of selecting the “pay functionality of the mobile payment application” to prime the device “to engage in a payment transaction.” *Id.*, [0060], [0057].



Id., FIG. 7, [0057], [0060].

452. Furthermore, a POSITA would have recognized that payment priming is a type of device priming. Deibert discloses disabling a device priming on further button pressing, stating that “the consumer can manually disable the mobile phone application, thereby returning the mobile phone to the idle state.” *Id.*, [0024].

Deibert further teaches that “[i]f no payment transaction occurs within the predetermined timeout time, then *after the predetermined timeout time, the mobile payment application on the phone will automatically disable* so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]. Additionally, [o]nce a transaction has occurred, the mobile phone can go back to the idle state.” *Id.*, [0024], [0059]-[0060].

453. Therefore, in my opinion, the combination of Gomez, Amacker, Spodak, and Deibert would have rendered claim 14 of the '579 Patent as a whole obvious to a POSITA.

I. Ground 2C: Claim 13 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Spodak, Deibert, and Power

454. In my opinion, the combination of Gomez, Amacker, Spodak, and Power renders obvious as a whole claim 13 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Power with the Combination of Gomez, Amacker, Spodak, and Deibert

455. All five references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS terminals. Further, all five references are concerned with security of wireless payment transactions. EX1007, 1:58-2:12; EX1008, 3:15-22; EX1009; [0002], [0027], [0034]; EX1012, [0004]; EX1016, 1:7-28. In particular, Deibert at [0004] addresses the problem of unauthorized “sniffing” of data from contactless cards and Power provides additional teachings that would have been beneficially applied to the combination of Gomez, Amacker, Spodak, and Deibert to prevent such unauthorized sniffing. A POSITA would have been motivated to adopt a selection of security mechanisms to enhance the security of the combination of Gomez, Amacker, Spodak, and Deibert based on these teachings of Power.

456. As discussed above, Power teaches a number of techniques for activating the wireless payment device only for an imminent transaction when the payment device is in physical contact with the user. EX1016, 1:58-67. This can be done using one or more of a resistive sensor, a capacitive sensor, or a pressure sensor for sensing that the user is holding the payment device. *Id.* A POSITA would have applied these teachings regarding only activating the device for a wireless payment transaction based on the teachings of Power to the combination of Royyuru, Phillips, Casey, and Deibert to “protect” transaction information from being inadvertently transmitted when the user does not intend to conduct a financial transaction. *Id.*, 2:47-3:5. This additional level of security would have further helped to prevent unintended or fraudulent charges to the user’s payment cards while “increas[e/ing] security.” *Id.* Furthermore, such protections are not overly burdensome and provide “ease of use” because the user only needs to make physical contact with the card to maintain the priming state. *Id.*

2. Claim 13

[13]: A method of claim 1, wherein the priming operation comprises: a button double press; and a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation; and further comprising: denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user, until after successfully re-validating a user; and wherein re-validating a user requires a correct user passcode re-entry; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.

457. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

458. A POSITA would have applied the teachings of Power to Gomez-Amacker-Spodak-Deibert in the same manner and for the same reasons as discussed with respect to the Royyuru-Phillips-Casey-Deibert-Power combination. *Supra*, Ground 1E.

459. Spodak discloses that the device can be primed to perform a payment transaction (“activated for use”) when the user pushes a button or taps or bends the universal card itself. EX1009, [0045], [0084]. This button push falls within the disclosure of a button double press in the '579 Patent. EX1001, 9:64-10:3, 17:19-23. A “button double press” could involve pressing the same button twice, or a sequence of two different buttons. There is no disclosure of pressing the same

button twice in the '579 Patent, so I understand “button double press” to comprise pressing two different buttons. Furthermore, Gomez discloses requiring PIN (passcode) entry to re-validate a user, which a POSITA would have recognized as adding an extra layer of security when combined with Power’s physical contact detection requirement. EX1007, 20:43-21:20, 20:12-23.

460. Furthermore, a POSITA would have applied the teachings of Power to Gomez-Amacker-Spodak-Deibert to require biometric sensing of the device continuously remaining in contact of the valid user (e.g., using Power’s capacitive sensor) and disabling the priming operation when the device is not continuously in contact with the user. Power teaches that the device “detects a presence or an absence of a gating signal.” EX1016, 2:1-3. In some embodiments, presence of the gating signal (to allow use of a smart payment device) requires continued contact with “the customer’s body.” *Id.*, 4:37-43. The device includes a transducer to “monitor[] the one or more physical phenomena” and enables/disables the wireless-communication circuit in response to detection or absence of the physical phenomena. *Id.*, 2:52-60, 3:51-67. The transducer(s) can detect a temperature, resistance, capacitance, or pressure change “when the user is holding the payment card” such that the device “is only active (and able to communicate the financial information) when it is being used by customer.” *Id.*, 1:55-62, 3:65-4:19.

461. A POSITA would have applied these teachings of Power to Gomez-Amacker-Spodak-Deibert to protect transaction information from being inadvertently transmitted when the user does not intend to conduct a financial transaction, thereby preventing unintended or fraudulent charges to the user's payment cards and "increas[e/ing] security." EX1016, 2:47-3:5.

462. Deibert provides that the Gomez-Amacker-Spodak-Power combination provides all remaining elements of claim 13 for the reasons discussed in Grounds 1D-1E, 2B, *supra*. Specifically, Deibert discloses disabling a device priming on further button pressing, stating that "the consumer can manually disable the mobile phone application, thereby returning the mobile phone to the idle state." EX1012, [0024]. Deibert further teaches that "[i]f no payment transaction occurs within the predetermined timeout time, then ***after the predetermined timeout time, the mobile payment application on the phone will automatically disable*** so that contactless payments cannot be made." *Id.*, [0025]-[0026], [0058]. Additionally, "[o]nce a transaction has occurred, the mobile phone can go back to the idle state." *Id.*, [0024], [0059]-[0060].

463. Therefore, in my opinion, the combination of Gomez, Amacker, Spodak, Deibert, and Power would have rendered claim 13 of the '579 Patent as a whole obvious to a POSITA.

J. Ground 2D: Claims 4 and 22 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Spodak, and Carlson

464. In my opinion, the combination of Gomez, Amacker, Spodak, and Carlson renders obvious claims 4 and 22 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Carlson with Gomez, Amacker, and Spodak

465. All four references are not only in the same field of endeavor, but deal specifically with consumer transactions conducted at contactless merchant POS.

466. A POSITA would have been prompted to apply the teachings of Carlson to the Gomez-Amacker-Spodak combination such that Gomez's seed value is "set to expire...after a certain time period" because "[d]oing so can help to ensure that if for some reason [the seed value] is revealed to anyone other than an authorized user, the amount of damage that can be done is limited due to the limited lifetime of the pseudo primary account number." *See* EX1013, [0036].

Implementing the seed value to "have a limited lifetime... provides a level of protection to the consumer's account" because it would likely "expire[]" before any illicit use could be made." *Id.*, [0044]. Therefore, setting an expiration for the seed value can prevent fraudulent use of the seed value to generate authentication cryptograms by unauthorized devices.

467. Furthermore, a POSITA would have recognized that application of Carlson's teachings to the Gomez-Amacker-Spodak system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification.

2. Claim 4

[4]: The method of claim 1, wherein a limited-use number comprises a device account number, and wherein the device account number is of a limited time-duration of valid use, and wherein further a card issuing authority provides said device account number for use only by the electronic device, in place of card issuer information in performing payment transactions by the electronic device, and further comprising: performing payment transactions by the electronic device including the limited-use number; combining the limited-use number and said device account number within a device generated payment information; and conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.

468. As shown above, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 1 of the '579 Patent as a whole obvious.

469. In the Gomez-Amacker-Spodak-Carlson system, the seed value is "set to expire...after a certain time period" by the payment processor or issuer.

EX1013, [0036], [0044], [0086]. The seed value therefore has an expiration date of limited duration of validity and is therefore of limited time-duration of valid use.

All other limitations of claim [4] are disclosed by the Gomez-Amacker-Spodak-Carlson combination for the reasons discussed in Ground 2A, *supra*.

470. Therefore, in my opinion, the combination of Gomez, Amacker, Spodak, and Carlson would have rendered claim 4 of the '579 Patent as a whole obvious to a POSITA.

3. Claim 22

[22]: The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates from a card issuing authority and is for limited-use by the specific electronic device only; and wherein said static device-specific device account information is valid for a limited duration, and wherein the generating a limited-use payment information comprises the processor generating a one-time limited-use cryptogram number and combining said limited-use static device account information and said one-time use cryptogram number to produce the limited-use payment information.

471. As shown above in Ground 2A, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 19 of the '579 Patent as a whole obvious.

472. The “limited duration” limitation of claim 22 is disclosed by Carlson. As discussed above, in the Gomez-Amacker-Spodak-Carlson system, the seed value is “set to expire...after a certain time period” by the payment processor or issuer.

EX1013, [0036], [0044], [0086]. The seed value therefore has an expiration date of

limited duration of validity and is therefore of limited time-duration of valid use. All other limitations of claim [22] are disclosed by the Gomez-Amacker-Spodak-Carlson combination for the reasons discussed in Ground 2A, *supra*.

473. Therefore, in my opinion, the combination of Gomez, Amacker, Spodak, and Carlson would have rendered claim 22 of the '579 Patent as a whole obvious to a POSITA.

K. Ground 2E: Claim 21 of the '579 Patent Is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker Spodak, Carlson, and Royyuru

474. In my opinion, the combination of Gomez, Amacker, Spodak, Carlson, and Royyuru renders obvious as a whole claim 21 of the '579 Patent for at least the reasons discussed below.

1. Motivation to Combine Royyuru with Gomez, Amacker, Spodak, and Carlson

475. A POSITA would have been prompted to apply the teachings of Royyuru to the Gomez-Amacker-Spodak-Carlson to use additional values when generating the authentication cryptogram including one or more unpredictable/undeterminable and one or more expiration dates. EX1004, [0057], [0051]. A POSITA would have recognized that using these additional values when generating Gomez's authentication cryptogram would have increased security because the cryptogram would be based on additional values that would be difficult for third parties to determine or intercept to allow the device to more "securely

handl[e] a financial transaction.” EX1004, [0004]. Furthermore, a POSITA would have recognized that application of Royyuru’s teachings to the Gomez-Amacker-Spodak-Carlson system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification.

476. In applying Royyuru to the Gomez-Amacker-Spodak-Carlson combination, a POSITA would have recognized that it would have been beneficial to combine the seed value with the expiration date for the seed value when generating the authentication cryptogram in the combination to increase the difficulty for third parties to replicate the authentication cryptogram. Carlson teaches that in the combination the seed value is “set to expire...after a certain time period” by the payment processor or issuer. EX1013, [0036], [0044], [0086]; *supra* Ground 2D. Royyuru discloses that values similar to the seed value (Royyuru’s IKCV) can be combined with their respective expiration dates or other unpredictable/undeterminable numbers known to the device (which would include the expiration for the seed value in the combination) to increase security of the cryptogram. EX1004, [0057], [0051].

2. Claim 21

[21]: The electronic device of claim 19, wherein the memory is accessible to the processor, wherein said memory comprises a static device-specific device account number of limited-use that originates from a card issuing authority and is limited to use by the electronic device in place of a card issuer account information, wherein further said static device-specific device account number has an expiration date of limited duration of validity, and wherein the generating a limited-use payment information comprises the processor generating said limited-use payment information by combining said static device-specific device account number, said device account expiration date, when said issuer payment account method is selected.

477. As shown above in Ground 2A, the combination of Gomez, Amacker, and Spodak would have rendered parent claim 19 of the '579 Patent as a whole obvious.

478. In applying Royyuru to the Gomez-Amacker-Spodak-Carlson combination, a POSITA would have recognized that it would have been beneficial to combine the seed value with the expiration date for the seed value when generating the authentication cryptogram in the combination to increase the difficulty for third parties to replicate the authentication cryptogram. Carlson teaches that in the combination the seed value is “set to expire...after a certain time period” by the payment processor or issuer. EX1013, [0036], [0044], [0086]; *supra* Ground 2D. Royyuru discloses that values similar to the seed value (Royyuru’s IKCV) can be combined with their respective expiration dates or other

unpredictable/undeterminable numbers known to the device (which would include the expiration for the seed value in the combination) to increase security of the cryptogram. EX1004, [0057], [0051]. The Gomez-Amacker-Spodak-Carlson-Royyuru combination provides the remaining limitations of Claim [21] for the reasons discussed with respect to Claim [4] (Grounds 2A, 2D) and Claim [22] (Grounds 2A, 2D), *supra*.

479. A POSITA would have applied the teachings of Carlson to the Gomez-Amacker-Spodak combination to set the seed value to expire after a certain time period in the same manner and for the same reasons discussed in Ground 2D, *supra*. All other limitations of claim [21] are disclosed by the Gomez-Amacker-Spodak-Carlson combination for the reasons discussed in Ground 2A *supra*.

480. Therefore, in my opinion, the combination of Gomez, Amacker, Spodak, Carlson, and Royyuru would have rendered claim 21 of the '579 Patent as a whole obvious to a POSITA.

XI. JURAT

481. In signing this Declaration, I understand that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear remotely for

cross-examination within the United States during the time allotted for cross-examination.

482. I hereby declare that all statements made in this Declaration of my own knowledge are true, that all statements made on information and belief are believed to be true, and further, that these statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: July 20, 2025 By: 

Michael I. Shamos, Ph.D.