

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EARLY WARNING SERVICES, LLC
Petitioner

v.

INTELLECTUAL VENTURES II LLC
Patent Owner

IPR2024-01221

U.S. Patent No. 7,314,167

DECLARATION OF THOMAS PURVES

TABLE OF CONTENTS

	Pages
I, Thomas Purves, declare as follows:	6
I. BACKGROUND AND QUALIFICATIONS	6
II. LEVEL OF SKILL IN THE ART	11
III. LEGAL STANDARDS	12
A. Anticipation	12
B. Obviousness.....	12
C. Printed Publication Prior Art.....	15
D. IPR Standard.....	16
IV. THE '167 PATENT	16
V. TECHNICAL BACKGROUND	19
A. Wang et al. (Ex. 1004)	19
B. Take an Order (Ex. 1005).....	20
C. Palm Treo Manual (Ex. 1006).....	23
D. Drummond (Ex. 1008)	25
E. Raines (Ex. 1009).....	26
F. Denso (Ex. 1026).....	27
VI. CLAIM CONSTRUCTION	27
A. "Forward"	27

B.	“Image capture device”	28
C.	“Predetermined Information”	31
VII.	INVALIDITY ANALYSIS	31
A.	Overview	31
A.	Ground I: Claims 1, 4, 5, 7, 12, 17, 23, 26, 27, 29, 34, and 43 are anticipating by Wang and obvious over Wang in view of Drummond.	32
	Independent Claim 1	35
	Dependent Claim 4	52
	Dependent Claim 5	52
	Dependent Claim 7	52
	Dependent Claim 12	53
	Dependent Claim 17	53
	Independent Claim 23	53
	Dependent Claim 26	59
	Dependent Claim 27	59
	Dependent Claim 29	60
	Dependent Claim 34	60
	Independent Claim 43	60
B.	GROUND II: Wang anticipates Claims 1, 2, 4, 7, 12, and 17.	61

Independent Claim 1	62
Dependent Claim 2	66
Dependent Claim 4	66
Dependent Claim 7	67
Dependent Claim 12	67
Dependent Claim 17	67
C. GROUND III: Claims 19-21 and 39-41 are obvious over Wang in view of Drummond.	67
Independent Claim 19	70
Dependent Claim 20	76
Dependent Claim 21	76
Independent Claim 39	76
Dependent Claim 40	77
Dependent Claim 41	77
D. GROUND IV: Claims 8 and 30 are obvious over Wang and Denso.	77
Dependent Claims 8, 30	80
E. GROUND V: Claim 13 is obvious over Wang and Raines.	80
Dependent Claim 13	83
F. GROUND VI: Claims 1, 4, 5, 7, 23, 26, 27, 29, and 43 are obvious over TAO in view of PTM and Wang.....	85

Independent Claim 1	91
Dependent Claim 4.....	96
Dependent Claim 5.....	96
Dependent Claim 7.....	97
Independent Claim 23	97
Dependent Claim 26.....	99
Dependent Claim 27.....	100
Dependent Claim 29.....	100
Independent Claim 43	100
VIII. CONCLUSION.....	101
SKILLS	115
PROFESSIONAL EXPERIENCE.....	115
EARLY CAREER.....	116
EDUCATION	116
STARTUP & INDUSTRY LEADERSHIP.....	117

I, Thomas Purves, declare as follows:

I. BACKGROUND AND QUALIFICATIONS

1. I am over eighteen years of age, and I am competent to testify as to the matters set forth herein if I am called upon to do so.
2. I have prepared this Declaration for consideration by the Patent Trial and Appeal Board in an Inter Partes Review of U.S. Patent No. 7,314,167 (“the ’167 patent”) (Ex. 1001).
3. I have written this Declaration at the request of Kilpatrick Townsend & Stockton, LLP, which represents Early Warning Services, LLC (“Petitioner”) in connection with the above-captioned Inter Partes Review. My compensation is hourly and unaffected by the substance or outcome of my opinions.
4. In forming my opinions, in addition to my knowledge and experience, I have considered the Petition filed by Petitioner and the Exhibits listed in Appendix B. I agree with all factual assertions contained in the Petition.
5. All statements in my Declaration, unless indicated otherwise, are based on my knowledge and experience in the field.
6. I have over 25 years of experience in the fields of payment transaction systems and secure digital banking. I have developed a robust expertise in designing and implementing secure electronic transaction solutions. Currently, I serve as an independent fintech consultant and expert advisor at Lahave

Technologies Inc., where I leverage my extensive background to advise innovative financial services companies in technical product design and commercialization strategy.

7. I received a BSc in Computer & Electrical Engineering in 1998 from Queen’s University, Kingston, Ontario, Canada. My degree studies included microprocessor design, computer architecture, computer programming, computer vision, and image processing, which provided a solid technical foundation for my subsequent work in secure electronic transactions and digital banking.

8. From May 1997 to October 2000, I was employed by TD Bank Product Designer, Online Services. At TD Bank, I led the product and user experience design for “TD WebBanking,” at the time recognized as Canada’s most award-winning online banking service by third parties such as Gomez and Quicken.ca. I was responsible for designing secure online banking services, including loan and account applications over encrypted channels, secure authentication, and everyday banking transactions. Additionally, I researched and prototyped solutions for delivering WAP-based mobile banking services to early cell phones and PDAs.

9. From December 2000 to November 2002, I was employed as a CertaPay Product Manager. At CertaPay, a fintech SaaS startup, I led product development, launch, and growth of “EmailMoney Transfers”—the world’s first real-time inter-bank person-to-person payment platform. This service, built as a SaaS solution,

was ultimately adopted by all Canadian financial institutions and processes over \$40 billion in annual payment volume today. While at CertaPay, I also was responsible for designing the user experiences and technical specifications for an online commerce payment scheme Interac Online.

10. In the 2002-2003 time frame, I made critical technical and design contributions to the creation of multiple secure domestic payment schemes still ubiquitously used in Canada: Interac E-Transfers, and Interac Online Debit. In 2003, as a consultant to Visa Inc., I contributed a whitepaper on the technical design for the 3D Secure technical standard for secure electronic transactions. This contribution helped shape the development of secure payment protocols that are still in use today.

11. From February 2003 to February 2006, I was employed as a Group Manager, New Product Development, for CIBC Bank in Toronto, Canada. In this role, I led product innovation initiatives, researching, evaluating, and developing new payment products for CIBC Bank. I led the CIBC program that implemented the new ecommerce payment scheme Interac Online, a system that required sophisticated methods for users to remotely, and securely, authenticate themselves to their financial institution and authorize access to deposit account, while shopping at an ecommerce merchant. This project also depended on encryption technologies and digital signatures for secure communication and relied on pre-

determined information such as pre-established online-banking passwords for authentication. While at CIBC, I was instrumental in the development of digital e-money products such as transit payment smart cards, and secure portable payment devices such as nearfield-wireless fob devices.

12. From June 2007 to Sept. 2011, I served as Business Leader, Product Innovation, for Visa Canada Inc. As Visa Canada's Innovation and New Products Specialist, I adapted and launched multiple new products in the market including world-first NFC mobile payments pilots. These projects involved the development and testing of encrypted payment credentials stored within mobile phones. This work also involved the development and testing of new payment standards and messaging protocols for communicating transaction data between mobile devices and point of sale terminals.

13. From October 2011 to April 2021, I was employed in various positions as Vice President, Global Digital Products in San Francisco, California. My two main roles between 2011 and 2021 were Visa Checkout, and Global Product Architecture. At Visa Inc., I led the product and engineering teams responsible for building the Visa Checkout digital wallet and checkout button. Visa Checkout has been used by over 45 million global users and the digital checkout button was integrated into hundreds of thousands of web and smartphone mobile applications. I was able to lead this role thanks to my established deep technical expertise in

secure electronic transaction systems, mobile devices and related technologies. During my tenure at Visa Inc., I was a prolific inventor and solution innovator, with over 80 global patent grants in fields of mobile payments, QR code payments, digital wallets and transaction processing. These patents underscore my contributions to the advancement of secure payment systems, as well as the constituent security, encryption and authentication sub-components that are essential to the functional those systems.

14. As the head of the Buyer Digital Enablement Team at Visa Inc., I created and commercialized products that facilitated the secure encryption and storage of credit card payment credentials in mobile digital wallets such as Apple ApplePay, Google AndroidPay and Samsung's SamsungPay.

15. With 25+ years in payment transaction systems and secure digital banking, I have consistently been at the forefront of technological advancements in secure electronic transactions. At TD Bank, I developed systems and user experiences for secure online banking, including loan and account applications over encrypted channels and secure authentication for everyday banking transactions. I also researched and prototyped solutions for delivering WAP-based mobile banking services to early cell phones and PDAs.

16. During my time at CertaPay, I designed secure methods for person-to-person money transfers using advanced cryptography, protected by pass-codes and

passwords, which also relied on commonly available message protocols of email and SMS for communicating transaction data from sender to recipient.

17. With a career spanning over two decades, I have demonstrated a consistent ability to innovate and lead in the field of secure electronic transactions. My extensive experience, coupled with a strong technical background and numerous contributions to industry standards, positions me as a leading expert in this domain.

18. My *Curriculum Vitae* is appended hereto as Appendix C.

II. LEVEL OF SKILL IN THE ART

19. I understand that a person of ordinary skill in the art (“POSA”) is a hypothetical person presumed to be aware of all pertinent art, to think along with the conventional wisdom in the art, and to have ordinary creativity. It is my opinion that, for the ’167 patent, a POSA is a person with a relatively high level of skill, such as having at least a bachelor’s degree in the field of computer science and/or electrical engineering, together with 2-3 years in the financial technology sector. The POSA would have knowledge of the commercial and scientific literature pertaining to securing transactions, before the priority date. A POSA would also have knowledge of processing devices.

20. As of the earliest priority date of the ’167 patent, I met and, in fact, exceeded the standard for a POSA. I am an expert in the relevant field.

III. LEGAL STANDARDS

A. Anticipation

21. I am not an attorney and have no formal legal training. But I have been advised by the Kilpatrick attorneys that a claim is anticipated if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.

22. I understand that a prior art reference that fails to expressly set forth a particular element of a claim still anticipates the claim if that element is “inherent” in the disclosure. I understand that this principle applies even if the inherent feature would not have been recognized by a POSA. Thus, a limitation claiming the “natural result” flowing from the prior art’s limitations is considered disclosed in the prior art.

B. Obviousness

23. I further understand that a claim is obvious in light of the prior art if the difference or differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious, at the time the invention was made, to a person having ordinary skill in the art.

24. I understand that several factual inquiries underlie a determination of obviousness. These inquiries include (1) scope and content of the prior art, (2) the

level of ordinary skill in the field of the invention, (3) the differences between the claimed invention and the prior art, and (4) any objective evidence of non-obviousness. Such objective evidence of non-obviousness include the invention's commercial success, commercial acquiescence (i.e., licensing), a long felt but unresolved need, the failure of others, skepticism by experts, praise by others, teaching away by others, recognition of a problem, laudatory statements by the infringer, and copying of the invention by others.

25. I have been advised that it is against this backdrop that the obviousness or non-obviousness of the subject matter is determined. The party challenging the patent must also show that one of ordinary skill in the art would have a reason to combine the elements as recited in the claims. A claim is unpatentable if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Furthermore, I understand that there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

26. I understand that the obviousness analysis does not require express teachings but may be based on the common sense, inferences, and creative steps expected of a person of ordinary skill in the art. I understand that this expansive and flexible approach, not only permits, but requires, consideration of common

knowledge and common sense. Additionally, I understand that when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. I understand that the inquiry is whether the improvement is more than the predictable use of prior art elements according to their established function.

27. I understand the test for obviousness is an expansive and flexible approach using common sense. I also understand that any need or problem known in the field of endeavor at the time of invention can provide a reason for combining the elements in the manner claimed. I further understand that certain factors may show obviousness:

- a. a combination of known elements with no change in their respective functions is likely to be obvious when the combination does no more than yield predictable results,
- b. a predictable variation of a work in the same or a different field of endeavor is likely to be obvious if a person of ordinary skill would be able to implement the variation without undue experimentation,
- c. an invention is likely obvious if it is the use of a known technique to improve a similar device in the same way, unless the actual

application of the technique would have been beyond the skill of the person of ordinary skill in the art,

- d. an invention is likely obvious if there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims,
- e. inventions that were "obvious to try" — chosen from a finite number of identified, predictable solutions, with a reasonable expectation of success — are likely obvious, and
- f. an explicit teaching, suggestion, or motivation in the art to combine references, while not a requirement for a finding of obviousness, remains "a helpful insight" in determining upon which a finding of obviousness may be based.

28. Finally, I understand that in determining whether a claim is obvious, obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

C. Printed Publication Prior Art

29. I understand that prior art may come in different forms, one of which is a printed publication. I have been told that public accessibility is the "touchstone" of whether a reference constitutes a printed publication. I understand that determining whether a reference is publicly accessible and thus qualifies as a printed publication requires a case-by-case inquiry into the facts surrounding the

reference's disclosure to members of the public. I understand that this factual inquiry broadly considers whether the reference was disseminated or otherwise made available such that the POSA, exercising reasonable diligence, would have been able to find the reference. I understand that an important factor in determining whether a document is a printed publication is the perceived purpose of the document.

30. I also understand that establishing a specific date of public accessibility of a printed publication, although helpful, is not necessary for a document to qualify as a printed publication. For example, evidence of routine business practices regarding accessibility is sufficient to establish an approximate date when a reference became accessible. This is especially persuasive, I understand, where the approximate accessibility date is well in advance of the effective filing date.

D. IPR Standard

31. I have been advised that an IPR petition must demonstrate "a reasonable likelihood that the petitioner would prevail with respect to at least one of the claims challenged in the petition." It is my opinion that the Petition exceeds that threshold.

IV. THE '167 PATENT

32. The '167 patent is directed to an apparatus for providing a secure transaction. Ex. 1001, abstract. The apparatus includes an image capture device

configured to capture an image, the image having information embedded therein.

Id. The apparatus also comprises a memory configured to store predetermined information, an input unit configured to receive input information provided by a user, a processor, and an output unit. *Id.* The processor is configured to verify the user based on the input information to ensure that the user is authorized to use the apparatus, and generate an output based on the information embedded in the image and the predetermined information. *Id.* The output unit is configured to forward the output generated by the processor. *Id.* Each component of this apparatus, as well as the combination and use of these components, was known in the art prior to the priority date of the '167 patent.

33. Challenged claim 1 is illustrative of the apparatus claimed in the patent and is comprised exclusively of conventional components:

1. An apparatus for providing a secure transaction, the apparatus comprising:
 - an image capture device configured to capture an image, the image having information embedded therein including information relating to a transaction;
 - a memory configured to store predetermined information;
 - an input unit configured to receive input information provided by a user; a processor configured to:
 - verify the user based on the input information to ensure that the user is authorized to use the apparatus; and

generate an output based on the information embedded in the image and the predetermined information; and
an output unit configured to forward the output generated by the processor,
wherein the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.

34. U.S. Patent No. 7,314,167 (“the ’167 patent”) is entitled “Methods and Apparatus for Providing Secure Identification, Verification and Authorization.” Ex. 1001. The ’167 patent issued on January 1, 2008 from Application No. 11/075,493, which was filed on March 8, 2005. *Id.* The ’167 patent is thus subject to pre-AIA § 102 and § 103 and is eligible for IPR.¹

35. It is my understanding that Petitioner requests cancellation of Claims 1, 2, 4, 5, 7, 8, 12, 13, 17, 19-21, 23, 26, 27, 29, 30, 34, 39-41, and 43 (“Challenged Claims”) of the ’167 patent.

36. The Challenged Claims are directed to an apparatus and a method for providing a secure transaction. Each apparatus claim recites well-known features,

¹ I understand that the “critical date” for prior art for purposes of this IPR is one year prior to the date for which the claim is entitled to priority. I also understand that any publicly available document that existed before the priority date can constitute prior art.

such as: 1) a device configured to capture an image, the image having information embedded therein (e.g., a bar code), 2) a memory, 3) an input unit, 4) a processor, and 5) an output unit. Ex. 1001 at 16:22-38. Each method claim similarly recites: 1) capturing an image having information embedded therein, 2) storing information, 3) receiving an input, 4) verifying the input, and 5) generating an output. The '167 patent describes common components and methods well known in the art, and the prior art anticipates or renders obvious each of the Challenged Claims.

V. TECHNICAL BACKGROUND

A. Wang et al. (Ex. 1004)

37. U.S. Patent Publication No. 2002/0023215 to Wang et al. (“Wang”) was published on February 21, 2002, more than a year before the priority date of the '167 patent and is thus prior art. Wang is directed to systems and methods of conducting secure transactions and is therefore in the same field of endeavor as the '167 patent.

38. Wang discloses a portable apparatus (a “PEAD”) that is usable to perform secure transactions. Ex. 1004 at [0002]. The PEAD includes a barcode scanner or optical character recognition (OCR) reader, two types of image capture devices, that read information from a barcode or UPC code to select an item for a transaction. *Id.* at [0115]. The PEAD also includes a memory that stores various

data (e.g., predetermined information), such as user identification data and a user's private key. *Id.* at [0044], [0115]. The apparatus generates transaction approval data and digitally signed receipts (e.g., outputs) based on the information from the barcode and the stored predetermined information. Ex. 1004 at [0051], [0055], [0085], [0115]. Wang also describes that accessing the user's predetermined private key to sign the output also depends on the apparatus verifying the user based on user inputs (e.g. passcode). The apparatus then forwards the transaction approval data and digitally signed receipts. Ex. 1004 at [0055], [0115].

B. Take an Order (Ex. 1005)

39. Take an Order ("TAO") is a prior art printed publication. TAO is directed to systems and methods of conducting financial transactions and is therefore in the same field of endeavor as the '167 patent.

40. TAO is a prior art printed publication in the form of a product advertisement which was generally available and known to the relevant technical community more than six months before the earliest possible priority date of the '167 patent. Ex. 1034 at 1-7.

41. Ex. 1034 is an Internet Archive declaration relating to an Aug. 25, 2004 capture of the TAO website. Ex. 1005 contains the same TAO capture and is a

true and accurate copy of the TAO web page as captured by the Internet Archive as of that date. Ex. 1034 at 1-7.

42. A reference is publicly available (and therefore, constitutes a prior art publication) if it is disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence can locate it. A POSA would have easily been able to access TAO using reasonable diligence to locate it.

43. Stevens Creek software was a well-known vendor of Palm software. A POSA of mobile device software of the era would recognize them as a leading developer of Palm software given their association with Palm's developer program and awards at Palm-sponsored developer conferences. *See* Ex. 1013 (<https://web.archive.org/web/20050402014734/http://stevenscreek.com/palm/custom.html>) ("1998 - Stevens Creek Software wins programming contest at Palm Developer's Conference," "1999 – Stevens Creek Software wins programming contest at Palm Developer's Conference!," "2001 - Stevens Creek Software's President, Steven Patt, becomes one of the first 'Palm-Powered Certified Developers,'""). *See also* Ex. 1028 at 2 (indicating "Stevens Creek Software is one of the premier software developers for the Palm Computing platform" and directing users to their website); Ex. 1029 at 1-2 (touting the TAO app, stating "Stevens Creek Software...is one of the leading developers of software for Palm,"

and directing those interested in such software to www.stevenscreek.com). As evidenced by the foregoing, a POSA would have known that Stevens Creek Software was a leading provider of software solutions for the Palm Computing Platform, and a POSA searching for Palm software solutions would have known to access the Stevens Creek website to learn about their software products.

44. Also, since the website was indexed and searchable, a POSA conducting a simple internet search using terms such as “Palm Treo,” “taking orders,” and “point of sale software” would be expected to return the Take and Order! website at the top of their internet search results. In fact, the Stevens Creek Software homepage was one of the top three search results when I conducted this search strategy. Once at the website, a POSA would be easily able to access TAO from the Stevens Creek Software home page with only one mouse click: Home Page→Take An Order! Ex. 1034 at 8-10 (Home Page) → Ex. 1034 at 4-7 (Take An Order!).

45. Additionally, TAO is a website advertisement that, by its very nature, is a public-facing document, further supporting that it is a printed publication. The totality of the evidence supports that TAO was publicly accessible to those skilled in the art and constitutes a printed publication at least as of August 2004.

46. TAO discloses software that is executable on a Palm Treo device. Ex. 1005, 1-3. The software enables the Palm Treo device to scan a barcode of an item to

add an item to an order (e.g., an output). *Id.* For existing customers having a standard discount (e.g., predetermined information), the order is automatically updated to reflect the discount. *Id.* at 1-2. Thus, the orders are generated based on both (i) barcode image information and (ii) predetermined discount information. TAO discloses that the order is forwarded to the user's desktop computer. *Id.* at 3.

C. Palm Treo Manual (Ex. 1006)

47. Palm Treo Manual ("PTM") is a user manual for the Palm Treo 600 device and was published as early as June 2004, i.e., before the priority date of the '167 patent. The PTM bears all of the hallmarks of a printed publication, including the indicia: "Copyright (c) 2004 palmOne, Inc. All rights reserved." Ex. 1006 at 2. As a publicly traded company with sales in the millions of devices (Ex. 1011), Palm would have been considered a reputable publisher for its product literature.

48. PTM is a prior art printed publication that was generally available, known, and accessible to the relevant technical community before the earliest possible priority date of the '167 patent. Ex. 1010 (confirming that PTM was available on the Palm webpage as indexed by the Internet Archive on June 12, 2004).

49. A POSA would have known that Palm was a leading provider of mobile devices such as the Palm Treo 600. In 2005, a person of ordinary skill in the art would recognize Palm Inc. as a leading vendor of mobile devices due to their significant market share. Through its history, Palm developed multiple popular

product lines, such as the PalmPilot (1996) and Treo 650 (2005) series, which were widely reviewed and acknowledged for having strong smartphone capabilities. Palm's devices were frequently reviewed and recommended in industry publications for their reliability and user-friendly interfaces. In 2005, New York Times columnist David Pogue wrote about the Palm Treo 650. In that column he described in 1996 how "Palm Computing developed the smash-hit Pilot organizer." Pogue, "The Awkward Smart Phone Grows Up," *New York Times* (June 30, 2005). Ex. 1025 at 1. In that article, he praised specific features of the model as "At 320 by 320 pixels, the bright, gorgeous color screen offers higher resolution than most rivals, meaning supersharp (if tiny) text and graphics. It's also a touch screen -- a skinny stylus tucks into the back of the phone -- which is handy if you install any of the thousands of Palm-compatible programs available online." *Id.* at 3.

50. In view of the notoriety of the Palm system, a POSA would have known that Palm was a leading provider of mobile devices such as the Palm Treo 600 and would have been able to easily access the PTM at least by conducting an internet search or accessing the Palm website. For example, since the Palm website was indexed and searchable, a POSA conducting a simple internet search using terms such as "Palm Treo 600" and "user manual" would be expected to return the PTM at the top of their search results. In fact, when I conducted such a search, the PTM

was the top search result. Moreover, a POSA would expect that they could access user manuals such as PTM on the Palm website as was the common practice in the industry. Specifically, a POSA would be easily able to access the PTM from the PalmOne home page (<http://www.palmone.com/us>) with only 4 mouse clicks: Home Page→Support→choose your model→Treo 600 (GSM)→User Guide. Ex. 1010 at 15→13→17→17→119-199.

51. Additionally, the PTM is a user manual that, by its very nature, is a public-facing document distributed with the smartphone packaging itself, further supporting that it is a printed publication. Ex. 1010 at 8 (“Inside the Treo 600 box is a...fairly thick user manual...”). The totality of the evidence supports that the PTM was publicly accessible to those skilled in the art and constitutes a printed publication at least as of June 2004.

52. PTM discloses that Palm Treo devices included internal memory and a processor. Ex. 1006 at 97, 109, 112, 173. PTM also discloses that the Palm Treo devices had keyboards and system locks that required a password to be entered on the device prior to accessing data stored on the device. Ex. 1006 at 24, 129.

D. Drummond (Ex. 1008)

53. U.S. Patent Publication No. 2003/0217005 to Drummond et al. (“Drummond”) was published on November 20, 2003, more than a year before the priority date of the ’167 patent. Drummond is directed to systems and methods of

conducting secure transactions and is therefore in the same field of endeavor as the '167 patent.

54. Drummond discloses that in addition or alternatively to receiving paper receipts, electronic receipts may be sent to one or more devices. Ex. 1008 at [0246], [0247]. The electronic receipts are sent via e-mail and/or text message (e.g., SMS), which enables the customer to: (1) choose to receive the receipt at a computer, such as their home or work computer, mobile phone, pager, PDA, other hand-held or portable computing device, or another device capable of receiving a message, (2) determine the level of information in the receipt, and (3) send additional receipt copies to additional selected systems and system addresses (e.g., a receipt may be sent to an associate or a party to a business transaction as an indication that a deposit or payment on a loan was made). Ex. 1008 at [0247]-[0251], [0301], [0307].

E. Raines (Ex. 1009)

55. U.S. Patent Publication No. 2004/0193538 to Raines ("Raines") was published on September 30, 2004, before the priority date of the '167 patent. Raines is directed to systems and methods of conducting secure transactions and is therefore in the same field of endeavor as the '167 patent. Raines discloses that transaction data in a credit card transaction includes an account number and credit card expiration data. Ex. 1009 at [0008].

F. Denso (Ex. 1026)

56. Japanese Patent Publication No. JP 2002-109420 to Denso Co. Ltd. (“Denso”) was published on April 12, 2002, more than a year before the priority date of the ’167 patent and is thus prior art under pre-AIA 35 U.S.C. § 102(b). Denso is directed to systems and methods of data communication, and in particular, data communication using two-dimensional matrix codes, and is therefore in the same field of endeavor as the ’167 patent. Ex. 1026 at [0019].

VI. CLAIM CONSTRUCTION

57. I understand that claims are construed in IPRs under the so-called *Phillips* standard in which claim terms are given their ordinary and customary meaning as understood by a POSA in view of the patent specification and prosecution history. I understand that an applicant’s statements characterizing its invention during prosecution may give rise to a disclaimer.

A. “Forward”

58. Independent claims 1 and 14 recite “an **output unit** configured to **forward** the output generated by the processor.” Ex. 1001 at 16:34-25; 17:10-11.

Independent claims 23, 39, and 43 each recite “**forward** the generated output to the user....” Ex. 1001 at 17:61, 18:60, 20:3. I have been asked to provide my view of the meaning of the term “forward,” as that term is used in the ’167 patent. The specification does not define “forward” but provides several examples using the

term “forward.” In some instances, the term “forward” is used in referring to sending the output to another device, e.g., to a secure device or server. *Id.* at 8:45-51,² 10:24-33, 12:48-58, 14:23-30, and 14:57-62. In Claim 5, the ’167 patent claims that the output unit, which forwards the output, “is a display.” Thus, Claim 5 expressly indicates that the display of the output on a display constitutes “forwarding,” at least as that term is used in the ’167 patent. Thus, consistent with the intrinsic evidence, it is my view that the term “forward” should be construed as either sending the output to another device or displaying an output on a display.

B. “Image capture device”

59. Independent claims 1 and 19 recite “an image capture device configured to capture an image...” *Id.* at 16:24, 19:29. I have also been asked to provide my view of the meaning of the term “image capture device,” as it is used in the ’167 patent. Although the specification does not define this term, it indicates that the image capture device or circuit 120 may include a digital camera or other type of image capturing device that is used to capture an image and/or video information. *Id.* at 5:8-11, 5:21-29. The patent also indicates that the image may be a barcode. *Id.* The term “image capture device” should therefore be construed as any device that can capture an image, such as a barcode scanner. Notably, an image capture device is any device capable of capturing and converting optical information into

² As used herein, the notation X:Y-Z refers to column X, lines Y-Z.

digital information or electronic signals. Examples of such devices include laser-based barcode scanners, QR code scanners, document scanners, and camera devices. Laser barcode scanners work by self-emitting a laser light across a code to be scanned, with a sensor tuned to capture the reflected light from the laser, rather than relying on ambient or external light sources in the case of a camera type device. It was well known in 2005 that mobile and smart phone devices could be configured with image capture devices including either digital cameras or laser barcode scanners for the purpose of scanning QR and/or Barcodes. For example, in 2005, the Steven's creek website provided content explaining between using a general-purpose digital camera, or a specialized laser scanner for the application of capturing barcode images. Here, the "Socket SDIO" in this context refers to an example "SDIO In-Hand Scan Card" made by Socket Communications for PalmOS units with an "SDIO" slot. Per Steven's Creek:

[T]he Socket SDIO scanner is a "camera" scanner, not a laser scanner. Whereas the laser scanner above can go "zap zap zap" and scan a series of barcodes in quick succession, the SDIO scanner can take a second or two to successfully scan....So the bottom line is that you really need to evaluate the SDIO scanner to see if it meets your needs. If it does, it's an excellent choice.

Ex. 1010 at 5-6. A POSA would understand from the above that barcode scanners and digital cameras are both categories of image capture device, specifically

within the context of the '167 patent for capturing images with digital information embedded therein. OCR readers are additional a category of image capture devices that perform Optical Character Recognition (OCR). The term refers to a device capable of capturing an image of printed text and converting visible text into digital information that can be stored and processed as text by a computer. OCR readers rely on a digital camera to scan images and OCR software algorithms to extract the textual information from the image. A New York Times article of December 2004 (Keeping Track of Business Cards, Simplified: A Scanner to Digitize Them) describes one such device (“CardScan Executive from Corex Technologies”) as a device that scans business cards capturing both the image as well as extracting the data from the captured image, with this data able to be synchronized to mobile devices and smart phones of the era.

Using proprietary optical-character-recognition software, the CardScan Executive can store a faithful image of the card, extract its data and place it in a searchable databank. The CardScan information can be synchronized with other devices, like Pocket PC and Palm organizers, BlackBerrys.

Ex. 1035 at 1 (<<https://www.nytimes.com/2004/12/09/technology/circuits/keeping-track-of-business-cards-simplified-a-scanner-to.html>>).

C. “Predetermined Information”

60. Independent claims 1 and 19 recite “a memory configured to store **predetermined information.**” *Id.* at 16:27, 17:31. Independent claims 23, 39, and 43 recite “store **predetermined information...**” *Id.* at 17:55, 18:54, 19:6. I have been asked to provide my view of the meaning of the term “predetermined information,” as it is used in the ’167 patent. Although the specification does not define “predetermined information,” it does disclose that predetermined information is stored in memory and may include, for example, address information, personal profile information, and payment account information. *Id.* at 6:17-22. The specification further discloses that the predetermined information may be used to generate an authentication code (e.g., an output). *Id.* at 6:55-66. This usage of the term “predetermined” is consistent with its definition, which is “established or decided in advance.” Ex. 1007. Based on its usage in the specification and definition, the term “predetermined information” should be construed as any information that is established and stored in memory in advance of generating the output.

VII. INVALIDITY ANALYSIS

A. Overview

61. I have reviewed Claims 1, 2, 4, 5, 7, 8, 12, 13, 17, 19-21, 23, 26, 27, 29, 30, 34, 39-41, and 43 of the ’167 patent and the prior art cited in this report, and I

have concluded that these claims are anticipated or obvious over the prior art. A summary of my conclusions is provided in the below table and the detailed bases for my opinion are provided thereafter.

Ground	35 U.S.C.	Claims	Basis
I	§§ 102/103	1, 4, 5, 7, 12, 17, 23, 26, 27, 29, 34, 43	Anticipated by Wang. Obvious over Wang in view of Drummond.
II	§ 102	1, 2, 4, 7, 12, 13, 17	Anticipated by Wang.
III	§ 103	19-21, 39-41	Obvious over Wang in view of Drummond.
IV	§ 103	8, 30	Obvious over Wang in view of Denso.
V	§ 103	13	Obvious over Wang in view of Raines.
VI	§ 103	1, 4, 5, 7, 23, 26, 27, 29, 43	Obvious over TAO in view of PTM and Wang.

A. Ground I: Claims 1, 4, 5, 7, 12, 17, 23, 26, 27, 29, 34, and 43 are anticipated by Wang and obvious over Wang in view of Drummond.

62. I have reviewed Wang (Ex. 1004). I also have compared the features of the Claims 1, 4, 5, 7, 12, 17, 23, 26, 27, 29, 34, and 43 of the ‘167 patent with Wang and reached the conclusion that each of these claims is anticipated by Wang.

Although Wang discloses an “output unit configured to forward the output generated by the processor” (as claimed in claim 1) in the form of a display and forwarding to a printer and hence anticipates these claims, I have additionally provided an obviousness position in Ground 1 based on Wang in view of Drummond in view of the fact that it would have been obvious to the POSA to

modify Wang to forward an output via conventional email or text messaging, as described in Drummond, and as discussed in the below claim chart. As such, I have determined that these claims are obvious over Wang in view of Drummond. My alternative invalidity position based on obviousness over Wang in view of Drummond applies to all claims in Ground 1.

Motivation to Combine Wang and Drummond

To the extent Wang does not disclose an output unit configured to “forward” an output generated by the processor, it would have been obvious to modify Wang to forward receipts via email or a text message, as explained by Drummond.

Drummond discloses that it was known to forward receipts using conventional output units to notify users of the status of a transaction. Ex. 1008 at [0246]-[0251], [0301], [0307]. A POSA would understand, for example, that by forwarding receipts via emails or SMS, the receipts can be sent to their personal devices for record keeping purposes, which could be important to cross-reference transactions against payment account statements such as credit card statements and/or retaining such documents for tax purposes. Additionally, users would be able to forward electronic copies of receipts to the merchant and/or to other interested individuals, for example, to another individual responsible for processing invoices or obtaining reimbursements. Drummond discloses that electronic receipts may be forwarded using message delivery protocols such email

and SMS. Ex. 1008 at [0248]. Use of such message delivery protocols would enable any mobile phone, including those disclosed in Wang, to forward the receipts. Further, Drummond indicates that the use of electronic receipts that are forwarded to another device provides several benefits over hard copy receipts, such as by enabling the customer to: (1) choose to receive the receipt at a computer, such as their home computer (e.g., pc), work computer, mobile phone, pager, PDA, other hand-held or portable computing device, or another device capable of receiving a message; (2) determine the level of information in the receipt; and (3) send additional receipt copies to additional selected systems and system addresses (e.g., a receipt may be sent to an associate or a party to a business transaction as an indication that a deposit or payment on a loan was made). *Id.* at [0246]-[0251], [0301], [0307]. For at least these reasons, a POSA would be motivated to modify Wang to forward its receipt outputs via email or SMS as taught by Drummond and would have had a reasonable expectation of success in doing so.

63. Like challenged Claim 1, Wang describes an apparatus and method for performing secure transactions. Ex. 1004 at [0002]. After authenticating a cell phone user, Wang describes that the cell phone may be used to scan barcodes to lookup prices from a lookup table for items to be purchased. *Id.* at [0072], [0115]. An output, such as an electronically signed receipt, may be generated based on the

information from the lookup table and from predetermined information stored on the cellular phone. *Id.* These outputs may be forwarded to a user and may be digitally signed. *Id.* at [0108], [0112], [0115], [0123]. Wang also describes (i) the use of memory for storing program data, and (ii) the use of predetermined information in the form of private keys that are used to digitally sign the outputs. *Id.* at [0050], [0085], [0115]. Wang anticipates claim 1. For the reasons I explain in the following claim charts, all of the features of the challenged claims are disclosed by Wang. As I show below, Claim 1 is anticipated by Wang and obvious over Wang in view of Drummond.

Independent Claim 1

Claim 1	Wang (Ex. 1004)
[Preamble 1] ³ 1. An apparatus for providing a secure transaction, the apparatus comprising:	Wang discloses an apparatus for providing a secure transaction. “portable electronic authorization devices (PEADs) which eliminate the security risks associated with... approving transactions” [0002]. An “Internet enabled cellular telephone...may be used to implement a...PEAD.” [0108].
[1a] an image capture device configured to capture an image, the image having information embedded therein including	Wang discloses an image capture device (e.g., a barcode or OCR scanner) that captures an image (e.g., a barcode or OCR image) that has information embedded therein (e.g., index data for price lookup) that is usable for generating an electronically signed receipt relating to a purchase transaction . [0115].

³ The various claim elements have been numbered in brackets in the claim charts and are listed for all claims in a Claims Appendix at Appendix A.

Claim 1	Wang (Ex. 1004)
information relating to a transaction;	“Another implementation of the... transaction is to use the PEAD as [a] self checkout terminal.” [0115]. This includes “scanning in the...barcode using the input device built into the PEAD such as a barcode scanner or OCR reader ...generate the receipt with the list of item prices by querying the item price using the barcode as the index for price lookup table...” <i>Id.</i>
[1b] a memory configured to store predetermined information;	Wang discloses storing “the user’s private key” (predetermined information) in “memory portion 304,” [0050] and discloses “the PEAD user can sign the receipt electronically using PEAD as described in U.S. Pat. No. 5,917,913.”⁴ [0115]. Wang discloses that “the PEAD may be employed to ‘sign’ any computer file for authentication purposes” and indicates that authentication is based on encryption “using the user’s private key.”⁵ [0085]. The private key is predetermined information since it is stored in the PEAD memory prior to initiation of any secure transactions.
[1c] an input unit configured to receive input information provided by a user;	“ user authentication mechanism 612 may require the user to enter a password , to furnish fingerprints or a voice print, or other biometrics” [0073]. A password or fingerprint constitutes input information . Thus, a “user authentication mechanism...to enter a password...” is an input unit

⁴ Wang repeatedly refers to U.S. Pat. No. 5,917,913, which is effectively an internal cross-reference to Wang itself since the ’913 patent is related to Wang and includes generally the same disclosure as Wang paragraphs [0002]-[0011] and [0018]-[0085]. *See* Ex. 1012.

⁵ *See* paragraphs 64 - 73.

Claim 1	Wang (Ex. 1004)
	configured to receive input information provided by a user.
[1d] a processor configured to:	“A microcontroller...executes codes stored in flash memory...and employs [RAM]...for the execution.” [0074]. A microcontroller is a processor, and a POSA would appreciate that the Wang microcontroller is configured to perform elements 1e-g. as claimed.⁶
[1e] verify the user based on the input information to ensure that the user is authorized to use the apparatus; and	“require the user to enter a password, to furnish fingerprints or a voice print, or other biometrics and/or identifying characteristics specific to the authorized user before PEAD 200 can be activated....” [0072].
[1f] generate an output based on the information embedded in the image and the predetermined information; and	Wang describes digitally signed “receipts” as outputs, which are based on image information (data from barcodes) and predetermined information (private key). After “agree[ing] to pay for the item, the user can approve the transaction by pressing the button on the phone....” The device then generates a digitally signed receipt as an output: “[T]he PEAD can generate the receipt....” [0115]. The digitally signed receipt is based on information embedded in an image (barcode information): “[T]he PEAD can generate the receipt...by querying the item price using the barcode as the index for price lookup table....”⁷ <i>Id.</i> The digitally signed receipt is also based on the predetermined information (private key): “[T]he

⁶ See paragraphs 74 - 77.

⁷ See paragraph 78.

Claim 1	Wang (Ex. 1004)
	PEAD user can sign the receipt electronically using PEAD....” [0115]. “[T]he PEAD may be employed to ‘sign’ any computer file for authentication purposes” and indicates that authentication is based on encryption “using the user’s private key.” [0085]. Thus, the private key (predetermined information) is utilized to digitally sign the receipt.⁸
[1g] an output unit configured to forward the output generated by the processor,	<u>Anticipation</u> Wang discloses two types of output devices, a display and a “local wireless communication port,” both of which “forward” the output (digitally signed receipt), as properly construed in Section VI.A. (Section VI.B.1. of the Petition). 1. “presenting the electronic receipt over the phone” [0115]. 2. “establishing the connection between the cellular phone and the receipt printer.” <i>Id.</i> <u>Obviousness</u> Additionally, it would have been obvious to modify Wang to send or “forward” the digitally signed receipt, e.g., to the user, in an email or text for the purpose of memorializing the transaction, as shown by Drummond, Ex. 1008, at [0246]-[0251], [0301], [0307].⁹
[1h] wherein the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	“The PEAD user can sign the receipt electronically using PEAD.” [0115]. The output (digitally signed receipt) is electronically signed. An electronic signature as disclosed in Wang is a digital signature.¹⁰ Ex. 1004 at [0108], [0112], [0123].

⁸ See paragraphs 79 - 81.

⁹ See paragraphs 62, 82 - 84.

¹⁰ See paragraphs 85 - 88.

Element 1b: Private Keys

64. As indicated above with respect to element 1b, Wang discloses the use of **private keys**. A person skilled in the art would understand that a public/private key pair is a fundamental component of asymmetric cryptography, a system where two keys are used: a public key, which can be freely distributed, and a private key, which is kept secret. The public key is used to encrypt data, while the private key is used to decrypt it. This ensures that even if the encrypted data is intercepted, it cannot be read without the private key.

65. In the Wang patent, the user's private key is stored in "memory portion 304." Ex. 1004 at [0050]. This private key enables generating digital signatures. The digital signature provides an additional factor of authentication for transactions performed by a user of a device. When a transaction is initiated, the mobile device uses its private key to sign the transaction data. This signature can be verified by the recipient using the corresponding public key, helping to ensuring the authenticity and integrity of the transaction. This method is consistent with the established principles of public/private key cryptography.

66. Wang discloses that authentication is based on encryption "using the user's private key." *Id.* at [0085]. This aligns with the use of asymmetric encryption, where the private key encrypts a hash of the transaction data to create a digital signature, and the public key decrypts it for verification. This process ensures that

only the holder of the private key (the user) could have generated the signature, thereby authenticating the transaction. By including transaction data, such as amount, time, or other odder details in the hash, the signature certifies what specifics of the transaction the user authorized.

67. Digital signatures use asymmetric cryptography to verify the authenticity and integrity of a message or document. A digital signature is created by generating a hash of the message and then encrypting it with the sender's private key. The recipient can decrypt this signature using the sender's public key and compare it to a hash of the received message. If the hashes match, the signature is verified, ensuring that the message has not been altered and confirming the sender's identity.

68. Wang describes that "the PEAD user can sign the receipt electronically using PEAD as described in U.S. Pat. No. 5,917,913" and that "the PEAD may be employed to 'sign' any computer file for authentication purposes." *Id.* at [0115], [0085]. This process involves the user's private key stored on the device, which is used to generate the digital signature.

69. At the time of Wang, various well-known standards existed for the employ of encryption and digital signatures for the facilitation of secure electronic transactions. In 2003, Visa described two such standards:

There are currently two protocols for Authenticated Payment:

3-D Secure™ – Leverages Transport Layer Security (TLS) technology, which is incorporated in most browsers currently in use. Provides confidentiality of information, ensures payment integrity, and authenticates cardholders. Note: TLS is the successor to Secure Sockets Layer (SSL).

SET Secure Electronic Transaction™ – Uses cryptography to provide confidentiality of information, ensure payment integrity, and authenticate both merchants and cardholders.

Ex. 1014 at 11 (accessible at <https://web.archive.org/web/20060314195418/http://partnernetnetwork.visa.com/pf/3dsec/download/trk_3dsec_system_overview_v102.pdf>).

70. Visa also states that 3-D secure “[i]s extensible into emerging channels such as mobile telephones, PDAs, and digital TV”. *Id.* at 12. A POSA would understand that devices described by Wang, TAO, and PTM would all fall under this definition. The 3-D in this framework stands for “Three Domains.” The “Three Domain Model enables issuers to authenticate their cardholders during online purchases. Acquirers and merchants have a flexible framework that can embrace a variety of technical approaches.” *Id.* at 22. In this protocol, the issuer has flexibility to implement a system to directly communicate with and authenticate their cardholders in the course of an electronic transaction initiated by the merchant. The issuer implements a system known as an Access Control Server

(ACS): “The ACS authenticates the cardholder by causing an authentication dialog to be displayed to the cardholder asking for password, or by some other authentication method, such as a Visa chip card. The ACS formats and digitally signs the authentication response, then returns it.” *Id.* at 28.

71. The Wang patent describes a method for approving transaction requests using a portable electronic authorization device (PEAD). This method involves receiving transaction data, decrypting the user’s private key with a decryption key from a remote server, and then using the private key to sign the transaction data. The critical aspect here is that a secret private key has been previously configured by a verifying party onto the PEAD device by a certifying authority (e.g. a card network or the user’s financial institution). The certifiable presence of that secret key provides an additional second physical factor of authentication. Transaction authentication is made more secure by the fact that an attacker would need to compromise both the user’s password, as well as the physical device in order to falsely authenticate a transaction. In this example, the PEAD device would perform the analogous function to a “Visa chip card” as described in the Visa 3-D secure protocol.

72. A POSA would recognize the value of utilizing a device as described by Wang to “sign any computer file for authentication purposes.” Ex. 1004 at [0085]. Wang’s method of decrypting and using the user’s private key to generate a digital

signature could be applied to the cardholder verification process in the 3D Secure protocol. By using the PEAD to sign transaction data, the card issuer's system could provide strong authentication of the cardholder's identity. The use of encryption and digital signatures would ensure that the transaction data is uniquely tied to the cardholder, providing a mechanism for verifying both the authenticity of the transaction and the identity of the user.

73. A POSA would be motivated to use the Wang device for cardholder verification due to the increased security it offers. The ability to securely sign transaction data using a private key that is only decrypted on-demand mitigates the risk of key compromise and aligns with the goals of the 3D Secure protocol to reduce fraud and enhance transaction security.

Element 1d: Microcontrollers

74. Concerning the microcontrollers discussed by Wang, it is well known that a microcontroller is a term to describe a processor as well as certain supporting hardware when packaged together for embedding in a small or low-power device. *See, e.g.,* Predko, M., *Programming and Customizing the 8051 Microcontroller* (1999), Ex. 1015, at 3 (“microcontroller (as I define it) is a chip which has computer processor with all its support functions (clocking and reset), memory (both program storage and RAM) and I/O (including bus interfaces) built into the device”).

75. In view of this understanding of the term, a POSA would understand that when Wang is describing a microcontroller, that this device would principally contain a computer processor. Further, that microcontroller would need to be configured to run any general purpose software applications or to perform input/output (I/O).

76. The configuration of the microprocessor would include hardware and software level configurations. Necessary hardware configuration would include selecting sufficient memory for storage, and hardware bus interfaces for input and output (e.g. for the microcontroller to be able to interact with camera device, networking chips, display screen etc. also included onboard PEAD). Software configuration would include preconfigured operating system software (e.g., in the way that Palm devices of the era were configured with PalmOS software, whereas other smartphone devices of the era might have been configured with RIM BlackberryOS or Nokia SymbianOS etc.). These operating systems would be configured in the microprocessor's memory prior to shipping the device to the user.

77. Finally, the microprocessor would rely on specific application software (as described in Wang) which would also be stored in the microprocessor's configured hardware memory. And applications would in turn be understood to store in memory preconfigured information (as described in Wang) such as a

user's private cryptographic key. A private cryptographic key would typically be configured by a relevant authority, for example, the user's financial institution as means of confirming the indented user's identity in authorizing future transactions or system access requests etc.

Element 1f: The receipt is linked to the barcode.

78. Wang explicitly describes two scenarios where the barcode data is directly linked to (and required for) initiating a transaction that results in a receipt output:

A) It is common knowledge that common transaction receipts may include itemized purchase information. Wang describes how item-specific transaction data being retrieved via a barcode "scan in the merchandise barcodes and generate transaction information as well as generate a unique transaction number (which contains the store number+counter number+transaction number for example)...It is also possible to enter the merchandise bar code number to the PEAD through the keypad or scanner..." Ex. 1004 at [0113]. Wang then describes that "the PEAD can generate the receipt...using the barcode" *Id.* at [0115].

B) Wang describes how the scanner can be used to create a trusted synchronous connection between a mobile device and point of sale system. A person skilled in the art of payments would obviously understand that explicitly identifying the buyer and the seller is necessary step initiating a transaction. Wang describes a common method used by payment schemes of the day to assign a

globally unique alias to one party of the transaction (e.g. a user's phone number, or a merchant Point of sale terminal ID) that can then be read or scanned via a bar code, to connect the two parties to begin exchanging transaction information.

When a receipt is created at the end of the transaction, the creation of that receipt depends on successful initiation and authorization of a transaction between the explicitly identified parties, a process that was initiated by data linked to the barcode. *Id.*

Element 1f: How the Private Key is used for authentication.

79. Using a predetermined private key to sign transaction data provides a method for ensuring the authenticity and integrity of transaction data. When a private key, known only to the authorized user, is used to create a digital signature, it binds the transaction data to the user, making it verifiable by anyone with access to the corresponding public key. This process guarantees that the transaction data has not been tampered with and confirms the identity of the signer. According to Schneier (1996), digital signatures created with private keys provide non-repudiation, meaning that the signer cannot later deny having signed the data, which is valuable for secure financial transactions and legal accountability. Ex. 1017 at 62-72.

80. According to Schneier: "In practical implementations, public-key algorithms are often too inefficient to sign long documents. To save time, digital

signature protocols are often implemented with one-way hash functions. Instead of signing a document, Alice signs the hash of the document. In this protocol, both the one-way hash function and the digital signature algorithm are agreed upon beforehand.” *Id.* at 68 (internal citations omitted). Additionally, “[t]here are many digital signature algorithms. All of them are public-key algorithms with secret information to sign documents and public information to verify signatures. Sometimes the signing process is called encrypting with a private key....” *Id.*

81. Schneier further explains that “[b]y combining digital signatures with public-key cryptography, we develop a protocol that combines the security of encryption with the authenticity of digital signatures. Think of a letter from your mother; The signature provides proof of authorship and the envelope provides privacy.” *Id.* at 71.

Element 1g: Obviousness over Drummund

82. Although I have formally construed the term “forward” above, additional background concerning this term is warranted in view of my obviousness analysis. In 2005, “forwarding” in the context of secure transactions could be taken to mean the process by which a device or system sends data from one point to another. This process includes transmitting generated output, such as digital signatures or authentication codes, from the device where the output was created to another device or system where it can be used or verified. In the context of payment

processing, there are commonly a chain of entities (e.g. a payment device (such as a payment card, smart card, or electronic wallet) merchant point of sale system, payment processor, a merchant acquiring bank, a payment network, a card issuing bank and a payor). Each of these parties would be responsible for sequentially responsible for receiving and forwarding payment authorization requests and authorization responses. A purchase transaction is generally only considered complete once an acknowledgment of the payment authorization is forwarded to the purchasee.

83. In the context of electronic communications of 2005. Forwarding was also commonly used in the context of email forwarding. For example, it was common for ecommerce merchants to forward purchase receipts, purchase orders or receipts by email to buyers.

84. In the context of mobile devices of 2005, two widely compatible methods of pushing a notification to a user of smart mobile device would be by SMS to a standard cell phone, or by email message to a smart phone capable of email.

Examples:

- Email Forwarding: In 2005, a common method of forwarding would be through email. For instance, after capturing an image and generating a digital signature, the mobile device would send this information via email to a recipient, e.g., for order fulfillment or for record keeping.

- SMS Forwarding: Another prevalent method was through SMS (Short Message Service). The device could forward the generated output, such as an authentication code, via SMS to a verifier or a user's phone number for completing a secure transaction.
- Display Forwarding: The output unit might also be a display on the mobile device itself, showing the generated digital signature or authentication code that the user would then manually input into another system or provide to a verifier.
- API Call Forwarding: Mobile applications could forward transaction data by making API calls to remote servers. For example, after capturing a QR code and generating a digital signature, the mobile application would use an HTTP POST request to send this data to a server endpoint for validation. In 2005, it was commonly understood that application software installed on certain mobile phones and devices could make network calls over data connections to nearby devices or remote computers. Wang describes forwarding user-inputted passcodes to a remote server for validation as an additional level of security to access private keys required to sign a transaction. Ex. 1004 at [0121]. For the reasons explained above, it would have been obvious to modify Wang to forward receipts via email or SMS, as described by Drummond.

Element 1h: The electronic signature in Wang is a digital signature

85. It was well known at the time that the term “digital signature” includes cryptographic mechanisms used to verify the authenticity and integrity of a message, transaction, or digital document. Digital signatures ensured that the message was created by a known sender (authentication) and that it had not been altered (integrity). Digital signatures were known to be created through the use of private and public cryptographic keys. In the context of secure payment transactions, standards were well established by 2005 for creating digital signatures using pre-determined public and private keys stored on a trusted device such as a smart card or merchant terminal.

86. In 2005, a POSA would be familiar, for example, with this contemporaneous description of digital signatures and electronic at the time:

Digital signature (or public-key digital signature) is a type of method for authenticating digital information analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public-key cryptography. A digital signature method generally defines two complementary algorithms, one for signing and the other for verification, and the output of the signing process is also called a digital signature.

The term electronic signature, although sometimes used for the same thing, has a distinct meaning in common law: it refers to any of several, not necessarily cryptographic, mechanisms for identifying

the originator of an electronic message. Electronic signatures have included cable and Telex addresses, as well as FAX transmission of handwritten signatures on a paper document.

Ex. 1018 at 1.

87. Notably, the '167 patent does not define the term “digital signature,” but it does state in its claims that the digital signature is “used to signify authorization by the user with respect to the transaction.” Ex. 1001 at 16:22.

88. Wang indicates that “[t]he PEAD user can sign the receipt electronically using PEAD as described in U.S. Pat. No. 5,917,913.” Ex. 1004 at [0115]. The reference to the '913 patent is effectively a cross-reference to an earlier portion of Wang as previously mentioned. This earlier portion of Wang states that “a transaction embodied in the transaction request from the electronic transaction system may be appended with data representative [of] an ‘electronic signature’ prior to being encrypted and retransmitted back to the electronic transaction system.” Ex. 1004 at [0051]. This description is consistent with the Wang electronic signature being “used to signify authorization by the user with respect to the transaction” as claimed in the '167 patent. Additionally, this description is consistent with the well-understood meaning of the term “digital signature.” Thus, it is my view that the claim term “digital signature” in the '167 patent reads on the electronic signature in Wang.

89. As I show below, Claim 4 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 4

Claim 4	Wang (Ex. 1004)
4. The apparatus of claim 1 wherein the input information includes one of a personal identification number and biometric information.	“require the user to enter a password, to furnish fingerprints or a voice print, or other biometrics... ” [0072], [0045].

90. As I show below, Claim 5 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 5

Claim 5	Wang (Ex. 1004)
5. The apparatus of claim 1 wherein the output unit is a display.	“presenting the electronic receipt over the phone” [0115]. Presenting the electronic receipt over the phone equates to displaying the receipt (i.e., the output).

91. As I show below, Claim 7 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 7

Claim 7	Wang (Ex. 1004)
7. The apparatus of claim 1 wherein the image includes a barcode.	“scanning in the... barcode. ” [0115].

92. As I show below, Claim 12 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 12

Claim 12	Wang (Ex. 1004)
12. The apparatus of claim 1 wherein the transaction includes an online transaction.	“employ the PEAD to perform any type of authentication tasks online. ” [0084]. The transaction is described as being performed “through the wireless network and Internet...” i.e., online. [0115].

93. As I show below, Claim 17 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 17

Claim 17	Wang (Ex. 1004)
17. The apparatus of claim 1, wherein the apparatus is a cellphone.	“Internet enabled cellular telephone ...may be used to implement a...PEAD.” [0108].

94. As I show below, Claim 23 is anticipated by Wang and rendered obvious over Wang in view of Drummond.

Independent Claim 23

Claim 23	Wang (Ex. 1004)
[Preamble 23] 23. A method of providing secure transaction, the method comprising:	Wang discloses a method for providing a secure transaction. <i>See Preamble 1 analysis.</i>

Claim 23	Wang (Ex. 1004)
[23d] configuring a portable device to:	Wang discloses a PEAD (a portable device) having a microcontroller and memory configured to perform the steps described in Wang and outlined in this claim chart. [0074], [0115]. For the PEAD to perform the functions described in Wang, it must have been configured to do so.¹¹ <i>See also Element 1d analysis.</i>
[23a] capture an image, the image having information embedded therein, the information embedded in the image including information relating to a transaction;	Wang discloses an image capture device (e.g., a barcode or OCR scanner) that captures an image (e.g., a barcode or OCR image) that has information embedded therein (e.g., index data for price lookup) that is usable for generating an electronically signed receipt relating to a purchase transaction. [0115]. “Another implementation of the...transaction is to use the PEAD as [a] self checkout terminal.” [0115]. This includes “scanning in the...barcode using the input device built into the PEAD such as a barcode scanner or OCR reader...generate the receipt with the list of item prices by querying the item price using the barcode as the index for price lookup table” <i>Id.</i>

¹¹ See paragraphs 74 - 77.

Claim 23	Wang (Ex. 1004)
[23b] store predetermined information;	Wang discloses storing “the user’s private key” (predetermined information) in “memory portion 304,” [0050] and discloses “the PEAD user can sign the receipt electronically using PEAD as described in U.S. Pat. No. 5,917,913.”¹² [0115]. Wang discloses that “the PEAD may be employed to ‘sign’ any computer file for authentication purposes” and indicates that authentication is based on encryption “using the user’s private key.” [0085] The private key is predetermined information since it is stored in the PEAD memory prior to initiation of any secure transactions.¹³
[23c] receive input information provided by a user;	“user authentication mechanism 612 may require the user to enter a password, to furnish fingerprints or a voice print, or other biometrics.” [0072]. A password or fingerprint constitutes input information. Thus, a “user authentication mechanism...to enter a password...” is an input unit configured to receive input information provided by a user.
[23e] verify the user based on the input information to ensure that the user is authorized to use the portable device;	“require the user to enter a password, to furnish fingerprints or a voice print, or other biometrics and/or identifying characteristics specific to the authorized user before PEAD 200 can be activated....” [0072].

¹² Wang repeatedly refers to U.S. Pat. No. 5,917,913, which is effectively an internal cross-reference to Wang itself since the ’913 patent is related to Wang and includes generally the same disclosure was Wang paragraphs 1-85. *See* Ex. 1012.

¹³ *See* paragraphs 64 - 73.

Claim 23	Wang (Ex. 1004)
[23f] generate an output based on the information embedded in the image and the predetermined information; and	Wang describes digitally signed “receipts” as outputs, which are based on image information (data from barcodes) and predetermined information (private key). After “agree[ing] to pay for the item, the user can approve the transaction by pressing the button on the phone....” The device then generates a digitally signed receipt as an output: “[T]he PEAD can generate the receipt...” [0115]. The digitally signed receipt is based on information embedded in an image (barcode information): “[T]he PEAD can generate the receipt...by querying the item price using the barcode as the index for price lookup table....”¹⁴ <i>Id.</i> The digitally signed receipt is also based on the predetermined information (private key): “[T]he PEAD user can sign the receipt electronically using PEAD....” <i>Id.</i> “[T]he PEAD may be employed to ‘sign’ any computer file for authentication purposes” and indicates that authentication is based on encryption “using the user’s private key.” [0085]. Thus, the private key (predetermined information) is utilized to digitally sign the receipt.¹⁵

¹⁴ See paragraph 78.

¹⁵ See paragraphs 79 - 81.

Claim 23	Wang (Ex. 1004)
[23g] forward the generated output to the user,	<u>Anticipation</u> <i>See</i> Element 1g analysis. Notably, displaying the receipt by the user would necessarily require forwarding (e.g., displaying) the receipt to the user . Similarly, the act of sending the receipt to the printer, the printout of which would be accessed <i>by the user</i> , constitutes forwarding the receipt to the user . ¹⁶ <u>Obviousness</u> <i>See</i> Element 1g analysis.
[23h] wherein the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	“The PEAD user can sign the receipt electronically using PEAD.” [0115]. The output (digitally signed receipt) is electronically signed. An electronic signature as disclosed in Wang is a digital signature. ¹⁷ [0108], [0112], [0123].

Element 23g: Forwarding “to the user”

95. Although I formally construed the term “forward” above, additional discussion is warranted concerning how displaying the receipt on the display screen and forwarding the receipt to the printer is the same as forwarding “to the user.” “Forwarding” is not a specific term of art in the relevant fields of mobile devices, computer science or transaction processing. It is a common term to which multiple definitions can apply. Looking textually at the ‘167 patent, the term is

¹⁶ *See* paragraphs 95 - 96.

¹⁷ *See* paragraphs 85 - 88.

used in the context of “an output unit configured to forward the output generated by the processor.” Ex. 1001 at 16:34.

96. Taking the ’167 contextual use of the word “forward,” the term is suggested to apply to the function performed by any output unit connected to a computer processor. Again, from the specific definition suggested by ’167, any of the configured output options specified by Wang including a screen for display, or a printer for printing a receipt would fit the definition of forwarding output. Further, the device user would be a recipient of information displayed on the user’s device screen—specifically because it is displayed on the user’s device. The commonly understood intended recipient of purchase receipts is also the purchaser who authorized the transaction. Additionally, the ’167 patent indicates that the user prints the receipt, and so the act of forwarding the receipt to the printer is the same as forwarding the output to the user, in the sense as the term as used in the ’167 patent. *See* Ex. 1004 at [0115] (“The user can then walk out the store by presenting the electronic receipt over the phone or goes to the receipt printer to print out the hardcopy.”). Thus, the displaying of the receipt on the user’s screen and the printing the receipt are the same as forwarding the receipt “to the user.”

97. As I show below, Claim 26 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 26

Claim 26	Wang (Ex. 1004)
26. The method of claim 23 wherein the input information includes one of a personal identification number and biometric information.	See Claim 4 analysis.

98. As I show below, Claim 27 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 27

Claim 27	Wang (Ex. 1004)
27. The method of claim 23 further comprising: configuring the portable device to display the output.	See Claim 5 analysis. To display the receipt image as taught by Wang, the PEAD must be configured to do so. ¹⁸

The Wang PEAD is configured to display an output

99. A POSA would understand that Wang is indicating that the PEAD of Wang must be configured to display the receipt in order to do so. That configuration would consist of: at the hardware level, specifying and assembling the device to contain a screen output device connected to the processor; at the software application level, to provide instructions to the processor to visually format and display the receipt output on the screen.

¹⁸ See paragraph 99.

100. As I show below, Claim 29 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 29

Claim 29	Wang (Ex. 1004)
29. The method of claim 23 wherein the image includes a barcode.	<i>See Claim 7 analysis.</i>

101. As I show below, Claim 34 is anticipated by Wang and obvious over Wang in view of Drummond.

Dependent Claim 34

Claim 34	Wang (Ex. 1004)
34. The method of claim 23 wherein the transaction includes an online transaction.	<i>See Claim 12 analysis.</i>

102. As I show below, Claim 43 is anticipated by Wang and obvious over Wang in view of Drummond.

Independent Claim 43

Claim 43	Wang (Ex. 1004)
Preamble 43	<i>See Preamble 23 analysis.</i>
Elements 43a-g	<i>See Elements 23a-g analysis.</i>
Element 43h	“Internet enabled cellular telephone ...may be used to implement a...PEAD.” [0108].

B. GROUND II: Wang anticipates Claims 1, 2, 4, 7, 12, and 17.

103. From my review of Wang, it was apparent that Wang describes multiple types of predetermined information and outputs. In addition to the “private key” predetermined information discussed in Ground 1, Wang discloses the use of predetermined information in the form of “user identification data,” which may include, for example, “the user’s name, his birth date, [or] his social security number,....” Ex. 1004 at [0045]. Likewise, in addition to an output in the form of a digitally signed receipt, as discussed in Ground 1, Wang discloses generating “transaction approval data” as an output. *Id.* at [0075]-[0083], [0115]. As shown in FIG. 3B, reproduced below, the transaction approval data 350 contains:

transaction data 352, representing a portion of or the entire transaction request received...appended with certain user identification data 354.... Once appended, the transaction approval data 350 is then encrypted prior to being retransmitted back to the electronic transaction system.

Id. at [0051].

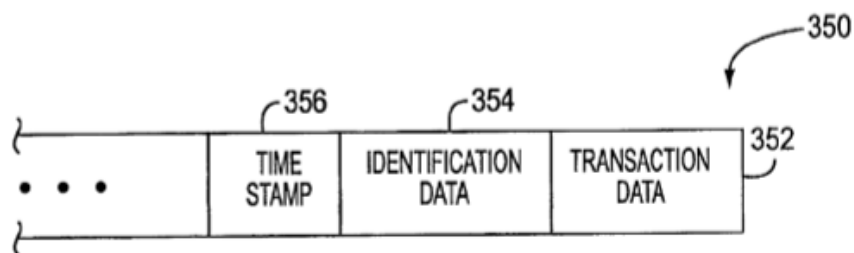


FIG. 3B

Wang’s use of “user identification data” as predetermined information and “transaction approval data” as an output forms the basis of Ground 2.

104. Wang describes a PEAD apparatus (optionally a cellular phone) and method for performing secure transactions. *Id.* at [0002]. After authenticating a user of the cellular phone, Wang describes that a barcode scanner of the PEAD may be used to scan barcodes to select and lookup prices for items for a purchase transaction from a lookup table. *Id.* at [0072], [0115]. Outputs, such as transaction approval data, may be generated based on scanned barcode information (information embedded in an image) and on the user identification data (predetermined information) stored on the PEAD. *Id.* at [0075]-[0083], [0115]. These outputs may be forwarded to a server of a transaction approval network and may be digitally signed. *Id.* at [0047]-[0051], [0108], [0112], [0115], [0123]. Wang discloses all features of Claims 1, 2, 4, 7, 12, and 17 for the reasons discussed below.

105. As I show below, Claim 1 is anticipated by Wang.

Independent Claim 1

Claim 1	Wang (Ex. 1004)
[Preamble 1] 1. An apparatus for providing a secure transaction, the apparatus comprising:	<i>See</i> Ground 1, Preamble 1 analysis.
[1a] an image capture device configured to	<i>See</i> Ground 1, Element 1a analysis.

Claim 1	Wang (Ex. 1004)
capture an image, the image having information embedded therein including information relating to a transaction;	
[1b] a memory configured to store predetermined information;	“[U]ser identification data...are always kept secure within the PEAD 200.” [0044]. “the [transaction program]...receives user’s data from the user (e.g., the user’s identification data, any data which may be required for the proposed transaction such as the address information, quantity information, size information, method of payment, credit card number, account number, and the like)” [0093]. “[I]f the user has already supplied the vendor with some of the requested data in the past (such as the user’s address), the TP may not ask for the same data again” indicating that it is stored in memory. [0094]. “Program/data memory” [0062]. “[A]ny of the required...user-supplied data may be stored in the PEAD” [0098]. The user’s data is predetermined information stored in memory.¹⁹
Element 1c-e	See Ground 1, Elements 1c-e analysis.
[1f] generate an output based on the information embedded in the image and the predetermined information; and	Wang describes that the PEAD can generate “transaction approval data” (an output) in response to the user agreeing to a transaction. [0075]-[0083], [0115]. <u>The output is based on information embedded in the image:</u>

¹⁹ See paragraph 106.

Claim 1	Wang (Ex. 1004)
	To approve and complete a transaction, the price of the item being purchased is required. [0115]. The price of the item is generated based on barcode data (information embedded in an image): “The cellular phone would display the price of the item the user entered (or scanned in). If the user agrees to pay for the item, the user can approve the transaction by pressing the button on the phone.” Id. Such approval, which is based on the embedded barcode image information, results in the generation of “transaction approval data.” [0076], [0115] (stating that “the approval process...is described in [related] U.S. Pat. 5,917,913,”²⁰ which describes the generation of “transaction approval data” in response to approval of a transaction). Thus, the transaction approval data (output) is based on price information embedded in a barcode image.²¹ <u>The output is based on predetermined information:</u> The transaction approval data is also based on predetermined information—specifically “user identification data.” Wang indicates that transaction approval data includes “transaction data,” and “user identification data.” [0051], FIG. 3B. The user identification data may include “the user’s name, his birth date, [or] his social security number...” [0045]. Thus, the transaction approval data (output) is based on user identification data (predetermined information).
[1g] an output unit configured to forward the output generated by the processor, wherein	“data path 212 is provided for transmitting [i.e., forwarding] transaction approval data” [0047]-[0048]. The data path is an output unit used to transmit

²⁰ See *supra* note 4.

²¹ See paragraph 78.

Claim 1	Wang (Ex. 1004)
	(forward) the transaction approval data. .
[1h] the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	“the transaction approval data...may be appended with data representative if [sic: of] an ‘electronic signature’” [0051]. “The PEAD user can sign the receipt electronically using PEAD.” [0115]. When the output is transaction approval data, the output may be electronically signed. A POSA would understand that an electronic signature is a digital signature in view of Wang’s disclosure.²² [0108], [0112], [0123].

Element 1b: User data must be stored in the PEAD’s memory

106. Wang’s PEAD is a computing device, and a POSA would interpret Wang as saying that, when the predetermined information is stored in the PEAD, that would mean it is stored in the device’s computer memory. In mobile device architectures of the time, that storage medium would consist of re-writable non-volatile storage such as internal flash memory modules, removable memory cards such as SD or CF card memory standards, or electrically programmable memory (EPROM). It was well known in the art that computing devices used these types of memory for long term storage of data. Ex. 1004 at [0062] (“Program/data memory 504 is preferably implemented using some form of non-volatile memory (NVM) such as flash memory, electrically programmable read-only memory

²² See paragraphs 85 - 88.

(EPROM), electrically erasable, programmable read-only memory (EEPROM), or the like. Temporary memory 506 serves as a scratch pad for calculation purposes and for the temporary storage of data, and may be implemented using some form of random access memory (RAM) such as static RAM or dynamic RAM, which are known in the art.”).

107. As I show below, Claim 2 is anticipated by Wang.

Dependent Claim 2

Claim 2	Wang (Ex. 1004)
2. The apparatus of claim 1 wherein the processor is further configured to generate the output using the input information.	Wang discloses that the transaction approval data (output) includes “user identification data.” [0051]. The user identification data may include a password, “unique biometrics or unique identifying data such as fingerprint....” (input information). [0045].

108. As I show below, Claim 4 is anticipated by Wang.

Dependent Claim 4

Claim 4	Wang (Ex. 1004)
4. The apparatus of claim 1 wherein the input information includes one of a personal identification number and biometric information.	<i>See</i> Ground 1, Claim 4 analysis.

109. As I show below, Claim 7 is anticipated by Wang.

Dependent Claim 7

Claim 7	Wang (Ex. 1004)
7. The apparatus of claim 1 wherein the image includes a barcode.	See Ground 1, Claim 7 analysis.

110. As I show below, Claim 12 is anticipated by Wang.

Dependent Claim 12

Claim 12	Wang (Ex. 1004)
12. The apparatus of claim 1 wherein the transaction includes an online transaction.	See Ground 1, Claim 12 analysis.

111. As I show below, Claim 17 is anticipated by Wang.

Dependent Claim 17

Claim 17	Wang
17. The apparatus of claim 1, wherein the apparatus is a cellphone.	See Ground 1, Claim 17 analysis.

C. GROUND III: Claims 19-21 and 39-41 are obvious over Wang in view of Drummond.

112. Claims 19-21 and 39-41 are obvious over Wang (Ex. 1004) in view of Drummond (Ex. 1008), as shown below.

113. As discussed above in Ground 1, Wang describes an apparatus and method for performing secure transactions. After authenticating a user of the cellular phone, Wang describes that a barcode scanner of a cellular phone may be used to

scan barcodes to select and lookup prices for items for a purchase transaction from a lookup table. *Id.* at [0072], [0115]. Outputs, such as digitally signed receipts, may be generated based on user identification data and a private key (both predetermined information) stored on the cellular phone prior to scanning the barcodes. *Id.* at [0064], [0072], [0115]. The receipts may be forwarded to a user. *Id.* at [0115]. Although implied, Wang does not expressly disclose that the output unit includes control logic configured to forward the output using a message delivery protocol. It would have been obvious, however, to modify Wang to include an output unit that includes control logic configured to forward the receipts using well-known email and SMS message delivery protocol as taught, for example, by Drummond, thereby rendering the challenged claims obvious. Ex. 1008 at [0246]-[0251], [0301], [0307].

Motivation to Combine Wang and Drummond

114. A POSA would understand certain advantages and be motivated to use established message delivery protocols (e.g. email or SMS) to deliver transaction information such as receipts. Doing so, for example, would eliminate the need or labor required for creating novel or specialized software on the transmitting or receiving device. Using well-established protocols and associated control logic would ensure broader compatibility with devices in the field in 2005, ease of use

for users as well as flexibility (e.g. the ability to re-forward receipts to additional recipients, like for group purchases, or for financial accounting or tax purposes).

115. Drummond discloses that it was known to use message delivery protocols (such as SMS and email) to forward receipts using known output units to notify users of a status of a transaction. Ex. 1008 at [0246]-[0251], [0301], [0307].

Forwarding the receipt using a message delivery protocol (such as SMS or email) would enable any number of devices, including computers, cellular phones, and the like, to receive such outputs using standard delivery protocols without modification, as the email and SMS message delivery protocols were common data formats that were already supported by a large array of devices, including cellular phones, such as those disclosed in Wang. Thus, email and SMS communications constitute a finite number of identified, predictable solutions for cellular communications under *KSR*. A POSA would further be motivated to use message delivery protocols such as email and SMS to forward the receipts of Wang to eliminate the need to install any specialized software on either the transmitting or receiving device. Additionally, by modifying Wang to forward the receipt using a message delivery protocol as taught by Drummond, the end user may send a record of the transaction (e.g., the receipt) to any number of conventional devices for storage and later reference. This could be helpful, for example, for tax purposes or to save receipts on a business trip for later

reimbursement. Forwarding receipts via SMS may be particularly desirable if the system employs a firewall, as described by Drummond. Ex. 1008 at [0301].

116. Further, Drummond indicates that the use of electronic receipts that are forwarded using a message delivery protocol provides several benefits over hard copy receipts, such as by enabling the customer to: (1) choose to receive the receipt at a computer, such as their home computer (e.g., pc), work computer, mobile phone, pager, PDA, other hand-held or portable computing device, or another device capable of receiving a message; (2) determine the level of information in the receipt; and (3) send additional receipt copies to additional selected systems and system addresses (e.g., a receipt may be sent to an associate or a party to a business transaction as an indication that a deposit or payment on a loan was made). *Id.* at [0246]-[0251], [0301], [0307]. For at least these reasons, a POSA would be motivated to modify Wang to forward its receipt outputs using a message delivery protocol as taught by Drummond.

117. As I show below, Claim 19 is obvious over Wang in view of Drummond.

Independent Claim 19

Claim 19	Wang (Ex. 1004) and Drummond (Ex. 1008)
[Preamble 19] 19. An apparatus for providing a secure transaction, the apparatus comprising:	<i>See</i> Ground 1, Preamble 1 analysis.
[19a-f]	<i>See</i> Ground 1, Elements 1a-f analysis.

Claim 19	Wang (Ex. 1004) and Drummond (Ex. 1008)
[19g] an output unit configured to forward the output generated by the processor, wherein	Drummond discloses output units configured to forward the output (receipts) generated by the processor via email or SMS. Ex. 1008 at [0247] (e.g., “host computer”), [0301], FIG. 65 (e.g., device 912).
[19h] the output unit includes control logic configured to forward the output using a message delivery protocol .	“presenting the electronic receipt over the phone” Ex. 1004 at [0115]. “establishing the connection between the cellular phone and the receipt printer” <i>Id.</i> “The receipt may be...in the form of an e-mail message sent to one or more e-mail addresses...[and] may also be a text message sent to a phone number of a mobile phone, pager, PDA, or other portable computing device.” Ex. 1008 at [0247], [0301]. A POSA would understand that an output unit for sending email or text would require “control logic.”²³ A POSA would understand that sending e-mail and text messages requires using message delivery protocol.²⁴

Element 19h: A POSA would understand that an output unit for sending email or text requires “Control Logic”

118. A POSA familiar with computer architecture design in 2005 would be familiar with how computing devices operate using control logic. In the context of computing devices, control logic is a familiar term for the functionality responsible for managing the execution of instructions and the overall operation of

²³ See paragraphs 118 - 123.

²⁴ See paragraphs 124 - 126.

the processor. Control logic interprets commands from the software and translates them into actions performed by the hardware components of the device.

119. Under one commonly understood definition, control logic can take the form of Microcode: a layer of hardware-level instructions or data structures involved in the application of higher-level machine code instructions in many computers. In the context of computing devices, control logic is a familiar term for the functionality responsible for managing individual execution units within a processor. For example, control logic governs the functionality of processor ALU (Arithmetic Logic Unit) or of a branch control unit that tells a processor when to continue with the next sequential instruction or conditionally branch to another instruction. Control logic is used to create low-level type of programming instructions for these functional units known as microcode or microinstructions. The control logic itself translates low-level instructions into specific electrical signals (known as control signals) that activate the respective digital circuits. In the well-known computing textbook *Computer Organization and Design: the Hardware/Software Interface*, Patterson and Hennessy explain:

[T]hink of the set of control signals that must be asserted in a state as instructions to be executed by the datapath...called *microinstructions*....
...

Designing the control as a program that implements the machine instructions in terms of simpler microinstructions is called *microprogramming*....The microprogram is a symbolic representation of the control that will be translated by a program to control logic.

Ex. 1019 at 3-4.

120. A POSA familiar with computer architecture design in 2005 would be familiar with how all computer processors are managed, at the most fundamental level, by control logic. In the book *Elements of Computing Systems* (2005), Noam Nisan explains that a CPU design is incomplete without control logic, stating:

[T]he CPU's control logic [is] designed to perform the following tasks:

Instruction decoding: Figure out what the instruction means (a function of the instruction).

Instruction execution: Signal the various parts of the computer what they should do in order to execute the instruction (a function of the instruction).

Next instruction fetching: Figure out which instruction to execute next (a function of the instruction and the ALU [Arithmetic Logic Unit] output).

Ex. 1033 at 3. *See also* Ex. 1019 at 3-4. In view of the foregoing, a POSA would also understand that arithmetic operations are essential to a processor's ability to perform encryption functions to create digital signatures or to tabulate prices in the generation of a receipt.

121. Further to the application of control logic in Wang. The Wang patent discloses that “[i]f access to user identification data 302 is desired, e.g., to approve a transaction, the access can only be made by encryption logic block” and describes how the user can “sign the receipt electronically.” Ex. 1004 at [0050], [0115]. While Wang does not explicitly mention control logic, a POSA would understand that any computing device executing such processes inherently relies on control logic. Simply put, there is no way for a computing device to function without control logic.

122. A POSA would appreciate that the Control logic in the context of Wang would be responsible for:

1. Executing Instructions: Performing the necessary steps to encrypt and sign the receipt using the user’s private key.
2. Managing Data Flow: Ensuring that the digitally signed receipt is correctly processed and forwarded.
3. Interfacing with Output Units: Handling the communication between the processor and the output units (e.g., for forwarding the signed receipt).

123. Wang discloses that an output, e.g., a digitally signed receipt, may be forwarded. Ex. 1004 at [0115]. As a practical matter, in view of the foregoing, a POSA would appreciate that computing devices operate using control logic. Thus, a POSA would understand that the output unit of Wang includes control logic for implementing the forwarding of the output. *Id.* A POSA would similarly

understand that to send email or SMS receipts, as described by Drummond, would similarly require control logic with instructions for doing so. Ex. 1008 at [0246]-[0251], [0301], [0307].

Element 19h: Sending an email/text requires message delivery protocol

124. In 2005, the SMS was explained as follows: “Short message service (SMS) is a service available on most digital mobile phones that permits the sending of short messages (also known as SMSes, text messages, messages, or more colloquially texts or even txts) between mobile phones, other handheld devices and, even, fixed-line phones.” Ex. 1030 at 1. SMS relies on an underlying protocol that constrains the length of text messages: Messages are sent with a “message payload is 140 bytes: either 160 7-bit characters, 140 8-bit characters, or 70 2-byte characters.” *Id.*

125. Email was and remains an alternate form of messaging protocol available to popular mobile devices of the era. E-mail messaging from phones, as popularized by NTT Docomo’s i-mode and the RIM BlackBerry, also typically use standard mail protocols such as SMTP over TCP/IP.

126. Email and text messaging (SMS) are two examples of message delivery protocols implemented at the application layer of communication networks. Sending email depends on an implementation of the internet standard SMTP email protocol as originally described in RFC 788 (November 1981) by J. Postel: “The

objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel.” Ex. 1032 at 3.

127. As I show below, claim 20 is obvious over Wang in view of Drummond.

Dependent Claim 20

Claim 20	Wang (Ex. 1004) and Drummond (Ex. 1008)
20. The apparatus of claim 19 wherein the message delivery protocol includes the Short Message Service.	<i>See</i> Ground 3, Elements 19g-h. “electronic receipt may also be a text message sent to a phone number of a mobile phone” Ex. 1008 at [0247], [0301]. The receipt may be sent “using the SMS protocol.” <i>Id.</i> at [0301].

128. As I show below, Claim 21 is obvious over Wang in view of Drummond.

Dependent Claim 21

Claim 21	Wang (Ex. 1004) and Drummond (Ex. 1008)
21. The apparatus of claim 19 wherein the message delivery protocol includes email.	<i>See</i> Ground 3, Elements 19g-h. “receipt may be...in the form of an e-mail message sent to one or more e-mail addresses” Ex. 1008 at [0247].

129. As I show below, Claim 39 is obvious over Wang in view of Drummond.

Independent Claim 39

Claim 39	Wang (Ex. 1004) and Drummond (Ex. 1008)
39. A method of providing secure transaction, the method comprising:	<i>See</i> Ground 1, Preamble 23 analysis.

Claim 39	Wang (Ex. 1004) and Drummond (Ex. 1008)
Elements 39a-f	<i>See</i> Ground 1, Elements 23a-f analysis.
forward the generated output to the user using a message delivery protocol.	<i>See</i> Ground 3, Elements 19g-h. “receipt may be...in the form of an e-mail message sent to one or more e-mail addresses...may also be a text message sent to a phone number of a mobile phone, pager, PDA, or other portable computing device.” Ex. 1008 at [0247], [0301].

130. As I show below, Claim 40 is obvious over Wang in view of Drummond.

Dependent Claim 40

Claim 40	Wang (Ex. 1004) and Drummond (Ex. 1008)
40. The method of claim 30 wherein the message delivery protocol includes the Short Message Service.	<i>See</i> Ground 3, Claim 20.

131. As I show below, Claim 41 is obvious over Wang in view of Drummond.

Dependent Claim 41

Claim 41	Wang (Ex. 1004) and Drummond (Ex. 1008)
41. The method of claim 39 wherein the message delivery protocol includes email.	<i>See</i> Ground 3, Claim 21.

D. GROUND IV: Claims 8 and 30 are obvious over Wang and Denso.

132. It is my opinion that Claims 8 and 30 are obvious over Wang (Ex. 1004) in view of Denso (Ex. 1026) for the reasons that follow.

133. As discussed above in Grounds 1 and 2, Wang describes an apparatus and method for performing secure transactions. Ex. 1004 at [0002]. After authenticating a user of the cellular phone, Wang describes that a barcode scanner of a cellular phone may be used to scan barcodes to select and lookup prices for items for a purchase transaction from a lookup table. *Id.* at [0072], [0115]. Outputs, such as electronically signed receipts (Ground 1) and transaction approval data (Ground 2) may be generated based on the information from the lookup table and from predetermined information stored on the cellular phone prior to scanning the barcodes. *Id.* at [0072]-[0083], [0115]. These outputs may be forwarded to a user and may be digitally signed. *Id.* at [0108], [0112], [0115], [0123]. Wang does not, however, disclose that the barcode is a multi-dimensional barcode. It would be obvious, however, to modify Wang to use a multi-dimensional barcode as taught by Denso for the reasons discussed below. Ex. 1026 at [0013].

Motivation to Combine Wang and Denso

134. Both barcodes and QR codes rely on an optical sensors ability to detect visible 1 or 2 dimensional patterns, and decode those patterns, via a predetermined protocol to a string of numeric or alphanumeric characters. The larger or more detailed the pattern, or the more dimensions, the more characters can be encoded. A barcode enables the display of a single row of symbols, whereas a 2-

dimensional encoding such as a QR code format, enables multiple rows of symbols, enabling more information to be encoded and conveyed to a reader. The most common well-known standard of barcodes is the UPC code which enables the representation of 12 numerical digits. The digits in industry standard barcodes are typically mapped to specific product SKU numbers. A POSA implementing any scheme where additional information beyond product SKUs, such as customer information, storeID, or other more detailed transaction data, would be motivated to choose a multi-dimensional barcode as taught by Denso.

135. Wang discloses that a barcode may be used to store information useable as an index to lookup an item price. Ex. 1004 at [0115]. Denso discloses that it was well known to use barcodes and multi-dimensional barcodes interchangeably to serve as an information code. Ex. 1026 at [0013]. The use of a two-dimensional barcode in place of a standard barcode would enable more data to be encoded within the same space, as the use of two-dimensions increases the data density of the image. The additional data capacity would not only support a greater amount of data, but would also support additional types of data, such as uniform resource locators (URLs), binary codes, and structured data. Multi-dimensional barcodes provide other benefits over standard barcodes, such as supporting error-correction that enables the multi-dimensional barcode to be read even if a portion of the barcode is stained or missing and the ability to be read at various angles. For at

least these reasons, a POSA would be motivated to modify Wang to use a multi-dimensional barcode as the barcode as taught by Denso.

136. The following claim charts demonstrate how Claims 8 and 30 are obvious over Wang in view of Denso.

Dependent Claims 8, 30

Claims 8, 30	Wang (Ex. 1004) and Denso (Ex. 1026)
8. The apparatus of claim 7 wherein the barcode includes a multi-dimensional barcode.	“barcode” Ex. 1004 at [0115] “an information code such as a barcode or a two-dimensional code.” Ex. 1026 at [0013].
30. The method of claim 29 wherein the barcode includes a multi-dimensional barcode.	

E. GROUND V: Claim 13 is obvious over Wang and Raines.

137. Claim 13 is obvious over Wang (Ex. 1004) in view of Raines (Ex. 1009), as explained below.

138. As discussed in Ground 2, Wang discloses all of the features of Claim 1. Wang discloses that the transaction approval data (output) includes user identification data and transaction data. Ex. 1004 at [0045], [0051]. Wang does not, however, explicitly disclose that the transaction approval data includes information relating to a payment card account. It would have been obvious, however, to modify Wang to include an account number and expiration date of a

credit card in its transaction approval data as taught, for example, by Raines, thereby rendering the challenged claims obvious.

Motivation to Combine Wang with Raines

139. Wang discloses that transaction approval data (e.g., an output) is generated based on and includes user identification data and transaction data. Ex. 1004 at [0051]. Wang discloses that user's data from the user (e.g., user-supplied data) includes a credit card number and that the user-supplied data may be stored on the PEAD. Ex. 1004 at [0093]. Raines discloses that it was known to include the account number and expiration date of the credit card in transaction information, as this information is necessary for a credit card transaction to be processed. Ex. 1009 at [0008].

140. Credit card numbers and expiration data are included in transaction approval when authorization requests are sent by a merchant to a card network for approval (ISO 8583, message type 0100). Ex. 1020 at 83. The credit card number (Primary Account Number or PAN) is part of the information required for a credit card processing network like Visa or Mastercard to route an authorization request to the cardholder's appropriate card-issuing bank for authorization. *Id.* A card-issuing bank uses the credit card number to identify their specific cardholder's account in question for the transaction. A card-issuing bank will also validate the provided expiration date as a factor in verifying the legitimacy of the transaction.

141. In response to an authorization request message (ISO 8583 message type 0110), a merchant would receive back a transaction message including data indicating an approval or a decline but not including an expiration date. *See* ISO 8583-1:2003 (now withdrawn), Ex. 1020 at 83, Table 28.

142. Without the inclusion of the credit card number in the transaction data, the purchase transaction using the PEAD could not be completed. Therefore, a POSA would be motivated to modify Wang to include the previously stored credit card number as transaction data in the transaction approval data (output) as taught by Raines to enable the transaction to be completed.

143. The following claim chart shows how the features of Claim 13 are disclosed or rendered obvious by Wang in view of Raines.

Dependent Claim 13

Claim 13	Wang (Ex. 1004) and Raines (Ex. 1009)
13. The apparatus of claim 1 wherein the predetermined information includes information relating to a payment card account; and	Wang recognizes that credit cards may be used for the transaction. Ex. 1004 at [0093]. Wang states that the transaction approval data includes “transaction data.” <i>Id.</i> at [0051]. A POSA would appreciate that transaction data would include information relating to a payment card account to the extent a card was used for the transaction. <i>Id.</i> Wang discloses that “user’s data from the user” (e.g., user-supplied data) includes “a credit card number” and that “user-supplied data may be stored on the PEAD.” <i>Id.</i> at [0093], [0098]. “[A] merchant must collect a variety of data associated with the transaction” including “the account number and expiration date of the credit card” and “the merchant transmits the transaction data.” Ex. 1009 at [0008].
wherein the output further includes some or all of the information relating to the payment card account to be used for payment with respect to the transaction.	A POSA would recognize that for a transaction funded with a card account, the transaction approval data (output) in Wang would include some or all such credit card information as relevant “transaction data.” ²⁵ Ex. 1004 at [0051].

Wang’s transaction approval data would include credit card information as relevant “transaction data.”

144. Wang describes a transaction program (TP), provided by a merchant, installed and running on a user’s device. Ex. 1004 at [0088]-[0102]. Wang describes the TP application as performing functions “for the user’s input approval, and/or authentication.” *Id.* at [0091]. A POSA would understand this as

²⁵ See paragraph 144.

a case where a merchant app, running on a user's phone, authenticates the legitimate identity of the user and solicits the approval of the user to a transaction. A POSA would understand that these actions would be sufficient to initiate a purchase but that further steps would be required to initiate and complete a corresponding credit card transaction. Initially, only the merchant's mobile app itself (e.g., Wang's TP), running locally on the user's device would be aware that the user had authorized a transaction and the specific order details. A POSA would find it obvious that the TP would need to generate an external output to inform the merchant of the successful authentication and user approval. Further, that output would need to include sufficient transaction data (such as specific order details or unique order identifier) for the merchant to know what order details would need to be fulfilled. To process a credit card transaction, additional transaction data required would include a credit card number and expiration date. These data elements were required by credit card networks for credit card authorization requests. *See generally* Ex. 1020. For these reasons, Wang's transaction approval data would include credit card information as relevant "transaction data."

F. GROUND VI: Claims 1, 4, 5, 7, 23, 26, 27, 29, and 43 are obvious over TAO in view of PTM and Wang.

145. Claims 1, 4, 5, 7, 23, 26, 27, 29, and 43 are obvious over TAO (Ex. 1005) in view of PTM (Ex. 1006) and Wang (Ex. 1004), as explained below and in the following claim charts.

146. As discussed above, TAO describes an apparatus and method for performing secure transactions. Ex. 1005 at 1-3. A user may scan in products using a barcode scanner of a cellular phone, such as the Palm Treo, which may add the products to an order. *Id.* Predetermined information about standard discounts is stored on the cellular phone and may be selected and added to the order. *Id.* The order may be generated by the cellular phone and forwarded to a user. *Id.* TAO does not expressly disclose that the cellular phone includes a memory, a processor, or an input device for verifying the user based on input information, or that the output includes a digital signature to be used to signify authorization by the user with respect to the transaction. It would have been obvious, however, to modify TAO to include such features—which were well-known to be present on the Palm Treo device—for the reasons discussed below, thereby rendering the challenged claims obvious.

Motivation to Combine TAO with PTM and Wang

147. Although it suggests it, TAO does not explicitly disclose a memory that stores predetermined information. Instead, TAO discloses that standard discounts

may be stored on the device and that its software may be used on the Palm Treo cellular phone. Ex. 1005 at 1-3. PTM indicates that the Palm Treo includes internal memory, which may store various information. Ex. 1006 at 112. A POSA would recognize that a cellular phone as disclosed by TAO would require a memory to properly function, to store the software for use by the cellular phone, and to store the standard discounts referenced in TAO. Additionally, the use of an internal memory would enable the software to store standard discounts and customer data, such as the name and address, on the internal memory to enable quicker order generation by eliminating the need to enter such data by hand. For at least these reasons, a POSA would be motivated to modify TAO to store the predetermined information in the memory of a cellular phone as taught by PTM.

148. TAO also fails to explicitly disclose an input device for receiving input information and verifying the user based on the input information, but TAO discloses that its software may be used on the Palm Treo cellular phone, which includes a keyboard (an input device). PTM indicates that the Palm Treo includes a keyboard and a system lock that requires input of a password to verify the user to access data on the device. Ex. 1006 at 24, 129. Use of a keyboard to enter a password for a system lock as taught by PTM would enable the user to restrict access to the handheld device to only authorized users, thereby enhancing security and protecting customer data stored on the device. More specifically, the use of a

password would prevent unauthorized users from attempting to generate unauthorized orders using the cellular phone. Additionally, the requirement of a password to access TAO's device would add a level of trust between the merchant and customer, as both parties would have assurance that the user conducting the transaction on the handheld device was an authorized user. For at least these reasons, a POSA would be motivated to modify TAO to include a keyboard (e.g., input device) and require a password for authentication as taught by PTM.

149. TAO also fails to explicitly disclose a processor. Here too, TAO discloses that its software may be used on the Palm Treo cellular phone. Ex. 1005 at 1-3; Ex. 1034 at 5-6. PTM indicates that the Palm Treo includes a processor. Ex. 1006 at 173. A POSA would recognize that the cellular phone disclosed by TAO would require a processor to properly function and to execute the software installed on the cellular phone to facilitate the generation of orders (outputs). For at least these reasons, a POSA would be motivated to modify TAO to include a processor as taught by PTM.

150. TAO also fails to explicitly disclose that the output includes a digital signature to be used to signify authorization by the user with respect to the transaction. A POSA would understand that there are multiple senses in which signatures are essential to the workflow involved in order processing and completing transactions.

151. For example, manual signatures were a standard requirement for the approval of purchase orders and payments before the widespread adoption of digital signature technology. The practice of requiring signatures ensured that transactions were authorized by the correct responsible parties, maintaining the integrity and accountability of financial operations.

152. By 2005 a POSA would be motivated to employ digital signatures to these workflows. By enabling electronic approvals, businesses could reduce the need for physical paperwork, and expediting the procurement process. As documented in “Applied Cryptography” by Bruce Schneier, digital signatures not only facilitate secure transactions but also provide a legal framework for electronic commerce by ensuring that signed documents are legally binding and enforceable. Ex. 1017 at 74-73.

153. Digital signatures were valuable in common purchasing workflows due to their ability to ensure the authenticity, integrity, and non-repudiation of electronic documents. Digital signatures provided a secure and efficient method for verifying the identity of the signer and confirming that the contents of the purchase order had not been altered after signing. According to the National Institute of Standards and Technology (NIST) in their Digital Signature Standard (DSS) publication, digital signatures authenticate the signer and bind their identity to the document, which is crucial for the approval process of purchase orders. (NIST FIPS PUB

140-2 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES,
Ex. 1031 at 5 (2000)).

154. In 2005 it was well understood by the general public as well as by persons skilled in the art, that retail transactions performed with credit cards required the user to sign a receipt. According to one source: “When a purchase is made, the credit card user indicates his/her consent to pay, usually by signing a receipt with a record of the card details and indicating the amount to be paid.” Ex. 1024 at 1.

155. Addressing the prior art, TAO discloses outputting an electronic order (e.g., a record of a purchase transaction, or a receipt), while Wang discloses that electronic receipts may include electronic signatures. Ex. 1004 at [0115]. Wang discloses that electronic signatures may be generated by appending identification data (such as private keys) onto the receipt. *Id.* at [0051], [0108], [0112], [0123]. The inclusion of an electronic signature on a receipt would allow the receiving party, such as a merchant, to identity and authenticate the party sending the order. As taught by Wang, access to private keys for electronic signatures may be accessed only after successful authentication of the user. *Id.* at [0123]. The authentication of the user and subsequent electronic signature accompanying the receipt therefore provides assurance of the identity of the device user to other parties (including a payment processor) in e-commerce transactions who

otherwise cannot verify the identity of the device user due to the online nature of the purchase.

156. The same purpose and benefit would apply to digitally signing the orders described in TAO. Thus, for at least these reasons, a POSA would be motivated to modify TAO to modify the order (output) to have a digital signature as taught by Wang, i.e., to verify that the order was created by an authorized user.

157. Concerning Claims 4 and 26, TAO fails to explicitly disclose that the input information includes one of a personal identification number and biometric information. TAO discloses that its software may be used on cellular phones, such as the Palm Treo cellular phone, which includes a system lock that requires input of a password to access data on the device, as evidenced by PTM. Ex. 1005 at 1-3; Ex. 1006 at 129. Wang discloses that it was known to use biometrics (such as fingerprints, voice prints, or other biometrics) to authenticate a user of a cellular phone. Ex. 1004 at [0072]. Use of biometrics, rather than just a password, would enhance the security of the device and transactions performed using the device. More specifically, as disclosed in Wang, the use of biometrics provides more complicated and elaborate authentication data than a simple password and make it harder for an unauthorized user to access and utilize the TAO device. *Id.* at [0045]. Biometrics, such as voice prints, would be possible using existing hardware of a cellular phone, such as a Treo, and would also provide enhanced

security over a password alone. For at least these reasons, a POSA would be motivated to modify TAO to utilize a biometric as input information as taught by Wang.

158. As I show below, Claim 1 is obvious over TAO in view of PTM and Wang.

Independent Claim 1

Claim 1	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
[Preamble 1] 1. An apparatus for providing a secure transaction, the apparatus comprising:	“the handheld tool” is an apparatus. Ex. 1005 at 1. “Taking orders from customers....” is a transaction. <i>Id.</i> “Our software runs on...PalmOS...and is licensed for use on handheld devices made by palmOne (including the Treo...).” Ex. 1005 at 3. The Treo “[r]equires a password to see any data...” indicating that it is secure. Ex. 1006 at 24, 129. Wang discloses an apparatus for providing a secure transaction. “portable electronic authorization devices (PEADs) which eliminate the security risks associated with...approving transactions...” Ex. 1004 at [0002].
[1a] an image capture device configured to capture an image, the image having information embedded therein including information relating to a transaction;	“barcode-scanning capability..., a PalmOS handheld equipped with a barcode scanner.” Ex. 1005 at 3. “point the scanner at the product, press the scan button, and the item is added to the order!” <i>Id.</i> at 2. A barcode scanner is an image capture device. TAO discloses an image capture device that captures an image (e.g., a barcode) that has information embedded therein (e.g., a pointer that identifies an item of a product catalog) that is usable for a purchase transaction.
[1b] a memory configured to store	“Our software runs on the Palm operating system....and is licensed for use on handheld devices made by palmOne (including the Treo...).” Ex. 1005 at 3.

Claim 1	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
predetermined information;	“If that customer has a standard discount, the order will be automatically set to indicate that.” <i>Id.</i> at 2. The standard discount is “predetermined information.” The Palm Treo has an “internal memory” and a POSA would understand that the standard discount information is stored in memory in order to be “automatically set to indicate that” as indicated by TAO.²⁶ Ex. 1006 at 97, 109, 112.
[1c] an input unit configured to receive input information provided by a user;	“use on handheld devices made by palmOne (including the Treo” Ex. 1005 at 3. The Treo has a “keyboard,” which is an input unit, and “[r]equires a password to see any data....” Ex. 1006 at 24, 129. A password is input information.
[1d] a processor configured to:	“use on handheld devices made by palmOne (including the Treo” Ex. 1005 at 3. “144 MHz Texas Instruments OMAP (ARM) processor.” Ex. 1006 at 73. The Treo has a processor and a POSA would recognize that, like other handheld devices, the processor is configured to perform the various functions of the device.
[1e] verify the user based on the input information to ensure that the user is authorized to use the apparatus; and	“use on handheld devices made by palmOne (including the Treo....” Ex. 1005 at 3. “Requires a password to see any data....” Ex. 1006 at 129.
[1f] generate an output based on the information embedded in the	“point the scanner at the product, press the scan button, and the item is added to the order!” Ex. 1005 at 1.

²⁶ See paragraphs 159 - 162.

Claim 1	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
image and the predetermined information; and	“If that customer has a standard discount, the order will be automatically set to indicate that...” <i>Id.</i> at 2. The order is an output generated by the handheld device based on the information embedded in the image (e.g., the barcode), which is used to add items to the order and the predetermined information (e.g., the standard discount).
[1g] an output unit configured to forward the output generated by the processor, wherein	“the order and summary information are transferred to your desktop...” Ex. 1005 at 3. The order (e.g., output) is forwarded by an output unit of the handheld device to a desktop computer.
[1h] the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	“As a further example, the PEAD may be employed to ‘sign’ any computer file for authentication purposes (e.g., to authenticate the date or the user).” Ex. 1004 at [0085]. A POSA would understand from TAO in view of Wang that the order of TAO may include a digital signature, as described in Wang, to provide verification that the order was created by an authorized user.²⁷

The standard discount information would be stored in internal memory.

159. A POSA would appreciate that for the software on the Palm Treo to have been configured (“automatically set”) to perform discount calculations, the instructions to do so must have been previously stored on the internal memory. A POSA would understand that the pricing and discount data also would also be stored in advance on the device. At a minimum, however, the processing instructions must have been stored locally in memory in advance. Those

²⁷ See paragraphs 150 - 156.

instructions would include control logic for the device processor to look up discount data from local memory storage or to dynamically look up the same data from a remote computer database.

160. Pre-storing discount information on the device would have the advantage of enabling calculation of pricing quickly and locally on the mobile device, with or without the availability of a reliable network connection. *See Oracle Mobile Application Foundation (2003), Ex. 1021, at 11-12.* A person experienced in developing mobile software in 2005 would understand that network coverage is not always reliable in speed or availability. Therefore, pre-storing information on devices adds user reliability and user convenience. Alternately, pricing or pricing discounts could be looked up dynamically from a central database managed by the merchant. This look up approach adds convenience for a merchant by helping to ensure that devices are referring to most current pricing or discount tables, or to enable more dynamic pricing. A POSA also would understand that these two approaches are not mutually exclusive, and that in either case the instructions and control logic on how, where, and when to look up discount data would have to have been preconfigured and stored locally on the device, in order for this process to be able to execute “automatically.”

161. In mobile devices, applications are typically stored in flash memory, a type of non-volatile storage that retains data even when the device is powered off.

Flash memory offers the durability and reliability needed for mobile environments, allowing applications and system software to be stored persistently. Flash memory provides a stable storage medium that can withstand numerous read and write cycles, making it ideal for storing applications that need to be readily accessible on a mobile device. *See* US Pat. No. 5,404,485 (Ban), Ex. 1022, at Abstract, 3:51-4:10.

162. At runtime, the processor accesses these stored applications by loading the necessary instructions and data from flash memory into short-term memory or RAM (Random Access Memory). This process is necessary for execution, as the processor operates much faster when using data stored in RAM. Programming instructions are themselves a form of stored short data sequences which can be decoded by the processor into individual instructions. As detailed by Hennessy and Patterson (1990), the fetch-decode-execute cycle begins with the processor fetching instructions from memory, which, in the case of mobile devices, involves reading from flash memory initially and transferring the data to RAM for quicker access. Ex. 1023 at 3. This allows the device to execute the applications efficiently, leveraging the faster access speeds of RAM while maintaining the persistent storage benefits of flash memory. In view of the foregoing, a POSA would appreciate that the discount information disclosed in TAO would be stored in its internal memory. To the extent that this feature is not expressly disclosed in

TAO, it would be obvious to modify TAO to store the discount information in the Palm Treo internal memory for the reasons discussed above.

163. As I show below, Claim 4 is obvious over TAO in view of PTM and Wang.

Dependent Claim 4

Claim 4	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
Element 4	“use on handheld devices made by palmOne (including the Treo” Ex. 1005 at 3. “Requires a password to see any data...” Ex. 1006 at 129. “require the user to enter a password, to furnish fingerprints or a voice print, or other biometrics” Ex. 1004 at [0073].

164. As I show below, Claim 5 is obvious over TAO in view of PTM and Wang.

Dependent Claim 5

Claim 5	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
5. The apparatus of claim 1 wherein the output unit is a display.	“the day’s sales are summarized and displayed and/or printed.” Ex. 1005 at 2-3. The day’s sales (e.g., orders) is an output that is presented on a display.

165. As I show below, Claim 7 is obvious over TAO in view of PTM and Wang.

Dependent Claim 7

Claim 7	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
7. The apparatus of claim 1 wherein the image includes a barcode.	“barcode-scanning capability...a PalmOS handheld equipped with a barcode scanner....” Ex. 1005 at 3. “point the scanner at the product, press the scan button, and the item is added to the order!” <i>Id.</i> at 1.

166. As I show below, Claim 23 is obvious over TAO in view of PTM and Wang.

Independent Claim 23

Claim 23	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
[Preamble 23] 23. A method of providing secure transaction, the method comprising:	<i>See</i> Ground 6, Element 1 preamble. TAO discloses a method for providing a secure transaction.
[23d] configuring a portable device to:	TAO discloses a handheld device configured to perform the steps described in TAO and outlined in this claim chart. For the device to perform the functions described in TAO, it must have been configured to do so.²⁸ <i>See also</i> Ground 6, Element 1d analysis. “software runs... on handheld devices made by palmOne (including the Treo...)” Ex. 1005 at 3. Software is used to configure the Palm Treo portable device to perform the various functions recited in TAO and Wang.
Element 23a-c,e,f	<i>See</i> Ground 6, Elements 1a-c,e,f analyses.

²⁸ *See* paragraph 167.

Claim 23	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
[23g] forward the generated output to the user,	“the order and summary information are transferred to your desktop” Ex. 1005 at 3. The use of “your” indicates the output is forwarded “to the user.”²⁹ The order (e.g., output) is forwarded by an output unit of the handheld device to a desktop computer.
[23h] wherein the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	<i>See</i> Ground 6, Element 1h.

Element 23d: The cited art discloses “configuring a device” to perform the recited steps.

167. A POSA would understand that TAO, PTM, and Wang indicate that the Palm Treo device mentioned in Take and Order and described in PTM must be configured to display the order for it to do so. That configuration would consist of: at the hardware level, specifying and assembling the device to contain a screen output device connected to the processor; at the software application level, providing instructions to the processor to visually format and display the order output on the screen.

²⁹ *See* paragraph 168.

Element 23g: TAO discloses forwarding the output “to the user.”

168. In the case of the TAO sales literature, the literature is drafted in the second person, with the use of “you” indicating the user of the TAO software, i.e., the merchant who is “selling products at a trade shows or expos...” Ex. 1005 at 1.

To be clear, the user in TAO is the merchant—not the customer. Further, the context of TAO makes clear that the “you” or “your” in their literature refers to the seller in a merchant transaction as the user and operator of the device running their software. Thus, by indicating that “the order and summary information are transferred to your desktop,” (emphasis added) TAO is indicating that the order is forwarded to the merchant’s desktop computer. Ex. 1005 at 3. That is, the use of “your” in this passage of TAO indicates the output is forwarded “to the user.”

169. As I show below, Claim 26 is obvious over TAO in view of PTM and Wang.

Dependent Claim 26

Claim 26	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
26. The method of claim 23 wherein the input information includes one of a personal identification number and biometric information.	<i>See</i> Ground 6, Claim 4 analysis.

170. As I show below, Claim 27 is obvious over TAO in view of PTM and Wang.

Dependent Claim 27

Claim 27	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
27. The method of claim 23 further comprising: configuring the portable device to display the output.	See Ground 6, Claim 5 analysis. To display the order as taught by TAO, the device must be configured to do so.

171. As I show below, Claim 29 is obvious over TAO in view of PTM and Wang

Dependent Claim 29

Claim 29	TAO (Ex. 1005), PTM (Ex. 1006), and Wang (Ex. 1004)
29. The method of claim 23 wherein the image includes a barcode.	See Ground 6, Claim 7 analysis.

172. As I show below, Claim 43 is obvious over TAO in view of PTM and Wang.

Independent Claim 43

Claim 43	TAO (Ex. 1005), PTM (Ex. 1006) and Wang (Ex. 1004)
Preamble 43	See Ground 6, Preamble 23 analysis.
Elements 43a-g	See Ground 6, Elements 23a-g analysis.
Element 43h	“ software runs on...handheld devices made by palmOne (including the Treo...). ” Ex. 1005 at 3.

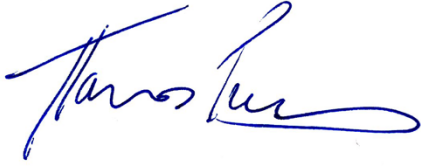
Claim 43	TAO (Ex. 1005), PTM (Ex. 1006) and Wang (Ex. 1004)
	The Palm Treo is a cellular phone as indicated by its full name “Treo 600 Smartphone by PalmOne”. Ex. 1006 at 1.

VIII. Conclusion

173. For the foregoing reasons, it is my opinion that Claims 1, 2, 4, 5, 7, 8, 12, 13, 17, 19-21, 23, 26, 27, 29, 30, 34, 39-41, and 43 of U.S. Patent No. 7,314,167 are neither novel nor non-obvious over the prior art of record.

I declare under penalty of perjury under the laws of the United States of America
that the foregoing is true and correct.

Executed on: July 29, 2024

A handwritten signature in blue ink, appearing to read "Tara L.", is written above a horizontal line.

By: _____

(Signature)

Appendix A

U.S. PATENT NO. 7,314,167 CLAIM APPENDIX

1. An apparatus for providing a secure transaction, the apparatus comprising:	Preamble 1
an image capture device configured to capture an image, the image having information embedded therein including information relating to a transaction;	Element 1a
a memory configured to store predetermined information;	Element 1b
an input unit configured to receive input information provided by a user;	Element 1c
a processor configured to:	Element 1d
verify the user based on the input information to ensure that the user is authorized to use the apparatus; and	Element 1e
generate an output based on the information embedded in the image and the predetermined information; and	Element 1f
an output unit configured to forward the output generated by the processor, wherein	Element 1g
the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	Element 1h
2. The apparatus of claim 1 wherein the processor is further configured to	Element 2

generate the output using the input information.	
3. The apparatus of claim 1 wherein the processor is further configured to decode the information embedded in the image for use in generating the output by using a decryption algorithm.	Element 3
4. The apparatus of claim 1 wherein the input information includes one of a personal identification number and biometric information.	Element 4
5. The apparatus of claim 1 wherein the output unit is a display.	Element 5
6. The apparatus of claim 1 wherein the output is provided to a verifier, the verifier having access to the information embedded in the image.	Element 6
7. The apparatus of claim 1 wherein the image includes a barcode.	Element 7
8. The apparatus of claim 7 wherein the barcode includes a multi-dimensional barcode.	Element 8
9. The apparatus of claim 1 wherein the image includes a set of barcodes.	Element 9
10. The apparatus of claim 9 wherein the set of barcodes includes a set of multi-dimensional barcodes.	Element 10
11. The apparatus of claim 1 wherein the output includes an authentication code to be used to authenticate the user with respect to the transaction.	Element 11

12. The apparatus of claim 1 wherein the transaction includes an online transaction.	Element 12
13. The apparatus of claim 1 wherein the predetermined information includes information relating to a payment card account; and	Element 13a
wherein the output further includes some or all of the information relating to the payment card account to be used for payment with respect to the transaction.	Element 13b
14. The apparatus of claim 1 wherein the information embedded in the image includes information relating to a password to be used to unlock a secured document; and	Element 14a
wherein the output includes the password to be used to unlock the secured document.	Element 14b
15. The apparatus of claim 1 wherein the information embedded in the image includes information relating to a challenge; and	Element 15a
wherein the output includes a password to be used to satisfy the challenge and unlock a secured document.	Element 15b
16. The apparatus of claim 1 wherein the information embedded in the image includes information provided by a vendor relating to a pending transaction; and	Element 16a

wherein the output includes some or all of the information provided by the vendor to be used to alert the user with respect to the pending transaction.	Element 16b
17. The apparatus of claim 1, wherein the apparatus is a cellphone.	Element 17
18. The apparatus of claim 1, wherein the apparatus includes a smartcard claim 1.	Element 18
19. An apparatus for providing a secure transaction, the apparatus comprising:	Preamble 19
an image capture device configured to capture an image, the image having information embedded therein;	Element 19a
a memory configured to store predetermined location;	Element 19b
an input unit configured to receive input information provided by a user;	Element 19c
a processor configured to:	Element 19d
verify the user based on the input information to ensure that the user is authorized to use the apparatus; and	Element 19e
generate an output based on the information embedded in the image and the predetermined information; and	Element 19f
an output unit configured to forward the output generated by the processor, wherein	Element 19g

the output unit includes control logic configured to forward the output using a message delivery protocol.	Element 19h
20. The apparatus of claim 19 wherein the message delivery protocol includes the Short Message Service.	Element 20
21. The apparatus of claim 19 wherein the message delivery protocol includes email.	Element 21
22. The apparatus of claim 19 wherein the message delivery protocol includes the Extended Message Service.	Element 22
23. A method of providing secure transaction, the method comprising:	Preamble 23
configuring a portable device to:	Element 23d ³⁰
capture an image, the image having information embedded therein, the information embedded in the image including information relating to a transaction;	Element 23a
store predetermined information;	Element 23b
receive input information provided by a user;	Element 23c

³⁰ In the claim appendix and claim charts, sub-elements a-h of claim 23 are out of order so that the claim 23 sub-elements correspond to similar sub-elements of claim 1.

verify the user based on the input information to ensure that the user is authorized to use the portable device;	Element 23e
generate an output based on the information embedded in the image and the predetermined information; and	Element 23f
forward the generated output to the user,	Element 23g
wherein the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.	Element 23h
24. The method of claim 23 further comprising: configuring the portable device to generate the output using the input information.	Element 24
25. The method of claim 23 further comprising: configuring the portable device to decode the information embedded in the image for use in generating the output by using a decryption algorithm.	Element 25
26. The method of claim 23 wherein the input information includes one of a personal identification number and biometric information.	Element 26
27. The method of claim 23 further comprising:	Element 27

configuring the portable device to display the output.	
28. The method of claim 23 wherein the output is provided to a verifier, the verifier having access to the information embedded in the image.	Element 28
29. The method of claim 23 wherein the image includes a barcode.	Element 29
30. The method of claim 29 wherein the barcode includes a multi-dimensional barcode.	Element 30
31. The method of claim 23 wherein the image includes a set of barcodes.	Element 31
32. The method of claim 31 wherein the set of barcodes includes a set of multi-dimensional barcodes.	Element 32
33. The method of claim 23 wherein the output represents an authentication code to be used to authenticate the user with respect to the transaction.	Element 33
34. The method of claim 23 wherein the transaction includes an online transaction.	Element 34
35. The method of claim 23 wherein the predetermined information includes information relating to a payment card account; and	Element 35a
wherein the output further includes some or all of the information relating to the payment card account to be used	Element 35b

for payment with respect to the transaction.	
36. The method of claim 23 wherein the information embedded in the image includes information relating to a password to be used to unlock a secured document;	Element 36a
and wherein the output includes the password to be used to unlock the secured document.	Element 36b
37. The method of claim 23 wherein the information embedded in the image includes information provided by a vendor relating to a pending transaction; and	Element 37a
wherein the output includes some or all of the information provided by the vendor to be used to alert the user with respect to the pending transaction.	Element 37b
38. The method of claim 23 wherein the information embedded in the image includes information relating to a challenge;	Element 38a
wherein the output includes a password to be used to satisfy the challenge and unlock a secured document.	Element 38b
39. A method of providing secure transaction, the method comprising:	Preamble 39
configuring a portable device to:	Element 39a
capture an image, the image having information embedded therein;	Element 39b

store predetermined information;	Element 39c
receive input information provided by a user;	Element 39d
verify the user based on the input information to ensure that the user is authorized to use the portable device;	Element 39e
generate an output based on the information embedded in the image and the predetermined information; and	Element 39f
forward the generated output to the user using a message delivery protocol.	Element 39g
40. The method of claim 30 wherein the message delivery protocol includes the Short Message Service.	Element 40
41. The method of claim 39 wherein the message delivery protocol includes email.	Element 41
42. The method of claim 39 wherein the message delivery protocol includes the 5 Extended Message Service.	Element 42
43. A method of providing secure transaction, the method comprising:	Preamble 43
configuring a portable device to:	Element 43a
capture an image, the image having information embedded therein;	Element 43b
store predetermined information;	Element 43c
receive input information provided by a user;	Element 43d

verify the user based on the input information to ensure that the user is authorized to use the portable device;	Element 43e
generate an output based on the information embedded in the image and the predetermined information; and	Element 43f
forward the generated output to the user,	Element 43g
wherein the portable device includes one of a cell phone, a personal digital assistant, and a smartcard.	Element 43h

APPENDIX B

Exhibit	Description
1001	U.S. Pat. No. 7,314,167 B1
1002	Declaration of Thomas Purves
1003	Prosecution History of the '167 Patent
1004	Wang (US Pub. No. 2002/0023215 A1)
1005	Take an Order (TAO)
1006	Palm Treo Manual (PTM)
1007	Oxford Dictionary: “predetermined”
1008	Drummond (US Pub. No. 2003/0217005 A1)
1009	Raines (US Pub. No. 2004/0193538 A1)
1010	Internet Archive Declaration (July 16, 2024)
1011	Palm Sales Article
1012	Comparison of Wang Ex. 1004 to US Pat. No. 5,917,913
1013	Stevens Creek Software Awards website
1014	Visa 3-D Secure System Overview
1015	Predko, Programming and Customizing the 8051 Microcontroller (1999).
1016	Reserved
1017	Schneier (1996), “Applied Cryptography”
1018	2005 Wikipedia entry: “Digital Signature”
1019	Patterson, “Computer Organization and Design: The Hardware/Software Interface” (1993)

1020	ISO 8583-1:2003
1021	Oracle Mobile Application Foundation (2003)
1022	Ban (US Pat. No. 5,404,485)
1023	Hennessy, <i>Computer Architecture: A Quantitative Approach</i> (2003)
1024	2005 Wikipedia entry: “Credit Card”
1025	Pogue, “The Awkward Smart Phone Grows Up,” <i>New York Times</i> (June 30, 2005)
1026	JP4396018B2 (Denso) (with translation)
1027	US Pat. No. 5,917,913 (Wang II)
1028	“Seiko Instruments...” <i>Business Wire</i> (2000)
1029	“SiPix’s Pocket Printer...” <i>PR Newswire</i> (2001)
1030	2005 Wikipedia entry: “Short Message Service (SMS)”
1031	NIST Security Requirements for Cryptographic Modules (2001)
1032	Postel, J., Simple Mail Transfer Protocol (1981)
1033	Nisan, “Elements of Computing Systems” (2005)
1034	Internet Archive Declaration (July 26, 2024)
1035	Marriott, “Keeping Track of Business Cards...,” <i>New York Times</i> (Dec. 9, 2004).

APPENDIX C

TOM PURVES

Digital Payments and Technology Consultant, ex. VP Global Product Architecture @ Visa, Startup CTO & CPO, Angel and advisor. Author of 80+ patents in mobile wallets, secure payment technology and cryptography.

SKILLS

Product & Technology partnerships, Scaling Teams, Scaling Products, Fintech SaaS, digital commerce, Card Products, Portfolio Management, Digital Issuance, AI, Generative AI, ML, Data Products, Open Banking, Embedded Finance, tokenization, digital wallets, compliance tech, fraud, AML/KYC, UI/UX, Experience Design, analytics, mobile commerce, GTM, mobile banking apps & SDKs

PROFESSIONAL EXPERIENCE

LaHave.io Product Strategy and AI Transformation Consulting, Seattle, WA,
April 2021 – Present

Co-founder

Strategic Product Consulting – Enabling fintechs and large Fis to launch and scale embedded fintech partnerships, AI Operations transformation and implementation

Fractional Startup CPO – product strategy, distribution strategy and executive coaching for diverse clients: global Cloud & AI startups Pingme & OkHi (alternative credit data for Sub-Saharan Africa); Grabbi (food service mobile checkout), and Flow Networks (payment engagement experiences), BizFi (AI-optimized B2B lending)

MainStreet, San Jose, CA, Mar 2022 – April 2023

CTO & Chief Product Officer

Enable thousands of SMB customers to unlock billions in eligible tax credits, B2B procurement and commercial banking products with easy-to-use AI & ML powered workflows build on top of data partnerships with platforms including Plaid, Stripe, Codat and Rippling

Led Product, Design and Engineering orgs, 75 directs. Navigated Mainstreet through 2022 fintech downturn, from blitz-scale growth to cashflow-positive.

Visa, San Francisco, CA, April 2011 – April 2021

VP, Global Digital Products

Conceived and led Visa's product portfolio for fintech partners, open banking and digital issuance solutions. Launched multiple products generating +40M ARR in <2 yrs. Unlocked distribution to many of the world's largest banks and fintechs, super-apps and digital banks through developer-friendly API & mobile SDK designs as well as first-time re-seller partnerships with processors and banking-as-a-

service vendors. Products including Visa Transaction Controls, In-app card provisioning, FX & currency services, card enrollment & lifecycle management and risk/fraud management and loyalty value add services.

Led a successful digital transformation of Visa’s global Account Level Management (ALM) and Rewards Program Management (RPM) platforms. From batch-only legacy processes to rich new UI tools and real-time APIs enabling instant digital card activation and personalized card loyalty and benefits. And, for portfolio managers ability to view, manage and control rewards programs, spend tracking and card benefits across 1Trillion+ global Visa Credit, Charge and Commercial card volume.

Led Visa’s global checkout products from 2011 to 2018. Scaled Visa Checkout from 400k to 45M registered users across 25 countries and 300,000 integrated merchants. Enabled easy 2-click checkout buttons across web and native apps, backed by Visa security and tokenization. Established Visa Checkout as a now-multi-brand global standard as SRC/Click-to-pay.

Prolific innovator with over 80+ global patents in checkout experiences, digital wallets, push payments, fraud/risk, identity and more.

EARLY CAREER

Trulioo, SF Vancouver Feb
 2014 – Mar 2018
Advisory Board, Investor
 Leading global vendor of KYC and identity verification services critical for digital services worldwide

Visa, Toronto Jun 2009 –
 Sep 2011
Business Leader, Product Innovation
 Led North America-first commercialization deals for Visa Direct, and NA-first mobile NFC pilots

CIBC, Toronto Feb
 2003 – Feb 2006
Group Manager, New Card Products
 Led Canada-first launch of Visa prepaid, Visa Debit products and mobile money transfers

Certapay, Inc., Toronto – Acquired by Interac Association Dec
 2000 – Nov 2002
Product Manager – Payments Startup
 Co-inventor of Interac E-Transfers [Canada’s Zelle] & Interac Online Debit: today 100’s B GPV

EDUCATION

Master of Business Administration University of Toronto, Toronto, CA

Bachelor of Science in Computer & Electrical Engineering Queen’s University, Kingston, CA

STARTUP & INDUSTRY LEADERSHIP

Tompurves.ai (AI, Fintech & Product Management)

Actionable AI in Banking (2024 CLA Bankers Summit)

DemoCamp Toronto – Event Organizer and Community Leader (2006-2011)

MEIC – Mobile Incubation Lab Board (2005-2007)

Advisory Board – Trulioo 1.8B fintech unicorn (2014-2018), BizFi Commercial lending (2024-current)

Fintech Investor – Trulioo, Clarity Money, Rebel Mail, Maybe, Asaak, Eco, Zama (2012-current)