

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EARLY WARNING SERVICES, LLC,

Petitioner,

v.

INTELLECTUAL VENTURES, LLC,

Patent Owner.

Case No. IPR2024-01221

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

DECLARATION OF KAI JOHNSON

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Qualifications.....	2
III.	Compensation	3
IV.	Materials Considered.....	4
V.	Summary of My Opinions	4
VI.	My Understanding of Certain Patent Law Principles.....	4
VII.	Level of Ordinary Skill in the Art	8
VIII.	Specification of the '167 Patent.....	8
A.	Background	8
1.	The use of static information such as a personal identification number (PIN) was only of nominal effectiveness in reducing payment card fraud	8
B.	Detailed Description Of The Invention.....	12
1.	General Embodiment – Figure 2.....	12
2.	Authentication Embodiment – Figure 3.....	14
3.	Embodiment For Secure Access To Physical Structures.....	19
4.	Alternate Authentication Embodiment – Figure 4.....	20
5.	Authorization Embodiment – Figure 5	23
6.	Alternate Authorization Embodiment – Figure 6	26
7.	Embodiment With Authorization Involving Multiple Parties.....	28
8.	Authorization With Offline Digital Signature – Figure 7.....	28
9.	Secure Document Distribution - Figure 8.....	29
10.	Digital Rights Management	30
11.	Conducting Transactions	31
12.	Checkout Process - Figures 10 and 11.....	32
13.	Defending Against Phishing Attacks - Figure 12	33
14.	Every Embodiment of the '167 Patent Relies on Embedded Information for Security	35

IX.	Claims of the '167 Patent	36
X.	Claim Construction.....	39
	A. “Image capture device” and “capture an image” (all claims)	39
	B. "The image having information embedded therein" (all claims).....	42
	C. “Predetermined information” (all claims).....	47
	D. “A digital signature to be used to signify authorization by the user with respect to the transaction” (claims 1 and 23)	48
XI.	Overview of the Alleged Prior Art	49
	A. U.S. Patent Publ. 2002/0023215 (Wang).....	49
	B. Take An Order (TAO).....	51
	C. U.S. Patent Publ. 2003/0217005 (Drummond)	51
	D. Palm Treo Manual (PTM).....	52
XII.	The Alleged Prior Art Does not Disclose or Suggest the Claims of the '385 Patent	52
	A. Ground I.....	53
	1. Petitioner has not shown that Wang anticipates capturing an image, the image having information embedded therein	53
	2. Petitioner has not shown that Wang anticipates storing predetermined information.....	55
	3. Petitioner has not shown that Wang anticipates generating an output based on the information embedded in the image and the predetermined information.....	57
	4. Petitioner has not shown that Wang anticipates a digital signature to be used to signify authorization by the user.....	59
	5. Petitioner has not shown that the '167 Patent is anticipated by Wang and obvious over Wang in view of Drummond	62
	B. Ground II	62
	1. Petitioner has not shown that Wang anticipates capturing an image, the image having information embedded therein	63
	2. Petitioner has not shown that Wang anticipates storing predetermined information.....	63

3.	Petitioner has not shown that Wang anticipates generating an output based on the information embedded in the image and the predetermined information.....	65
4.	Petitioner has not shown that Wang anticipates the limitation that “the output includes a digital signature to be used to signify authorization by the user with respect to the transaction”	67
5.	Petitioner has not shown that the ’167 Patent is anticipated by Wang	68
C.	Ground III.....	69
1.	Petitioner has not shown that Wang anticipates capturing an image, the image having information embedded therein	69
2.	Petitioner has not shown that Wang anticipates storing predetermined information.....	70
3.	Petitioner has not shown that Wang anticipates generating an output based on the information embedded in the image and the predetermined information.....	71
4.	Petitioner has not shown that the ’167 Patent is obvious over Wang in view of Drummond	72
D.	Ground VI.....	73
1.	Petitioner has not shown that capturing an image, the image having information embedded therein is obvious over TAO in view of PTM and Wang	73
2.	Petitioner has not shown that capturing an image is obvious over TAO in view of PTM and Wang.....	74
3.	Petitioner has not shown that verifying the user is obvious over TAO in view of PTM and Wang	76
4.	Petitioner has not shown that generating an output based on the information embedded in the image is obvious over TAO in view of PTM and Wang.....	79
5.	Petitioner has not shown that the ’167 Patent is obvious over TAO in view of PTM and Wang	80
XIII.	Conclusion	81

I. Introduction

1. My name is Kai Johnson. I have been retained by Petitioner and their counsel, Volpe and Koenig, P.C. (“Volpe Koenig”), as an independent expert consultant for this *Inter Partes* Review IPR2024-01221 of U.S. Patent No. 7,314,167 (“the ’167 Patent”) (Ex. 1001) filed by Early Warning Services, LLC (“Petitioner”).

2. In the Petition for *Inter Partes* Review of U.S. Patent No. 7,314,167 dated July 29, 2024 (the “Petition”), I understand that Petitioner is challenging the validity of claims 1, 2, 4, 5, 7, 8, 12, 13, 17, 19-21, 23, 24, 26, 27, 29, 30, 34, 39-41, and 43 (the “Challenged Claims”) under six grounds of unpatentability.

3. I have been asked to review and comment on statements made by Petitioner’s expert Thomas Purves in his declaration (the “Purves Declaration”, Ex. 1002) in support of the Petition.

4. This declaration is directed to the Challenged Claims of the ’167 Patent and contains statements of my opinions formed in this case to date and the bases and reasons for those opinions. The opinions I present are based on my own judgment. I am not an employee of the Patent Owner, Volpe Koenig, the inventors of the ’167 Patent, or of any affiliated companies. I may offer additional opinions based on further review of materials in this case, including opinions and/or testimony of other expert witnesses.

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

II. Qualifications

6. This section summarizes my educational background, career history, publications, and other relevant qualifications. My curriculum vitae is attached as Patent Owner's Exhibit 2002, which includes my detailed employment background, and professional experience.

7. I have a Bachelor of Science degree in Computer Science from the University of Wisconsin-Madison.

8. I am a consultant with over 32 years of business experience. I am currently the President of Sutton Abinger in San Diego, California, a consulting company focused on solutions for payment systems, security, transit, and mobile applications, through which I provide services to U.S. and international clients in the areas of payment systems, information security, cryptography, and mobile applications. I am also an Advisory Partner to Penser Consulting Ltd., a firm in London which provides consulting services related to the payments industry for clients in Europe, the Middle East, and Asia.

9. I was previously the Product and Technology Leader, Chief Architect,

and Chief Security Officer for Softcard (formerly known as Isis), a joint venture among AT&T, T-Mobile, and Verizon Wireless to develop contactless mobile payments and coupon and loyalty services for retail. Prior to that, I worked as a consultant to Verizon Wireless to develop consumer data products.

10. From 1999 to 2004, I worked in London, UK for enCommerce (acquired by Entrust) and SchlumbergerSema (acquired by Atos Origin) on both pre- and post-sales engagements for cyber security solutions, where many of my clients were in the telecom and financial services industries, and where some of my responsibilities included business development in security and cryptography applications for mobile phones.

11. I am a named inventor on the following six issued patents relating to mobile payments and retail applications: U.S. Patent Nos. 9,563,891; 9,859,953; 10,075,213; 10,387,873; 10,390,199; and 11,132,668.

III. Compensation

12. I am being compensated for my work in this proceeding at a rate of \$500 per hour and receiving reimbursement for expenses incurred in the course of my work. I am also reimbursed for all reasonable expenses that I incur during the course of this case. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any

other proceeding. I have no other interest in this proceeding or the outcome of this matter. I have no financial interest in Patent Owner or affiliation with any of the real parties in interest, the Patent Owner, or the named inventor of the '167 Patent. It is conceivable that I may own mutual funds whose portfolios include stock in the banks that own the Petitioner. If this is the case, the value of such holdings would not constitute a material part of my net worth.

IV. Materials Considered

13. In forming the opinions expressed in this declaration I have reviewed all materials filed in this IPR up to and including this date, including Exhibits 2003-2013 filed with the Patent Owner Preliminary Response.

V. Summary of My Opinions

14. After a review of the alleged prior art asserted by Petitioner and the Purves Declaration, it is my opinion that Petitioner has not shown a reasonable likelihood of success on the grounds of the Petition. My opinions, and the bases, therefore, are detailed throughout this Declaration.

VI. My Understanding of Certain Patent Law Principles

15. As a technical expert, I am offering technical assessments and opinions. In rendering my analysis, I have been informed by counsel regarding various legal standards for determining patentability. I have applied those standards in forming

my technical opinions expressed in this declaration.

16. I understand that an IPR is a proceeding before the USPTO for evaluating the patentability of an issued patent's claims based on prior-art patents and printed publications.

17. I understand that the claims of a patent are reviewed from the point of view of a hypothetical person of ordinary skill in the art ("POSITA") at the time of the filing of the patent. The "art" is the field of technology to which the patent relates.

18. I understand that in determining whether a patent claim is anticipated or obvious in view of the prior art, the Patent Office must apply the *Phillips* standard to construe the claims so that claim terms are given their ordinary and customary meaning as understood by a POSITA at the time of the invention. I understand that inventors are typically persons skilled in the field of the invention and that patents are addressed to and intended to be read by others of skill in the pertinent art. A person of ordinary skill is deemed to read the words used in the patent documents with an understanding of their meaning in the field, and to have knowledge of any special meaning and usage in the field. I understand that claim language is not read in isolation, and the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. I understand that the construction that stays true

to the claim language and most naturally aligns with the patent's description of the invention and the prosecution history will be, in the end, the correct construction.

19. I understand that, in this proceeding, Petitioners have the burden of proving that the challenged claims of the '167 Patent are unpatentable by a preponderance of the evidence. I understand that "preponderance of the evidence" means that a fact or conclusion is more likely true than not true.

20. I understand that there are two ways in which prior art may render a patent claim unpatentable. First, the prior art can "anticipate" the claim. Second, the prior art can render the claim "obvious" to a POSITA. I understand that for an invention claimed in a patent to be patentable, it must not be anticipated and must not be obvious based on what was known before the invention was made.

21. I understand that a patent claim may be invalid as "anticipated" under 35 U.S.C. § 102 if each and every limitation of the claim as properly construed is found, either expressly or inherently, in a single prior art reference, such as a publication or patent, that predates the claimed subject matter. I also understand that a patent claim may be invalid as obvious under 35 U.S.C. § 103 if the differences between the subject matter claimed and the prior art are such that the claimed subject matter as a whole would have been obvious to a POSITA at the time the invention was made. I also understand that several factual inquiries underlie a determination

of obviousness. These inquiries include (1) the 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 (i.e., “secondary considerations”).

22. I also understand that, when a party alleges obviousness based on a combination of references, that party should identify a reason why a POSITA would have been motivated to combine the asserted references in the manner recited in the claims and to explain why a POSITA would have had a reasonable expectation of success in making such combination.

23. I understand that an obviousness analysis permits the application of “common sense” in examining whether a claimed invention would have been obvious to a POSITA. For example, I understand that combining familiar elements according to known methods and in a predictable way may suggest obviousness when such a combination would yield nothing more than predictable results. And I understand a party asserting obviousness should still provide a specific motivation to combine the references as recited in the claims and explain why one would have reasonably expected to succeed in doing so.

24. I understand that one indicator of non-obviousness is when a prior art reference leads in a different direction or discourages that combination, recommends

steps that would not likely lead to the patent's result, or otherwise indicates that a seemingly inoperative device would be produced.

VII. Level of Ordinary Skill in the Art

25. For purposes of this declaration only, I have applied the definition of a POSITA proposed in the Petition.

26. I consider myself to have at least the credentials of a POSITA, and I am capable of addressing the issues from the perspective of such a person. My opinions in this declaration are from the perspective of a POSITA as defined above and during the relevant time frame.

VIII. Specification of the '167 Patent

A. Background

1. The use of static information such as a personal identification number (PIN) was only of nominal effectiveness in reducing payment card fraud

27. The '167 Patent was filed on March 5, 2005 and was directed "to methods and devices for providing secure identification, verification and authorization using a portable secure device" [Ex. 1001, 1:10-11, emphasis added]. At that time, payment card issuers were using various measures to reduce payment card fraud including the use of a personal identification number (PIN). However, as explained in the '167 Patent, use of such static information was only nominally effective in providing security:

... [C]ard issuers are employing various different measures in order to minimize and/or prevent such crimes. For example, in order to provide sufficient authentication, a user may be required to provide additional information during the card approval process, such as, certain numbers printed on the back of the card, the postal zip code for the billing address associated with the card, or a personal identification number (PIN) linked to the card. Because such information is static, it may be of nominal effectiveness. [Ex. 1001, 1:29-38, emphasis added].

28. As explained in the '167 Patent, there were systems where dynamic (non-static) information was used for security at the time, but they were inefficient because they required synchronization. One such system used “a static value and a dynamic variable to generate passwords. For every transaction to be completed, a fixed code is entered into the card by the user at the start of the access request procedure. This fixed code constitutes the static value. The dynamic variable is produced which varies dynamically as a function of time” [Ex. 1001, 1:40-46]. A drawback of this system was that it depended on “time-dependent synchronization” between the card and the server, which was inefficient [Ex. 1001, 1:56-63; 3:11-13].

29. Another prior art system used transaction sequences in both the credit card and the computer of the card issuer to perform verification. In this system, “[b]oth transaction sequence numbers, the one in the card and the one in the computer, are changed by an increment after the authorized transaction so that a different verification number is generated and used in the authorization in each

subsequent credit card transaction” [Ex. 1001, 2:17-21]. Again, this system suffered from the drawback that “[s]ynchronization between the card and the computer is required,” which was inefficient [Ex. 1001, 2:21-22].

30. In another prior art system used for managing financial data, the user’s financial and personal information was stored in a PDA [Ex. 1001, 2:29-30]. The ’167 Patent further described this system as follows:

A digital certificate is downloaded from a central server of a service provider. The digital certificate accomplishes the goal of identification verification by checking whether the digital certificate is expired before providing any credit card information. This system is intended for managing financial data. The foregoing system requires use of shared secret keys between the user and the verifier. It also requires time-dependent synchronization for user verification purposes. [Ex. 1001, 2:30-38]

31. Another prior art system employed tokens to generate unpredictable codes. “The token, which can be a credit-card sized clip or carried as part of a key chain, works in conjunction with hardware or software running on a supplier's server system to generate a new, unpredictable code every 60 seconds that is known to the supplier server” [Ex. 1001, 2:61-66]. Again, this system suffered from the drawback that it required “time-dependent synchronization” [Ex. 1001, 3:9].

32. As explained in the ’167 Patent, the prior art also included a token-based system where a user of the mobile device can order a token from a token issuing system, which produces a token and transmits it to the mobile device [Ex.

1001, 2:39-44]. The user of the mobile device can then later use the token by effecting a “transfer of the token to the token verification system, which receives and processes the token, and allows the user to obtain the benefit, right, or product associated with the token” [Ex. 1001, 2:44-49]. In connection with the transfer of the token to the token verification system, the mobile device included a display that displayed a barcode that contained an encrypted string representing the token. The verifying system (*e.g.*, a point-of-sale device) could include a scanning or image capture device for reading the barcode displayed on the mobile device and decrypting the encrypted string using a shared secret key [Ex. 1001, 2:51-59]. The mobile device in this token-based prior art system did not capture an input image but instead generated and displayed an image to be captured by the verifying system. In addition, the information in the image generated by the mobile device was readable by a conventional barcode scanner.

33. In the ’167 Patent’s review of prior art, existing systems that relied on only static information for security (like a PIN) lacked effectiveness, and systems that used dynamic information for security required synchronization, which was inefficient. In addition, the mobile device in the existing token-based verification system did not capture an input image in connection with obtaining the benefit, right, or product associated with the token. The ’167 Patent disclosed a secure transaction system that improved upon these existing solutions.

B. Detailed Description Of The Invention

34. The specification of the '167 Patent disclosed a portable secure device, and the use of the portable secure device to provide a secure transaction [Ex. 1001, 3:17-18]. In contrast to the prior art systems described above, the portable secure device did not rely solely on static information (like a PIN) for security, and did not require synchronization between the device and a server. Moreover, unlike the token-based system described above, the portable secure device disclosed in the '167 Patent secured the transaction through the use of “an image capture device configured to capture an image having information embedded therein” [Ex. 1001, 3:18-20, emphasis added]. As discussed more fully in relation to claim construction, the term “embedding” as used in the context of the '167 Patent is a term of art that refers to hiding data or information within an image [Ex. 2003, p. 2] (“Data embedding in images is an application that hides secret messages in digital images”).

35. The '167 Patent discloses thirteen embodiments, each of which is discussed in detail below. Significantly, in every embodiment, the embedded information corresponds to information that is hidden in an image and protected using a security technique such as encryption, decryption or a message authentication algorithm.

1. General Embodiment – Figure 2

36. Figure 2 describes the operation a general embodiment of the portable

secure device as follows:

The secure device 100 generally operates in the following manner, as shown in FIG. 2. At block 200, the secure device 100 via the image capture circuit 120 captures information on a still or moving image or a stream of images. The stream of images may constitute a video. The image or video may include, for example, a linear or 2D barcode. ... The image or stream of images contain embedded information that is relevant to the transaction to be conducted. The information embedded in the image or stream of images may be created using any one of a number of well-known decryption/encryption algorithms, such as, a symmetric system using shared keys an asymmetric system using public/private key pairs. ... Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know how to select the appropriate decryption/encryption algorithm for use according to the present invention.

At block 210, the secure device 100 also prompts a user to provide identification information via the input unit 130. The identification information may include a personal identification number (PIN), a password, and/or biometric information. The identification information is used to identify the user to ensure that the user is authorized to use the secure device 100.

At block 220, the secure device 100 via the processor 110 decodes the captured image or video and extracts the relevant embedded information. The processor 110 has knowledge of the encryption algorithm that is used to create the image and thus is able to use the corresponding decryption algorithm to decode the captured image. The decryption algorithm may use one or more input parameters for decoding. For example, if the image is created using a public key, the corresponding private key (as well as other information, such as, predetermined information stored in the memory 150 and the input information provided by the user) may be used to

decrypt or decode the captured image. The predetermined information may include, for example, address information, personal profile information and payment account information. The secure device 100 also checks the identification information provided by the user to verify or authenticate the user's identity. The identification information provided by the user is checked against information previously supplied by the user during registration.

At block 230, upon successful verification of the user's identity and decoding of the captured image, the secure device 100 generates the appropriate instructions or information for the user.

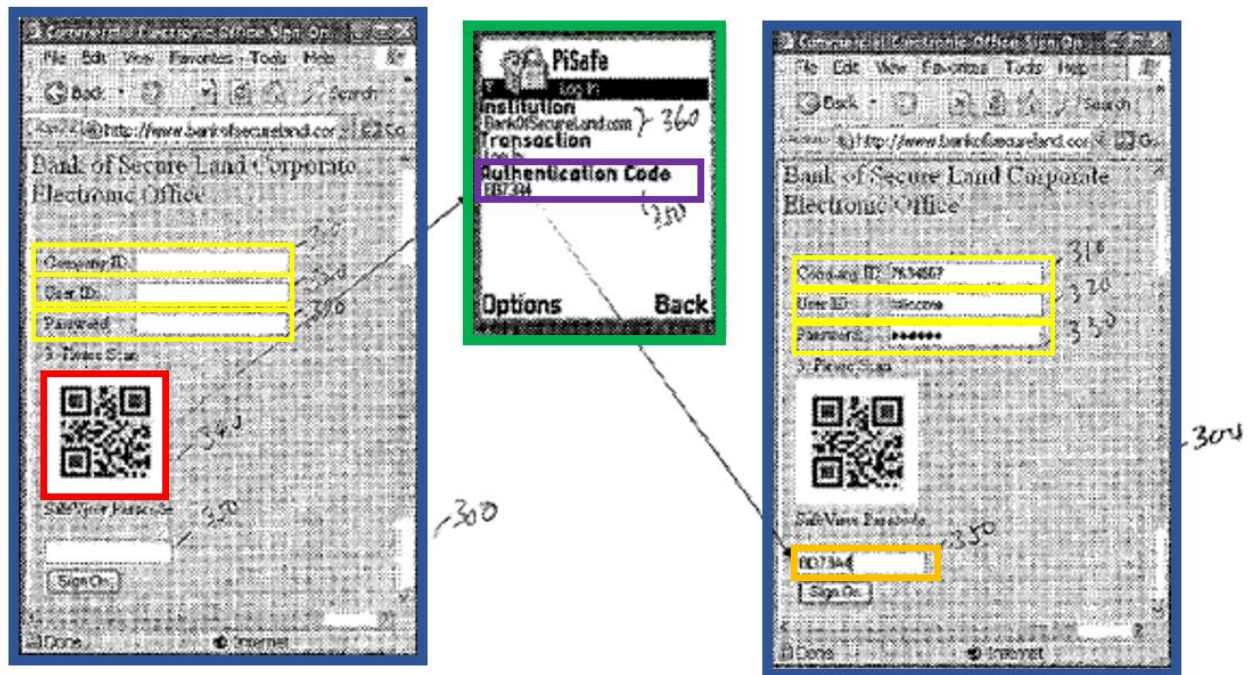
[Ex. 1001, 5:47-6:28, emphasis added]

37. Two aspects of the general embodiment of Figure 2 are worthy of note. First, the mechanism for protecting the embedded information in the general embodiment is an encryption algorithm, and the processor in the secure device requires knowledge of the encryption algorithm to “extract” the “relevant embedded information.” Second, the predetermined information is not the private key but rather “other information” like “address information, personal profile information and payment account information” [Ex. 1001, 6:15-22].

2. Authentication Embodiment – Figure 3

38. Figure 3 depicts an embodiment where the secure portable device “is used to effect authentication” and demonstrates the meaning of “embedded” information in an image within the context of the ’167 Patent [Ex. 1001, 6:40-41]. Figure 3 is reproduced below, where the colored boxes have been added by Patent

Owner. The blue boxes on the left and right identify the log-on screen of a web site requiring user authentication, while the green box in the center depicts the display of the portable secure device.



[Ex. 1001, Figure 3, color added]

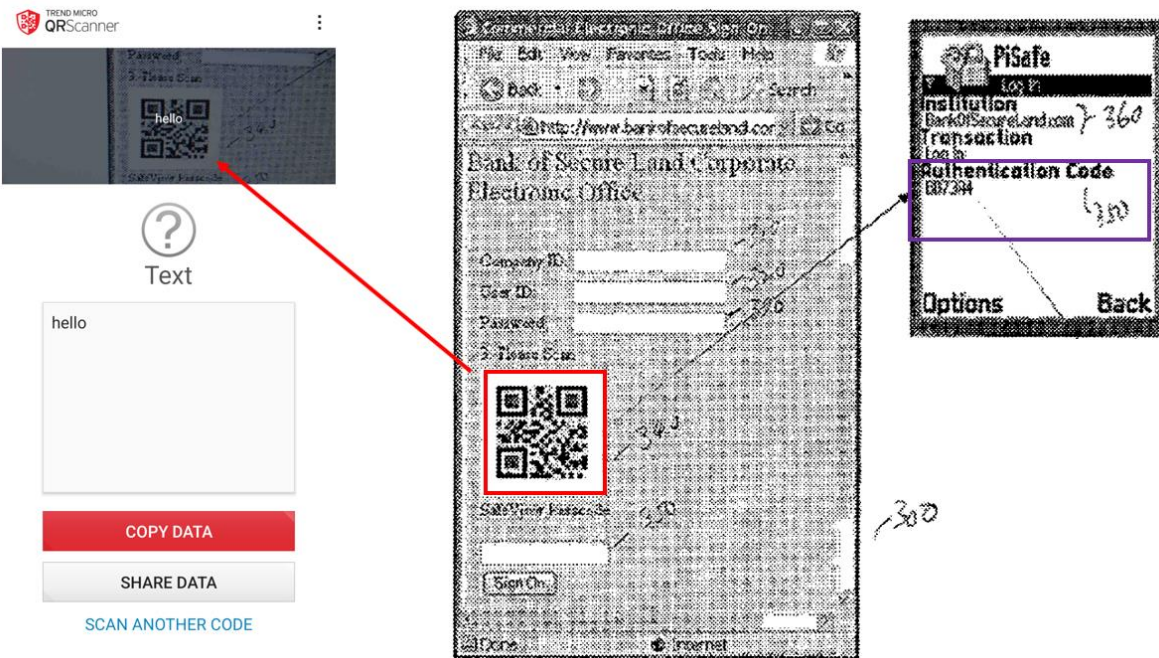
39. In the embodiment associated with Figure 3, “a user visits a website and is presented with a log-on screen 300” (blue boxes). [Ex. 1001, 6:43-44]. “The user is required to enter certain correct information (such as, company ID 310, user ID 320 and password 330) [shown in yellow boxes] before further access to the website is granted” [Ex. 1001, 6:45-47]. Additionally, in order to access the website, the correct authentication code 350 (purple box) must be derived by the portable secure device based on image 340 (red box) and entered by the user into the log-on

screen (orange box) [Ex. 1001, 6:49-54]. As explained in more detail in the '167 Patent:

The user activates the secure device 100 and uses the secure device 100 to scan the image or video 340 [red box]. As part of the activation process, the user may need to enter a password or other types of identification information into the secure device 100 to ensure that the user is authorized to use the secure device 100. The secure device 100 then derives the authentication code 350 [purple box] and other relevant information 360 based on the embedded information stored in the scanned image or video 340 and, optionally, other types of information including, for example, predetermined information stored in the secure device 100 and identification information provided by the user. The derivation process may be performed using an encryption, a decryption or a message authentication algorithm. If the image 340 [red box] has been generated using an encryption or decryption algorithm, the derivation process may correspond to the encryption or decryption algorithm used to create the information embedded in the image or video 340. The authentication code 350 [purple box] and other relevant information 360 are displayed on secure device 100 for viewing by the user. The user may then key in the authentication code 350 [orange box] as well as other required information (such as, company ID 310, user ID 320 and password 330) [yellow boxes] to obtain further access to the website. Since the website initially provides the image or video 340 [red box], the website also has knowledge regarding the correct authentication code 350 corresponding to the information embedded in the image or video 340. [Ex. 1001, 6:55-7:14, emphasis added]

40. Focusing on the “embedded information stored in the scanned image or video 340,” the illustration below (created by Patent Owner) demonstrates that the “embedded” information (which is used to derive the authentication code 350 in the

purple box) is hidden in the image of the QR code (red box) displayed on the webpage:



41. Referring to the diagram above, when image 340 (red box) is scanned using a conventional QR scanner (left side), the scanner interprets the unhidden aspects of the QR Code image as the word “hello.” However, hidden (or embedded) in the image is information corresponding to secret authentication code 350 (purple box) which is depicted as the alphanumeric string “B87394,” and which was not detected by the conventional QR scanner. Rather, only the secure device (which has knowledge of “the encryption or decryption algorithm used to create the information embedded in the image or video 340” [Ex. 1001, 6:10-12, 7:3-5]) is able to derive the authentication code from information embedded in the image. As explained in

the '167 Patent, the process of deriving the authentication code and other relevant information based on the embedded information from the image, is performed using such “encryption or decryption algorithm” [Ex. 1001, 6:60-7:5].

42. In contrast to the embodiment of Figure 3 where information is embedded in the image (using an encryption, decryption, or message authentication code), if the information in the image was limited to a standard UPC barcode which could be decoded using a public standard (like UPC) into digits (like the way a UPC barcode is used at every grocery store), the system would lack the capability to provide secure authentication for a transaction, since the authentication code could be derived from the image using only publicly available information.

43. Notably, the predetermined information in the embodiment of Figure 3 is not the private key used to derive the embedded information from the image. Instead, “predetermined information” in the embodiment of Figure 3 is one subset of “other types of information” stored in the secure device and “identification information¹ provided by the user” is another separate type of information that is distinct from “predetermined information” [Ex. 1001, 6:60-66] (“The secure device 100 then derives the authentication code 350 and other relevant information 360

¹ The '167 Patent explains that “identification information” may include “a personal identification number (PIN), a password and/or biometric information” and is “provided by the user to verify or authenticate the user’s identity” [Ex. 1001, 6:1-7 and 6:22-23].

based on the embedded information stored in the scanned image or video 340 and, optionally, other types of information including, for example, predetermined information stored in the secure device 100 and identification information provided by a user"). As was the case in the general embodiment of Figure 2 where the predetermined information was not the private key but rather "other information" such as "address information, personal profile information and payment account information" [Ex. 1001, 6:15-22], in the embodiment of Figure 3 the predetermined information is again distinguished from the private key and characterized as falling within "other types of information" such as "identification information provided by the user" [Ex. 1001, 6:63-66].

3. Embodiment For Secure Access To Physical Structures

44. After describing the scanning and extraction of embedded information from an image in connection with Figure 3, the '167 Patent explains that "[t]he secure device 100 may also be used to identify or authenticate persons for physical access to structures and/or vehicles through entry points, such as, doors and gates" [Ex. 1001, 7:24-26]. In this embodiment, after the secure device scans the image with the embedded information, "the output of the secure device 100 is transmitted in the form of a radio or sonic signal, [to] a station (e.g., a merchant, seller, vendor, third part service provider, guard)" [Ex. 1001, 7:26-29]. The recipient of "the transmitted signal may deem the user identified if the signal corresponds to an

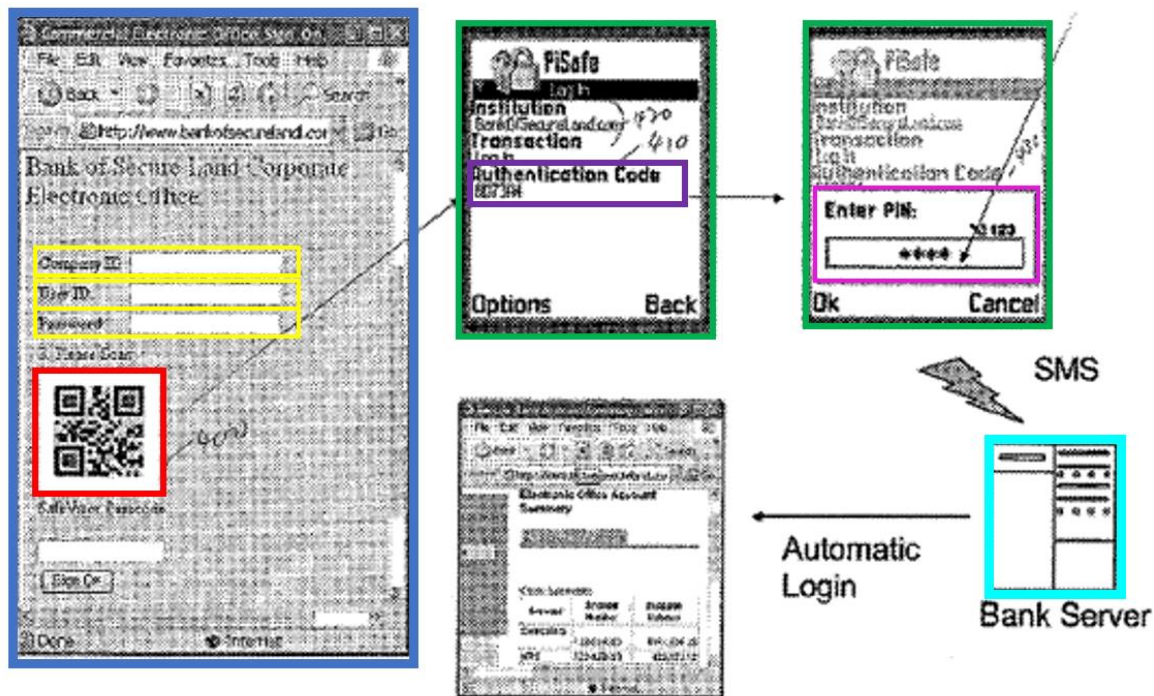
expected value at the station for a specific user and secure device 100.” [Ex. 1001, 7:29-37]. “The output from the secure device 100 received at a station may be compared to all the registered users and devices to identify the user and the secure device 100 that would generate the expected output. With suitable selection of the encryption protocols, the output can be rendered deterministically or probabilistically unique for each user and device combination” [Ex. 1001, 7:42-48, emphasis added]. “[T]he image or video captured by the secure device 100 may include a unique number, nonce, a transaction number or a random number, a number that the secure device 100 will use to derive the authentication code” [Ex. 1001, 7:55-59].

45. Like the general embodiment of Figure 2, the embodiment for securing access to physical structures described in the '167 Patent uses embedded (hidden) information (including, *e.g.*, a unique number, nonce, a transaction number or a random number) in an image [Ex. 1001, 7:56-58 and 8:8-9].

4. Alternate Authentication Embodiment – Figure 4

46. Figure 4 depicts an embodiment where the secure portable device "is used to effect authentication in an alternative manner." Ex. 1001, 8:38-40. Figure 4 is reproduced below, where the colored boxes have been added by Patent Owner. The blue box on the left identifies the log-on screen of a web site (*e.g.*, the website of a bank) requiring user authentication, while the green boxes depict the display of

the portable secure device.



[Ex. 1001, Figure 4, color added]

47. As was the case with the authentication embodiment of Figure 3, in the embodiment of Figure 4, the user “[s]imilarly ... uses the secure device 100 to derive the authentication code 410 [purple box] and other relevant information 420 from the scanned image or video 400 [red box]” [Ex. 1001, 8:40-42]. “The secure device 100 then further prompts the user to enter his/her personal identification number (PIN) 430 and/or other identification information [pink box]” [Ex. 1001, 8:42-44]. A message is then transmitted (via, *e.g.*, SMS) to server 440 (turquoise box) including the “identity of the user and secure device 100, a unique value generated

by the secure device 100, and a unique number, nonce, a transaction number or a random number embedded in the image” [Ex. 1001, 8:45-55]. “The server 440, by using the unique number, the nonce, the transaction number or the random number transmitted with the message, may identify the session that the user is using to authenticate his or her identity and may then deem the session as authenticated, thereby allowing the user to conduct any desired transactions on the website.” [Ex. 1001, 8:62-67].

48. The embodiment of Figure 4 follows the embodiment of Figure 3, where the mechanism for deriving the embedded information in the image was either "an encryption, a decryption or a message authentication algorithm." Id., 6:66-7:1. Given that, in the embodiment of Figure 4, the user “[s]imilarly ... uses the secure device 100 to derive the authentication code 410 ... from the scanned image or video 400” [Ex. 1001, 8:40-42], it is clear that in the embodiment of Figure 4 the process of deriving the embedded information from the image is “similarly” performed using an “encryption, a decryption or a message authentication algorithm.”

49. Also like the embodiment of Figure 3, when image 400 (red box) is scanned using a conventional QR scanner, the scanner interprets the unhidden aspects of the QR Code image as the word “hello.” However, hidden (or embedded) in the image is information corresponding to secret authentication code 410 (purple box) which is depicted as the alphanumeric string “B87394,” and which would not

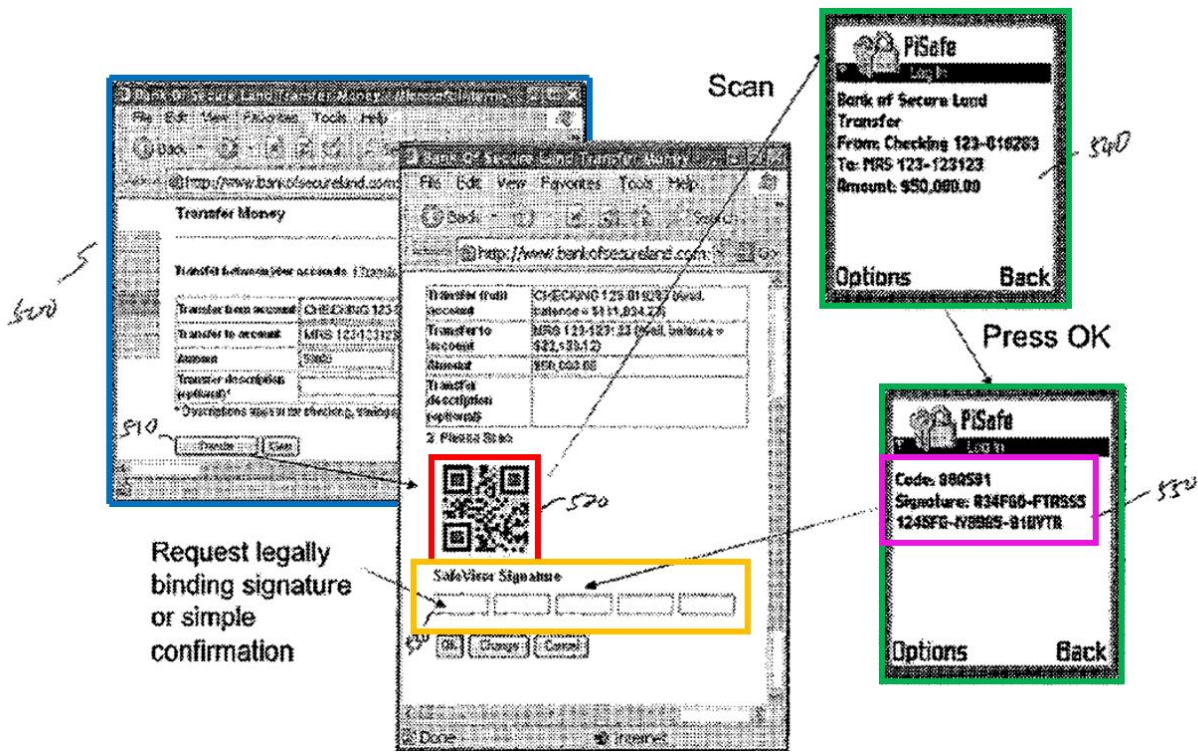
be detected by a conventional QR scanner. Rather, only the secure device (which “has knowledge of the encryption algorithm used to create the information embedded in the image or video”), is able to derive the authentication code from the image [Ex. 1001, 6:10-14].

50. In contrast to the embodiment of Figure 4, if the information in the image was limited to a standard UPC barcode which could be decoded using a public standard (like UPC) into digits (like a UPC code), the image itself would not add to the security of the system since all of the information in the image would be publicly available information. To the extent that the image was limited to publicly available information and the only other security for the transaction was a PIN, the system would be no more secure than the prior art system that relied on static information that was disparaged in the Background of the ’167 Patent [Ex. 1001, 1:37-38].

5. Authorization Embodiment – Figure 5

51. Figure 5 depicts an embodiment where the secure portable device “is used to effect authorization” (as distinguished from authentication) [Ex. 1001, 9:3-4, emphasis added]. In this embodiment, the user may be authenticated for permission to enter a website using the secure device “as described above or through other mechanisms,” or no prior authentication may have taken place [Ex., 9:5-8]. “After the user successfully logs into the website, terminal, server or device, the user may perform a desired transaction, such as, transferring money between accounts.

Such desired transaction may need to be further authorized to provide additional security.” [Ex., 9:11-13]. Figure 5 (reproduced below with colored boxes added by Patent Owner) depicts this authorization process which, as described below, is required to complete the transaction.



[Ex. 1001, Figure 5, color added]

52. In the embodiment of Figure 5, the user completes a form 500 [blue box] to effect transfer of money between accounts. “Upon hitting the ‘transfer’ button 510, the website, terminal, server or device displays an image or stream of images 520 [red box] and a blank designated entry 530 [orange box] for a confirmation signature. The image or stream of images 520 [red box] include

embedded information relating to the transfer transaction and possibly a unique transaction number” [Ex. 1001, 9:18-20, emphasis added]. The ’167 Patent explains this embodiment in further detail as follows:

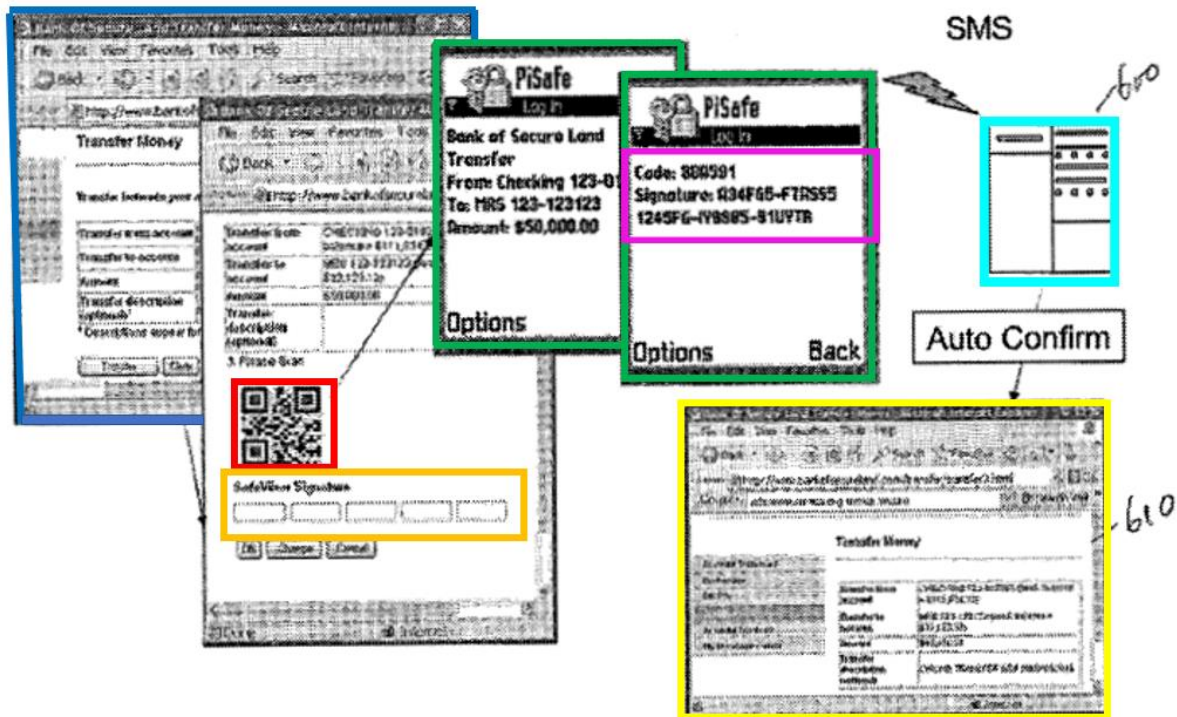
... the user may use the secure device 100 to scan the image or stream of images 520. The secure device 100 may then decode the scanned image or stream of images 520 and derive the embedded information. The derived information relating to the transfer transaction may then be shown on a display 540 [green box] ... The user may optionally be asked to enter his or her personal identification number for authentication. Upon completion of the authentication process, the secure device 100 may generate the corresponding confirmation signature 550 [pink box]. The confirmation signature may be a digital signature generated based on embedded information contained in the image or stream of images 520 and, optionally, other types of information ... The user may then input the generated confirmation signature or authorization code into the designated entry 530 [orange box]. The website, terminal, server or device may then check the generated confirmation signature or authorization code relative to the information embedded in the image or stream of images 520. If the generated confirmation signature is correct for a specific user and/or secure device 100, the transfer transaction will be completed. [Ex. 1001, 9:27-54, emphasis added]

53. The statement that the secure device may “then decode the scanned image or stream of images 520 and derive the embedded information,” makes clear that there are two distinct steps in the process of retrieving the “embedded” information: the first step is decoding the scanned image and the second step is deriving the embedded information. Had the patent stated that the secure device may

“then decode the scanned image or stream of images 520 [to] derive the embedded information” (which is clearly does not), it would have indicated that this was a one step process. Thus, the disclosed invention is distinct from a UPC barcode that is simply decoded in a single step rather than being processed using “decoding” followed by “deriving.”

6. Alternate Authorization Embodiment – Figure 6

54. In a “similar illustrative application, the secure device 100 can be used to effect authorization in an alternative manner, as shown in FIG. 6. The authorization process is similar to that described in connection with FIG. 5 above” [Ex. 1001, 9:59-62]. Figure 6 (reproduced below with colored boxes added by Patent Owner) depicts this alternative authorization process:



[Ex. 1001, Figure 6, color added]

55. The '167 Patent describes the embodiment associated with Figure 6 as follows:

[U]pon the secure device 100 generating the confirmation signature or authorization code [in a manner similar to that described in connection with Figure 5], the secure device 100 may transmit the generated confirmation signature or authorization code to a transaction server 600 [turquoise box] handling the transaction. The generated confirmation signature or authorization code may be transmitted in the form of a message in a number of ways including, for example, a wide area network (such as, a cellular or wireless network), email, SMS and EMS. The message may also include the unique transaction number embedded in the image or stream of images. In response, upon receiving the generated confirmation signature or

authorization code, the transaction server 600 may then use the transaction number to identify the session and check the generated confirmation signature or authorization code relative to the information embedded in the image or stream of images and, if appropriate, effect the transaction and display the confirmation information 610 to the user. [Ex. 1001, 9:63-10:13, emphasis added].

56. Like the embodiment of Figure 5, it is clear that the information used for secure authorization in the image in Figure 6 is embedded (hidden) in the image.

7. Embodiment With Authorization Involving Multiple Parties

57. The '167 Patent also includes an embodiment where authorization "involving multiple parties" is achieved [Ex. 1001, 10:14-16]. Consistent with the previously described embodiments, "the authorization can be achieved by embedding values derived from the transaction with secret information shared by the user of the secure device 100 and the other parties. The secrets shared by the user of the secure device 100 and the other parties can be credit card numbers, the expiration date of the card, the registered address of the user, and a password established by the user. The other parties can be merchants, banks, credit card issuers, and service providers that may need to be involved with the transaction." [Ex., 10:16-24, emphasis added].

8. Authorization With Offline Digital Signature – Figure 7

58. Figure 7 depicts an embodiment where "the secure device 100 can be used to provide offline digital signature to effect authorization." [Ex. 1001, 10:29-

30]. In this embodiment:

A sender seeking authorization for a transaction forwards a printed form 700 to a user. The printed form 700 includes certain transaction information as well as an image 710, such as a barcode, or a set of images, such as a set of barcodes. The image 710 includes embedded information relating to the transaction. The user using the secure device 100 scans the image 710. ... [T]he secure device 100 decodes the scanned image 710 and derives the embedded transaction information. ... The user may then provide approval of the transaction by entering the corresponding command into the secure device 100. The secure device 100 may then generate the corresponding confirmation signature or authorization code 740 based on the information embedded in the image 710 and ... display the generated confirmation signature or authorization code 740 to the user. In response, the user may then provide the generated confirmation signature or authorization code 740 to the sender to confirm authorization via, for example, a telephone, a wide area network (such as, cellular or wireless network), an email, SMS message, EMS message or facsimile 750. Since the sender initially provides the image 710, the sender also has knowledge with respect to the corresponding confirmation signature or authorization code. As a result, by receiving the generated confirmation signature or authorization code 740 from the user, the sender may verify whether the user is authorized to provide approval for the transaction. [Ex. 1001, 10:31-62].

59. Again, it is clear that the information used to secure the transaction is embedded (hidden) information in the image [Ex. 1001, 10:46-49].

9. Secure Document Distribution - Figure 8

60. In the embodiment of Figure 8, the secure device 100 is “used to provide secure document distribution” [Ex. 1001, 10:63-64]. Here, “a document is

created and secured using a password” Ex. 1001, 10:67-11:1]. Next, a message, such as an email or SMS is created for a recipient with the secured document being included as an attachment. An image is created that “includes embedded information relating to the password used to secure the document. The information embedded in the image or stream of images can be created using public keys that are stored locally or centrally managed” [Ex. 1001, 11:8-9, emphasis added]. The image is also included along with the secure document as part of the message, which is delivered to the recipient [Ex. 1001, 11:25-28]. Upon opening the message, the recipient uses the secure device 100 to scan the image and “derive the embedded information” from the image which is then displayed to the user [Ex. 1001, 11:28-35]. The user then uses the displayed information to access the secured document [Ex. 1001, 11:35-36].

61. Again, it is clear that the information used to secure the document is embedded (hidden) in the image [Ex. 1001, 11:30-34].

10. Digital Rights Management

62. In another embodiment, “the secure device 100 can be used to effect digital rights management” [Ex. 1001, 11:49-50]. In this embodiment, a document “may contain an access control list to limit the users to certain operations. For example, only certain users might be allowed to open, modify, change, copy and/or print the information embedded in a document” [Ex. 1001, 11:50-54]. “When a user tries to open, modify, change, print and/or copy the document,” the program

generates a challenge embedded in an image [Ex. 1001, 11:58-62]. In response, the user scans the image and the secure device uses a private key to generate an authentication code in response to the challenge [Ex. 1001, 11:63-12:1]. “The user may then provide the authentication code by entering it manually on a terminal. ... The program upon receiving the authentication code confirms the identity of the user by comparing the response received. If the identity of the user is confirmed and the operation that the user is trying to accomplish is allowed, the program performs the operation” [Ex. 1001, 12:1-11].

63. Again, in the digital rights management embodiment, it is clear that the information used to effect digital rights management is embedded (hidden) information in the image [Ex. 1001, 11:60-63].

11. Conducting Transactions

64. In this embodiment, an image (or stream of images) can be generated. “The secure device 100 upon deciphering² the image or stream of images can send a confirmation to the third party service provider through, for example, a wide area network (such as, a cellular or wireless network). The third party service provider can then cooperate with the server associated with the merchant to complete the transaction” [Ex. 1001, 13:5-13:10, emphasis added]. “In the situation where there

² In the context of the '167 Patent, the term deciphering would have been understood to require decryption or another process performed by the secure device that was the opposite of enciphering.

is no communication channel between the secure device 100 and the third party service provider or the merchant, the secure device 100 and the third party service provider or merchant can utilize a shared secret key and identification information assigned to the secure device 100 or to the user of the secure device 100. The shared secret key and the identification information are previously provided to the secure device 100 and the service provider. The secure device 100 can capture the image or stream of images and decode its embedded information. The secure device 100 can then combine the decoded information and the identification information and encode the combination using the shared secret key. The encoded value, including a portion of the identification information, can be displayed on the secure device 100. The user may then provide the encoded value to the terminal, device, or website or may call the merchant or third party service provider to provide the encoded information” [Ex. 1001, 13:16-33, emphasis added].

65. Again, it is clear that the information used to secure the transaction is embedded (hidden) in the image [Ex. 1001, 13:24-25].

12. Checkout Process - Figures 10 and 11

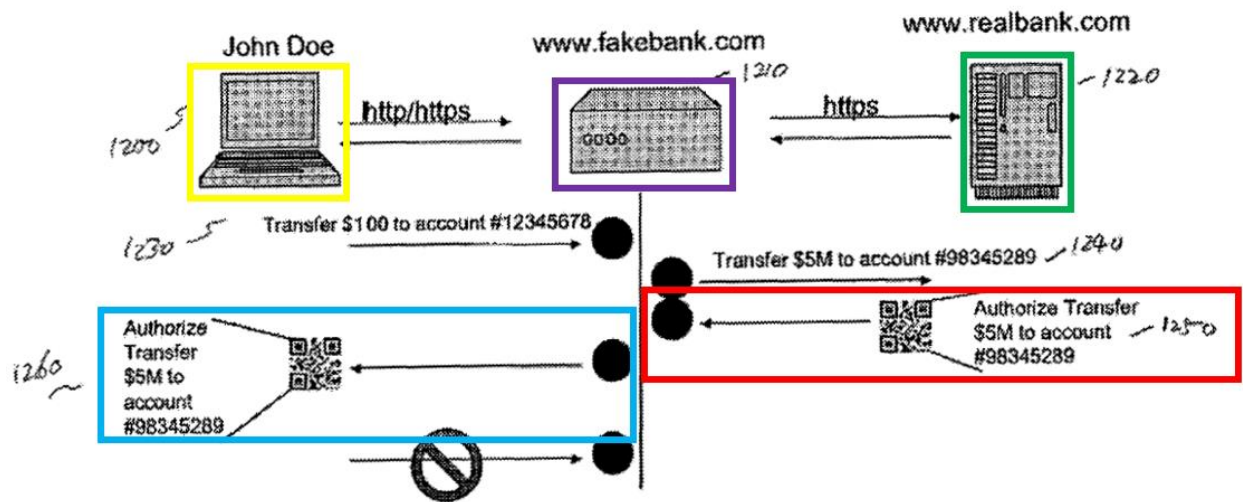
66. In further embodiments, “the secure device 100 can be used in a checkout process” [Ex. 1001, 13:40-41]. “[U]pon checkout, a register generates an image or a stream of images for a transaction. The image or stream of images includes embedded information relating to the transaction. The image or stream of

images is presented to the user. The user then uses the secure device 100 to scan the image or stream of images. The secure device 100 then derives the relevant information relating to the transaction from the barcode and displays such information to the user ... The user may then authorize the transaction. The secure device 100 may further require the user to provide a PIN, as shown in block 1020, to ensure that the user is indeed authorized to approve the transaction” [Ex. 1001, 13:42-53, emphasis added]. The check-out embodiment of Figure 11 is described similarly [Ex. 1001, 14:6-23].

67. In this embodiment, the merchant is verified using information embedded (hidden) in the image. Moreover, it would be inconsistent with the specification as a whole to read the embodiments of Figures 10 and 11 as a system that relied only on a PIN for security, given that such systems were disparaged earlier in the specification [Ex. 1001, 1:37-38].

13. Defending Against Phishing Attacks - Figure 12

68. “In yet another illustrative application, the secure device 100 can be used to defend against real-time phishing attacks, as shown in FIG. 12” [Ex. 1001, 14:42-44]. Figure 12 (reproduced below with colored boxes added by Patent Owner) depicts this embodiment:



[Ex. 1001, Figure 12, color added]

69. As described in the specification, “Phishing attacks involve fraudulently capturing information from a user, for example, via a fake website, and then using such information to conduct unauthorized transactions.” [Ex. 1001, 14:44-47]. In a phishing attack, a user [yellow box] unknowingly provides information to a fake website [purple box] while attempting to transfer money to account #12345678, thinking that they are dealing with the legitimate website [green box]. Upon capturing the information, the fake website [yellow box] modifies the account number in the instructions to account #98345289 and contacts the legitimate website [green box] attempting to conduct an unauthorized transaction where money is transferred to the fake website's account #98345289 (as opposed to account #12345678 designated by the user [yellow box]). To confirm the transaction, the legitimate website [green box] generates an image [red box] that requires

confirmation by the secure device 100. The fake website then forwards the image to the secure device 100 [blue box]. However, the fake website lacks the capability of deriving the embedded information from the image necessary to provide the confirmation because, *e.g.*, the information is encrypted. Instead, “the secure device 100 may then derive the confirmation information and display such information to the user, thereby allowing the user to detect that an unauthorized transaction has been attempted” [Ex. 1001, 14:58-62] In the example, the information displayed on the secure device of the user indicates that the unconfirmed transaction seeks to transfer money to account #98345289 (as opposed to account #12345678 designated by the user). “The user may then terminate any connection to the fake website” [Ex. 1001, 14:62-63].

70. Again, it is clear that the defense against the phishing attack is based on information that is embedded (hidden) in the image. If the information in the image necessary to authorize the transaction could be derived using public information, the fake website would derive the information itself (rather than forwarding the image with the embedded information to the user as shown in Figure 12) and the phishing defense would be completely ineffective.

14. Every Embodiment of the '167 Patent Relies on Embedded Information for Security

71. In every embodiment of the '167 Patent, the embedded information

corresponds to information that is protected at least in part by being hidden in the image. As explained above, if the information necessary to effect a secure transaction in the embodiments of the '167 Patent could be derived from the image using public information, the disclosed embodiments would not be directed “to methods and devices for providing secure identification, verification and authorization using a portable secure device,” as recited at the very beginning of the '167 Patent [Ex. 1001, 1:10-11, emphasis added].

IX. Claims of the '167 Patent

72. Claim 1 of the '167 Patent recites as follows (emphasis added):

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.

73. Independent claim 1 recites “the image having information embedded therein.” As discussed above in relation to the specification of the ’167 Patent, in every embodiment disclosed in the specification, such embedded information corresponds to information that is hidden in the image. All other independent claims in the ’167 Patent identically recite: “the image having information embedded therein.”

74. Independent claim 1 also recites “memory configured to store predetermined information.” The ’167 Patent explains that the predetermined information is not a key, but rather other information: “if the image is created using a public key, the corresponding private key (as well as other information, such as, predetermined information stored in the memory 150 and the input information provided by the user) may be used to decrypt or decode the captured image” [Ex. 1001, 6:15-19]. The ’167 Patent further explains that “predetermined information may include, for example, address information, personal profile information and payment account information” [Ex. 6:19-22]. The ’167 Patent also explains that

predetermined information is not “identification information³ provided by the user.” Rather, “identification information” is described another separate type of information that is distinct from predetermined information. [Ex. 1001, 6:60-66] (“The secure device 100 then derives the authentication code 350 and other relevant information 360 based on the embedded information stored in the scanned image or video 340 and, optionally, other types of information including, for example, predetermined information stored in the secure device 100 and identification information provided by a user”). All other independent claims in the ’167 Patent identically recite storage of such “predetermined information.”

75. Independent claim 1 also recites that an output is generated “based on the information embedded in the image and the predetermined information.” Thus, the information embedded in the image is used in combination with the predetermined information (other than a key), to generate an output, *e.g.*, an authentication code. *See, e.g.*, Ex. 1001, 3:25-28; 6:60-66. All other independent claims in the ’167 Patent identically recite generation of an output “based on the information embedded in the image and the predetermined information.”

76. Finally, independent claim 1 recites that “the output includes a digital

³ The ’167 Patent explains that “identification information” constitutes information such as “a personal identification number (PIN), a password and/or biometric information” and is “provided by the user to verify or authenticate the user’s identity” [Ex. 1001, 6:1-7 and 6:22-23].

signature to be used to signify authorization by the user with respect to the transaction.” This limitation corresponds, for example, to the digitally signed confirmation signature in the embodiments of Figures 5 and 6 as discussed in relation to the specification of the ’167 Patent above, where the confirmation signature is necessary for the transaction to be effected [Ex. 1001, 9:52-54] (“If the generated confirmation signature is correct for a specific user and/or secure device 100, the transfer transaction will be completed”) and [Ex. 1001, 9:63-10:13] (“[U]pon receiving the generated confirmation signature or authorization code, the transaction server 600 may then use the transaction number to identify the session and check the generated confirmation signature or authorization code ... and, if appropriate, effect the transaction”). Like claim 1, independent claim 23 similarly requires that “the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.”

X. Claim Construction

A. “Image capture device” and “capture an image” (all claims)

77. The Petition proposes to construe the term “image capture device” as it is used in the ’167 Patent and cites the specification to argue 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. Ex. 1001 at 5:8-11, 5:21-29. The patent also indicates that the image may be a barcode. *Id.*” [Pet., p.

15]. However, the patent says much more about the image capture device (or circuit) than the Petition considers in its construction:

The image capture circuit **120** may include a digital camera or other types of image capturing devices. The image capture circuit **120** is used to capture image and/or video information. The captured image and/or video information may include a barcode including a one-dimensional barcode, such as a linear barcode, or a multi-dimensional barcode, such as a 2D barcode, multiple barcodes in a single image or multiple barcodes in multiple images where multiple images form a stream of images or a video. [Ex. 1001, 5:21-29, emphasis in original].

78. The Petition concludes that the term “image capture device” should be construed as “any device that could capture an image, such as a barcode scanner” [Pet., p. 15]. The problem with this construction is that many barcode scanners are only capable of decoding the information in one-dimensional barcodes and cannot capture an image at all.

79. Linear barcode scanners cannot capture an image or read two-dimensional barcodes: “Matrix codes are a two-dimensional pattern of data cells in the shape of a square, circle, or polygon. Unlike linear and stacked barcodes, matrix codes must be read with an image-based reader. They cannot be decoded by a laser scanner” [Ex. 2011, p. 1]. Furthermore, most barcode scanners produced at the time of the patent lacked circuitry to produce an image. An image is “a visual representation of something: such as (1) a likeness of an object produced on a

photographic material (2) a picture produced on an electronic display (such as a television or computer screen)” [Ex. 2012, Merriam Webster] or in the case of the ’167 Patent, data that could be used to produce a picture on an electronic display. Therefore in the context of the ’167 Patent, to “capture an image” is to “collect data that encodes a visual representation of something and that could be used to produce a likeness of the object.” Decoded barcode data is merely the characters or numbers encoded in the barcode, and not a visual representation of the barcode. Furthermore, (as discussed in relation to the construction of “the image having information embedded therein” below) merely decoding barcode data would be insufficient to recover information embedded in an image where the body of the image depicts a barcode and the embedded information is hidden in the image. Absent specific information identifying the type of barcode scanner, it would be impossible to know whether a barcode scanner could capture an image. Therefore, the Petition’s conclusion that any barcode scanner could capture an image is incorrect.

80. The Petition’s assertion that any barcode scanner is capable of capturing an image is plainly false. And given the explanation in the specification that the image capture device (or circuit) in the ’167 Patent could capture linear barcodes, two-dimensional barcodes, multiple barcodes in a single image, or multiple barcodes in a video, the correct construction of the term “image capture device” as it is used in the ’167 Patent is “a device that can capture an image or

video, such as a still-image camera or video camera.”

B. "The image having information embedded therein" (all claims)

81. In the context of the '167 Patent, information “embedded” in an image refers to information that is hidden in the image and used to provide security for the transaction. This is the correct construction for at least three reasons.

82. First, as discussed in detail in relation to the specification of the '167 Patent above, in every embodiment disclosed in the specification, the information embedded in an image corresponds to information that is hidden in the image and used to provide security for the transaction. Thus, Patent Owner’s construction aligns with the specification.

83. Second, each independent claim recites that it is an apparatus or method “for providing a secure transaction.”⁴ This claim language is in keeping with the first sentence of the '167 Patent which states:

The present invention relates generally to secure transactions, and more specifically, to methods and devices for providing secure identification, verification and authorization using a portable secure device. [Ex. 1001, 1:8-11, emphasis added]

84. Thus, both the claim language and specification demonstrate that the claims are limited to techniques for providing a secure transaction. Patent Owner's

⁴ Claims 1 and 19 recite: “An apparatus for providing a secure transaction ...”; and claims 23, 39 and 43 recite: “A method of providing a secure transaction”

construction stays true to the claim language and specification by clarifying that the information “embedded” in an image refers to information that provides security for the transaction.

85. Third, the ’167 Patent is directed to the field of secure transactions⁵ and, in that field, “embedding” data or information in an image is a term of art that refers to hiding the data or information in the image. As one author writing before the filing date of the ’167 Patent stated:

Data embedding in images is an application that hides secret messages in digital images. The message may be any type of bit stream data, such as text, image, voice, etc.
...

Many techniques about *data embedding in images* have been proposed. Some of the techniques are based on modifying the least significant bits (LSBs) of the pixels of the cover image (Turner, 1989, Walton, 1995). Bender et al. (1997) proposed a patchwork method for embedding information by adding or subtracting a value to or from the gray values of pixels. The texture block coding method (Bender et al., 1996) and the fractal-based steganography method (Davern and Scott, 1996) embed information by modifying small regions of images. Image hiding can also be applied in frequency or other transform domains, such as the method which uses randomly sequenced pulse position modulated codes (Koch and Zhao, 1995), the wavelet-based embedding methods (Ohnishi and Matsui, 1996, Chae and Manjunath, 1998), the secure spread

⁵ Under the heading “Field,” the ’167 Patent provides: “The present invention relates generally to secure transactions, and more specifically, to methods and devices for providing secure identification, verification and authorization using a portable secure device” [Ex. 1001, 1:7-11, emphasis added].

spectrum method (Cox et al., 1997), and the DCT-based embedding methods (Hsu and Wu, 1998, Barni et al., 1998). Recently, a number of methods exploit the human visual system (HVS) to guarantee that the modification made to the cover image is imperceptible. These methods are based on spatial or frequency masking (Girod, 1989, Legge and Foley, 1990).⁶

86. Another author writing prior to the filing date of the '167 Patent similarly used “data embedding” in images synonymously with data hiding:

... A novel lossless (reversible) data embedding (hiding) technique is presented. The technique provides high-embedding capacities, allows complete recovery of the original host signal, and introduces only a small distortion between the host and image bearing the embedded data.⁷

87. A further author writing prior to the filing date of the '167 Patent described “data embedding” in images as either a stenographic process or watermarking process, each of which secure data by hiding it in the image:

Data embedding applications could be divided into two groups ... The first group is formed by steganographic applications in which the message has no relationship to the cover image and the cover image plays the role of a decoy to mask the very presence of communication. ... The second group of applications is frequently addressed as digital watermarking. In a typical watermarking application, the message has a close relationship to the cover image. The message supplies additional information

⁶ “*Embedding Of Any Type Of Data In Images Based On A Human Visual Model And Multiple-Based Number Conversion*,” Da-Chun Wu and Wen-Hsiang Tsai, Pattern Recognition Letter, Volume 20, Issue 14, December 1999, Pages 1511-1517 (emphasis added).

⁷ “*Lossless Generalized-LSB Data Embedding*,” Celik, Mehmet Utku, et al., *IEEE transactions on image processing* 14.2 (2005): 253-266 (emphasis added).

about the image, such as ... author signature, image authentication code, etc. (emphasis added).

* * *

The embedding technique starts with extracting the subset *B* and continues with losslessly compressing it. The compressed bitstream is concatenated with a secret message (payload) and inserted into object *X* in place of subset *B*. ... The extraction of the hidden message proceeds by extracting the subset *B* and reading the concatenated bit stream consisting of the compressed bitstream and the message.⁸

88. Yet another author writing at the time also referred to “data embedding” in images as synonymous with stenography or watermarking:

The technology associated with adding watermarks is called steganography, (digital) watermarking, data embedding, or fingerprinting. In this paper, the act of adding watermark is called embedding, and retrieving the information encoded in the watermark for perusal is called extraction.⁹

89. Artisans in the field at the time of the '167 Patent similarly described data embedding in the context of barcode images:

This paper presents a novel approach for embedding uncompressed images in a standard PDF417 2D barcode using a blind digital watermarking technique. ... This paper proposes a novel approach to embed uncompressed

⁸ “Lossless Data Embedding For All Image Formats,” Fridrich, Jessica, Miroslav Goljan, and Rui Du. In *Security and watermarking of multimedia contents IV* (Vol. 4675, pp. 572-583). SPIE, 2002 (emphasis added).

⁹ *Embedding Data in 3D Models*, R. Ohbuchi *et al.*, IBM Japan Tokyo Research Laboratory, Interactive Distributed Multimedia Systems and Telecommunication Services: 4th International Workshop, IDMS'97 Darmstadt, Germany, September 10–12, 1997 Proceedings 4, Springer Berlin Heidelberg, 1997 (emphasis added).

face and fingerprint images without affecting the maximum text capacity of the PDF417 barcode. ... The face and fingerprint images are used as watermarks and embedded into the dark regions of a barcode image.¹⁰

90. The fact that data or information “embedding” was a term of art at the time is underscored by the fact that papers at the time used the term “embedding” as “keywords” for indexing purposes. *See, e.g.*, Ex. 2004, p. 1057 ("Index Terms—Arithmetic coding, conditional entropy coding, context modeling, data embedding, data hiding, least significant bit (LSB) modification, watermark"); Ex. 2008, p. 696 ("Index Terms—Data hiding, digital watermarking, multilevel embedding, video data hiding.").

91. In summary, in the context of the '167 Patent, information “embedded” in an image refers to information in the image that is hidden in the image and used to provide security for the transaction. This is the correct construction because it: (i) aligns with every embodiment in the specification, (ii) is true to both the claim language and specification which are directed to secure transactions, and (iii) recognizes that “embedding” data or information in images was a term of art at the time of the '167 Patent used to describe hiding data or information in the image.

¹⁰ *Embedding Biometric Identifiers In 2D Barcodes For Improved Security*, Noore, Afzel, Nikhil Tungala, and Max M. Houck. *Computers & Security* 23.8 (2004): 679-686 [Ex. 2007, p. 3, emphasis added].

C. “Predetermined information” (all claims)

92. The '167 Patent made clear that “predetermined information” is information “other than” either a private key or identification information provided by the user to verify or authenticate the user's identity. In distinguishing “predetermined information” from a private key, the '167 Patent stated:

... The decryption algorithm may use one or more input parameters for decoding. For example, if the image is created using a public key, the corresponding private key (as well as other information, such as, predetermined information stored in the memory 150 and the input information provided by the user) may be used to decrypt or decode the captured image. The predetermined information may include, for example, address information, personal profile information and payment account information. [Ex. 1001, 6:8-22, emphasis added].

93. Here, the '167 Patent clearly distinguishes a “private key” from “other information,” such as “predetermined information” which may include “address information, personal profile information and payment account information.”

94. The '167 Patent also distinguished “predetermined information” from “identification information” which the patent describes as a “personal identification number (PIN), a password, and/or biometric information” used to “verify or authenticate the user's identity” [Ex. 1001, 6:1-7 and 6:22-23]. In this regard, the '167 Patent stated:

The user activates the secure device 100 and uses the secure device 100 to scan the image or video 340. As part of the activation process, the user may need to enter a

password or other types of identification information into the secure device 100 to ensure that the user is authorized to use the secure device 100. The secure device 100 then derives the authentication code 350 and other relevant information 360 based on the embedded information stored in the scanned image or video 340 and, optionally, other types of information including, for example, predetermined information stored in the secure device 100 and identification information provided by the user. [Ex. 1001, 6:55-66, emphasis added]

95. In referencing “predetermined information” and “identification information provided by a user,” the ’167 Patent refers to both together as “other types” (plural) of information, which makes clear that “predetermined information” is a separate and distinct type of information than “identification information.”

96. A person of ordinary skill in the art would understand from the specification that the predetermined information is not a private key or identification information used to verify or authenticate the user, but rather “other information, such as, ... address information, personal profile information and payment account information.”

D. “A digital signature to be used to signify authorization by the user with respect to the transaction” (claims 1 and 23)

97. Independent claims 1 and 23 recite that “the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.” The claim language includes a temporal component that characterizes the digital signature as something “to be used” to signify that the transaction is

authorized. As explained in the specification, the digital signature to be used to signify authorization of the transaction is a prerequisite to completion of the transaction, *i.e.*, the confirmation signature is necessary for the transaction to be effected [Ex. 1001, 9:52-54 (“If the generated confirmation signature is correct for a specific user and/or secure device 100, the transfer transaction will be completed”) and 9:63-10:13 (“[U]pon receiving the generated confirmation signature or authorization code, the transaction server 600 may then use the transaction number to identify the session and check the generated confirmation signature or authorization code ... and, if appropriate, effect the transaction”). Accordingly, a person of ordinary skill in the art reading the claims in light of the specification would understand that “a digital signature to be used to signify authorization by the user with respect to the transaction” is a digital signature that is necessary to effect (or complete) the transaction.

XI. Overview of the Alleged Prior Art

98. With respect to the independent claims of the '167 Patent, the Petition relies on four references, namely, Wang, Take An Order (TAO), Drummond and the Palm Treo Manual (PTM). The pertinent features each of these references are discussed below.

A. U.S. Patent Publ. 2002/0023215 (Wang)

99. Wang discloses “a portable electronic authorization device (PEAD)

carried by a user” [Ex. 1004, Abstract]. Like the ’167 Patent, Wang refers to “identification data” as the data used to authenticate the user:

To enhance security to the user's account, electronic transaction systems typically request the user to provide identification data to authenticate him as the user authorized to approve the proposed transaction or transactions. If the user fails to provide the requested identification data, the proposed transaction or transactions are not authorized and will not be processed. [Ex. 1004, ¶0004, emphasis added]

100. In contrast to earlier devices, in Wang such "identification data" remains with the PEAD at all times. From Wang:

The present invention is different from the prior art technique of FIG. 1 in that the user is required in the prior art to enter his identification data into the electronic transaction system, e.g., into ATM 100, to authenticate himself. In contrast, the present invention keeps the identification data related to the user secure within PEAD 200 at all times. Ex. 1004, [0040].

101. In one embodiment (the one relied on in the Petition), the PEAD is used as a “self-checkout terminal” [Ex. 1004, ¶0115; Pet., pp. 33-34]. In this embodiment, the PEAD includes a barcode scanner for scanning UPC barcodes:

Another implementation of Point-of-Sale Transaction is to use PEAD as self checkout terminal. By entering the UPC code or barcode using keypad on the PEAD or scanning in the UPC code or barcode using the input device built into the PEAD such as a barcode scanner or OCR reader, the PEAD can generate the receipt with the list of item prices through the wireless network and Internet by querying the item price using the barcode as the index for price lookup table which is stored in a server system. The PEAD user

can sign the receipt electronically using PEAD [Ex. 1004, ¶0115, emphasis added]

102. Wang makes clear that transmission of “an approved transaction request to the server” (rather than a signed receipt) is required “to complete the transaction,” and “[t]he approved transaction request [rather than the signed receipt] signifies an approval of the transaction” [Ex. 1004, ¶0014].

B. Take An Order (TAO)

103. TAO describes point-of-sale software for the Palm devices whereby a vendor can take orders from customers at, for example, a trade show [Ex. 1005, p. 1]. Certain PalmOS devices compatible with the TAO software included a barcode scanner that the vendor could use to scan items to generate an order [Ex. 1005, p. 1]. The software includes a popup which lets the vendor key in the customer’s name, credit card number, and expiration date [Ex. 1005, p. 2]. The software includes the capability to print receipts, quotations, invoices, and delivery reports by connecting to a variety of printers [Ex. 1005, p. 3]. The reference does not disclose that the information stored in the barcodes is secured in any way.

C. U.S. Patent Publ. 2003/0217005 (Drummond)

104. The Petition relies on Drummond as disclosing that, in addition or alternatively to receiving paper receipts, electronic receipts may be sent to one or more devices via e-mail and/or text message [Pet., p.28, citing Ex. 1008, ¶¶0246-0251, 0301, and 0307].

D. Palm Treo Manual (PTM)

105. The Petition relies on the Palm Treo Manual (PTM) to show that Palm Treo devices included an internal memory, a processor, a keyboard and system locks that required a password to be entered on the device prior to accessing data stored on the device [Pet., p. 27, citing, Ex. 1006, pp. 24, 97, 109, 112, 129, and 173].

XII. The Alleged Prior Art Does not Disclose or Suggest the Claims of the '385 Patent

106. Petitioner asserts in six Grounds that the Challenged Claims are anticipated or obvious over the alleged prior art. This table summarizes Petitioner's assertions:

Ground	35 U.S.C.	Claims	Alleged Basis
I	§§ 102/103	1, 4, 5, 7, 12, 17, 23, 26, 27, 29, 34, 43	Anticipated by Wang and 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

107. In my opinion, the alleged prior art does not anticipate each and every limitation of the Challenged Claims. Even in combination, the differences between the Challenged Claims and the alleged prior art are such that the claimed subject matter as a whole would not have been obvious to a POSITA as of the priority date of the '167 Patent.

A. Ground I

108. The Petition makes two arguments in Ground I. First, that claims 1, 4, 5, 7, 12, 17, 23, 26, 27, 29, 34, and 43 are anticipated by Wang, and second that Elements 1g, 23g, and 43g are obvious over Wang in view of Drummond and that the remaining aspects of the claims challenged in Ground I are anticipated by Wang. However, Petitioner’s analysis of Wang is deficient, and the claims challenged in Ground I are not anticipated by Wang, as described in detail below.

1. **Petitioner has not shown that Wang anticipates capturing an image, the image having information embedded therein**

109. Elements 1a, 23b, and 43b of the claims challenged in Ground I all relate to image capture and to information embedded in the image (emphasis added):

Element 1a	Element 23b	Element 43b
an image capture device configured to capture an image, <u>the image having information embedded therein</u> including information relating to a transaction; [Ex. 1001, 16:24-26]	capture an image, <u>the image having information embedded therein</u> , the information embedded in the image including information relating to a transaction; [Ex. 1001, 17:51-54]	capture an image, <u>the image having information embedded therein</u> ; [Ex. 1001, 19:4-5]

110. Petitioner’s argument in relation to these claims rests entirely on two quotes from Wang. Petitioner’s citation to Wang is reproduced here:

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.... *Id.* [Pet., p. 33, emphasis in original]

111. Elements 1a, 23b, and 43b specifically require that the image has “information embedded therein.” As properly construed in the context of the ’167 Patent, “the image having information embedded therein” means information that is hidden in the image and used to provide security for the transaction.

112. Although Wang uses the term “embedded,” it only uses it in the context of combining hardware elements, *e.g.*, “FIG. 5C represents an external view of the PEAD of FIG. 5B after being embedded in a card-like package for ease of carrying and insertion into a Serial I/O port of the electronic transaction system” [Ex. 1004 at 0069]. Wang never uses the term “embedded” in the context of information in an image.

113. Wang at 0115 discusses the use of the barcode or OCR scanner only in the context of reading a Universal Product Code (or “UPC code”) or a “StoreID” barcode. A UPC code is a barcode used worldwide for identifying and tracking goods in stores. The data in a UPC code is explicitly public and not secured from unauthorized access because UPC codes are intended for public use and the information they contain must be read by various stockkeeping and checkout systems. Wang provides no information to suggest that the StoreID barcode is secured from unauthorized access and Wang’s stipulation that the StoreID could be

manually entered by the user [Ex. 1004 at 0115] implies that the information in the StoreID is public and unsecured. The information in the UPC and StoreID barcodes is not “embedded” as required by the ’167 Patent. Rather, the data stored in such barcodes can be decoded by anyone with a conventional barcode scanner using the public UPC standard.

114. The Petition points to Wang at 0115 as the sole reason that “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**” [Pet., p. 33, emphasis in original]. However, Petitioner has not shown that the UPC barcodes captured in Wang have information embedded therein, where the information in the image is hidden in the image and used to provide security for the transaction as required by the ’167 Patent. Therefore, Petitioner has not shown that Wang discloses Element 1a, 23b, or 43b of the ’167 Patent.

2. Petitioner has not shown that Wang anticipates storing predetermined information

115. Elements 1b, 23c, and 43c of the claims challenged in Ground I all refer to storing predetermined information (emphasis added):

Element 1b	Element 23c	Element 43c
a memory configured to store <u>predetermined information</u> ; [Ex. 1001, 16:27]	store <u>predetermined information</u> ; [Ex. 1001, 17:55]	store <u>predetermined information</u> ; [Ex. 1001, 19:4-5]

116. As properly construed in the ’167 Patent, “predetermined information”

includes, for example, “address information, personal profile information and payment account information” [Ex. 1001, 6:19-22] and explicitly excludes public and private keys [Ex. 1001, 6:15-18], input information provided by the user [Ex. 1001, 6:15-18], identification information provided by the user [Ex. 1001, 6:63-66].

117. Petitioner incorrectly construes “predetermined information” to include the user’s private key [Pet., p. 21] even though the ’167 Patent explicitly describes “predetermined information” as distinct from the public and private keys [Ex. 1001, 6:15-18].

118. Having incorrectly construed the term “predetermined information,” Petitioner cites three paragraphs from Wang in relation to Elements 1b, 23c, and 43c:

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.”⁵ [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]. (Pet. at pp. 33-34, emphasis in original.)

119. The quotes from Wang ¶0115 and ¶0085 are not directed to storing the user’s private key in memory and so are not relevant to Petitioner’s argument in relation to Elements 1b, 23c, and 43c. Footnote 5 in the Petition acknowledges that U.S. Pat. No. 5,917,913 “includes generally the same disclosure as Wang.” Only the

quotes from Wang at ¶0050 are relevant to Petitioner’s argument. Petitioner’s argument in relation to Elements 1b, 23c, and 43c rests solely on the quotes from Wang at ¶0050 which refer to “the user’s private key.”

120. However, as discussed above in Claim Construction, the ’167 Patent makes an explicit distinction between “predetermined information” and the user’s private key: “the corresponding private key (as well as other information, such as, predetermined information stored in the memory ...) may be used to decrypt or decode the captured image” [Ex. 1001, 6:16-19, emphasis added].

121. As clearly distinguished by the ’167 Patent, the private key is not and cannot be interpreted as “predetermined information.” The Petition is wrong to assert that the private key in Wang is “predetermined information” as defined by the ’167 Patent since it clearly cannot be. Therefore, Petitioner has not shown that Wang discloses Element 1b, 23c, or 43c of the ’167 Patent.

3. Petitioner has not shown that Wang anticipates generating an output based on the information embedded in the image and the predetermined information

122. Elements 1f, 23f, and 43f of the claims challenged in Ground I all use the same language in the claim limitations (emphasis added):

Element 1f	Element 23f	Element 43f
generate an output based on the <u>information embedded in the image</u> and the <u>predetermined</u>	generate an output based on the <u>information embedded in the image</u> and the <u>predetermined</u>	generate an output based on the <u>information embedded in the image</u> and the <u>predetermined</u>

<u>information;</u> [Ex. 1001, 16:33-34]	<u>information;</u> [Ex. 1001, 17:59-60]	<u>information;</u> [Ex. 1001, 20:1-2]
---	---	---

123. The Petition’s arguments in relation to Elements 1f and 23f are the same, and the Petition’s argument in relation to Element 43f merely cites the argument in relation to Element 23f, so the Petition only has one argument in relation to these three claim elements.

124. The Petition’s argument in relation to Elements 1f, 23f, and 43f incorrectly refers to barcode information in Wang as information embedded in an image: “The digitally signed receipt is based on **information embedded in an image** (barcode information)” [Pet., pp. 35, 40, emphasis in original]. As discussed above, the UPC barcodes in Wang do not have information embedded therein as properly construed in the ’167 Patent.

125. The Petition also incorrectly refers to the private key in Wang as predetermined information: “The digitally signed receipt is also based on the **predetermined information** (private key) ... Thus, the private key (predetermined information) is utilized to digitally sign the receipt” [Pet., pp. 35, 40, emphasis in original]. As discussed above, the ’167 Patent explicitly excludes the private key from predetermined information, so the private key of Wang cannot be predetermined information.

126. Petitioner has not shown that Wang can generate an output based on the

information embedded in the image and the predetermined information because the barcode information in Wang is not information embedded in an image as required by the '167 Patent, and the private key in Wang is not predetermined information as required by the '167 Patent. Therefore, the Petitioner has not shown that Wang anticipates Elements 1f, 23f, and 43f of the '167 Patent.

4. Petitioner has not shown that Wang anticipates a digital signature to be used to signify authorization by the user

127. Elements 1h and 23h of the claims challenged in Ground I use the same language in the claim limitations (emphasis added):

Element 1h	Element 23h
wherein the output includes a <u>digital signature to be used to signify authorization by the user</u> with respect to the transaction; [Ex. 1001, 16:35-38]	wherein the output includes a <u>digital signature to be used to signify authorization by the user</u> with respect to the transaction; [Ex. 1001, 17:62-64]

128. Petitioner's entire argument in relation to Elements 1h and 23h is, "The output (digitally signed receipt) is electronically signed. An electronic signature as disclosed in Wang is a digital signature" The Petition does not explain how a digitally signed receipt is to be used to signify authorization by the user of the transaction. [Pet., pp. 36, 41].

129. Digital signatures can be used for a wide variety of purposes in addition to authorization. Digital signatures can be used to ensure the authenticity and integrity of signed data, such as signing a document to ensure that it comes from a

trusted source and that it has not been modified. Digital signatures can be used for authentication, such as to verify the identity of a party or entity. Digital signatures can be used for non-repudiation, to ensure that once a message has been signed, the signer cannot deny having signed it. This variety of uses of digital signatures was well known at the time of the '167 Patent and would have been familiar to a POSITA [Ex. 2013, p. 1].

130. The Petition uses a single quote from Wang to support its argument: ““The PEAD user can **sign the receipt electronically** using PEAD....’ [0115]” [Pet., p. 41]. Neither the Petition’s sole argument nor its single quote refer to a “digital signature to be used to signify authorization by the user” as required by the '167 Patent, *e.g.*, “by receiving the generated confirmation signature or authorization code 740 from the user, the sender may verify whether the user is authorized to provide approval for the transaction” [Ex. 1001, 10:59-62].

131. As explained above, a person of ordinary skill in the art reading the claims in light of the specification would understand that “a digital signature to be used to signify authorization by the user with respect to the transaction” is a digital signature that is necessary to effect (or complete) the transaction. In contrast, the quote from Wang cited by Petitioner refers to a digital signature on a receipt. A digital signature by a user on a receipt would signify nothing more than that the user signed the receipt and that the receipt had not been modified since the signing.

However, a receipt would necessarily be produced after a transaction has been completed and not prior to a transaction when the authorization by the user with respect to the transaction is in question.

132. Indeed, Wang describes the generation and use of the receipt as separate from and following the transaction: “If the user agrees to pay for the item, the user can approve the transaction by pressing the button on the phone. The approval process using the PEAD is described in U.S. Pat. No. 5,917,913. 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” [Ex. 1004, ¶0115]. That is, the approval of the transaction happens first, and then either a digitally signed or hardcopy receipt is produced.

133. It does not follow from the fact that the user has signed the receipt that the underlying transaction that led to the receipt was in fact authorized by the user, as claimed by the Petition. In fact, a user could sign a receipt for a transaction that was not authorized or never occurred. Or a user could sign a forged receipt. None of these things would signify authorization by the user with respect to the transaction. And the Petition does not say how a digitally signed receipt would signify authorization by the user with respect to the transaction.

134. In summary, Petitioner does not argue that Wang anticipates a digital

signature to be used to signify authorization by the user with respect to the transaction as required by the '167 Patent, and the Petition's quote from Wang in support of Petitioner's argument does not show a digital signature to be used to signify authorization by the user with respect to the transaction. Therefore, Petitioner has not shown that Wang anticipates Elements 1h and 23h of the '167 Patent.

5. Petitioner has not shown that the '167 Patent is anticipated by Wang and obvious over Wang in view of Drummond

135. As discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates each and every element of claims 1, 23, and 43. Petitioner makes a secondary argument in Ground I that Elements 1g, 23g, and 43g are obvious if Wang is modified as shown by Drummond. However, even in this secondary argument, Petitioner has not shown that the combination of Wang and Drummond anticipates each and every element of claims 1, 23, and 43 because Petitioner has not shown that Wang anticipates Elements 1a, 1b, 1f, 1h, 23b, 23c, 23f, 23h, 43b, 43c, and 43f of the claims.

136. Therefore, Petitioner has not shown that the claims of the '167 Patent challenged in Ground I are unpatentable by a preponderance of the evidence.

B. Ground II

137. The Petition argues in Ground II that claims 1, 2, 4, 7, 12 and, 17 are anticipated by Wang. However, Petitioner's analysis of Wang is deficient, and the claims challenged in Ground I are not anticipated by Wang, as described in detail

below.

1. Petitioner has not shown that Wang anticipates capturing an image, the image having information embedded therein

138. Petitioner’s argument in Ground II in relation to Element 1a of claim 1 merely cites Petitioner’s analysis in Ground I. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang discloses Element 1a of the ’167 Patent.

2. Petitioner has not shown that Wang anticipates storing predetermined information

139. Element 1b of claim 1 challenged in Ground II refers to storing predetermined information (emphasis added): “a memory configured to store *predetermined information*;” [Ex. 1001, 16:27].

140. As properly construed in the ’167 Patent, “predetermined information” includes, for example, “address information, personal profile information and payment account information” [Ex. 1001, 6:19-22] and explicitly excludes public and private keys [Ex. 1001, 6:15-18], and identification information provided by the user [Ex. 1001, 6:63-66].

141. Petitioner incorrectly construes “predetermined information” to include “user identification data” [Pet., p. 43] even though the ’167 Patent explicitly describes “predetermined information” as distinct from identification information provided by the user [Ex. 1001, 6:63-66].

142. Having incorrectly construed the term “predetermined information,” Petitioner cites two paragraphs from Wang in relation to “user identification data”:

“[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].

[Pet., p. 45]

143. However, as discussed above, the ’167 Patent makes an explicit distinction between “predetermined information” and user identification data: “The Secure device 100 then derives the authentication code 350 and other relevant information 360 based on the embedded information stored in the scanned image or video 340 and, optionally, other **types** of information including, for example, predetermined information stored in the secure device 100 and identification information provided by the user.” [Ex. 1001, 6:60-66, emphasis added]. Here, the ’167 Patent identifies three categories of information and distinguishes among them: (1) “other types of information,” which includes the examples that follow; (2) “predetermined information,” which is one type of “other information”; and (3) “identification information provided by the user,” which is another type of “other information.”

144. The phrase “identification information provided by the user” in the ’167 Patent has the same meaning as the phrase “user identification information” in Wang because as cited by the Petitioner, “the [transaction program]...receives user’s data from the user (e.g., the user’s identification data” [Wang, ¶0093, emphasis added], so the “user identification data” in Wang is identification information provided by the user.

145. As clearly distinguished by the ’167 Patent, the user identification data is not and cannot be interpreted as “predetermined information.” The Petition is wrong to assert that the user identification data in Wang is “predetermined information” as defined by the ’167 Patent since it clearly cannot be. Simply put, the Petition’s mapping in relation to Element 1f in Ground II fails because Wang’s “identification data” is outside the scope of “predetermined information” in the context of the ’167 Patent. Therefore, Petitioner has not shown that Wang discloses Element 1b of the ’167 Patent.

3. Petitioner has not shown that Wang anticipates generating an output based on the information embedded in the image and the predetermined information

146. Element 1f of claim 1 challenged in Ground II recites (emphasis added): “generate an output based on the information embedded in the image and the predetermined information;” [Ex. 1001, 16:33-34].

147. The Petition’s argument in relation to Element 1f incorrectly refers to

barcode information in Wang as information embedded in an image: “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)” [Pet., p. 46]. As discussed above, the UPC barcodes in Wang do not have information embedded therein as properly construed in the ’167 Patent.

148. The Petition also incorrectly refers to user identification data in Wang as predetermined information: “The transaction approval data is also based on predetermined information—specifically ‘user identification data.’” [Pet., p. 47]. As discussed above, the ’167 Patent explicitly excludes user identification data from predetermined information, so the user identification data of Wang cannot be predetermined information.

149. Petitioner has not shown that Wang can generate an output based on the information embedded in the image and the predetermined information because the barcode information in Wang is not information embedded in an image as required by the ’167 Patent, and user identification data in Wang is not predetermined information as required by the ’167 Patent. Therefore, the Petitioner has not shown that Wang anticipates Element 1f of the ’167 Patent.

4. Petitioner has not shown that Wang anticipates the limitation that “the output includes a digital signature to be used to signify authorization by the user with respect to the transaction”

150. As in Ground I, the Petition cites Wang’s signature on the receipt in Ground II: ““The PEAD user can **sign the receipt electronically** using PEAD.’ [0115]” [Pet., p. 47, emphasis in original]. The Petition does not make any additional arguments in Ground II in relation to an electronically signed receipt, and as discussed in relation to Ground I, the Petition does not show that Wang anticipates a digital signature to be used to signify authorization by the user with respect to the transaction as required by the ’167 Patent.

151. Additionally, Element 1h of claim 1 challenged in Ground II recites: “wherein the output includes a digital signature to be used to signify authorization by the user with respect to the transaction” [Ex. 1001, 16:35-38]. The phrase “the output” in Element 1h refers to the output generated in Element 1f: “generate an output based on the information embedded in the image and the predetermined information” [Ex. 1001, 16:33-34]. This output is based on the “information embedded in the image” and “predetermined information” referenced in Elements 1a and 1b respectively.

152. However, as discussed above in relation to Elements 1a, 1b, and 1f, Petitioner has not shown that Wang can capture an image, the image having

information embedded therein, as required by Element 1a; that Wang has a memory configured to store predetermined information as required by Element 1b; or that Wang can generate an output based on the information embedded in the image and the predetermined information as required by Element 1f.

153. Petitioner has not shown that Wang anticipates Elements 1a, 1b, and 1f of claim 1 and the Petition makes no new arguments in relation to these Elements in the context of Element 1h. Without the output required by Element 1f, there is no way to satisfy the requirement in Element 1h that the output includes a digital signature to be used to signify authorization by the user with respect to the transaction.

154. Therefore, Petitioner has not shown that Wang anticipates Element 1f of claim 1 challenged in Ground II.

5. Petitioner has not shown that the '167 Patent is anticipated by Wang

155. As discussed above in relation to Ground II, Petitioner has not shown that Wang anticipates each and every element of claim 1. The remaining claims challenged in Ground II are dependent on claim 1. Therefore, Petitioner has not shown that the claims of the '167 Patent challenged in Ground II are unpatentable by a preponderance of the evidence.

C. Ground III

156. The Petition argues in Ground III that claims 19-21 and 39-41 are obvious over Wang in view of Drummond. However, Petitioner's analysis of the alleged prior art is deficient, and the claims challenged in Ground III are not obvious over Wang in view of Drummond, as described in detail below.

1. Petitioner has not shown that Wang anticipates capturing an image, the image having information embedded therein

157. Petitioner's argument in Ground III in relation to Element 19a of claim 19 merely cites Petitioner's analysis of Element 1a in Ground I. Elements 1a and 19a both recite the phrase "an image capture device configured to capture an image, the image having information embedded therein" [Ex. 1001, 16:24-25 and 17:29-30]. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates Element 1a of the '167 Patent because Wang does not disclose an image capture device configured to capture an image, the image having information embedded therein. Therefore, Petitioner has not shown that Wang anticipates Element 19a in Ground III.

158. Petitioner's argument in Ground III in relation to Element 39b of claim 39 merely cites Petitioner's analysis of Element 23b in Ground I. Elements 23b and 39b both recite the phrase "capture an image, the image having information embedded therein" [Ex. 1001, 17:51-52 and 18:52-53]. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates Element 23b

of the '167 Patent because Wang does not disclose capturing an image, the image having information embedded therein. Therefore, Petitioner has not shown that Wang anticipates Element 39b in Ground III.

2. Petitioner has not shown that Wang anticipates storing predetermined information

159. Petitioner's argument in Ground III in relation to Element 19b of claim 19 merely cites Petitioner's analysis of Element 1b in Ground I. Elements 1b and 19b both recite the phrase "a memory configured to store predetermined information"¹¹ [Ex. 1001, 16:27 and 17:31]. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates Element 1b of the '167 Patent because the private key in Wang is not predetermined information. Therefore, Petitioner has not shown that Wang anticipates Element 19a in Ground III.

160. Petitioner's argument in Ground III in relation to Element 39c of claim 39 merely cites Petitioner's analysis of Element 23c in Ground I. Elements 23c and 39c both recite the phrase "store predetermined information;" [Ex. 1001, 17:55 and 18:54]. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates Element 23c of the '167 Patent because the private key in Wang is not predetermined information. Therefore, Petitioner has not shown that

¹¹ The actual text of Element 19b is "a memory configured to store predetermined location;" However, from the file history, this is clearly a transcription error. See Ex. 1003 at pp. 58, 77.

Wang anticipates Element 39c in Ground III.

3. Petitioner has not shown that Wang anticipates generating an output based on the information embedded in the image and the predetermined information

161. Petitioner's argument in Ground III in relation to Element 19f of claim 19 merely cites Petitioner's analysis of Element 1f in Ground I. Elements 1f and 19f both recite the phrase "generate an output based on the information embedded in the image and the predetermined information" [Ex. 1001, 16:33-34 and 17:36-37]. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates Element 1f of the '167 Patent because the barcode information in Wang is not information embedded in an image as required by the '167 Patent and the private key in Wang is not predetermined information as required by the '167 Patent. Therefore, Petitioner has not shown that Wang anticipates Element 19f in Ground III.

162. Petitioner's argument in Ground III in relation to Element 39f of claim 39 merely cites Petitioner's analysis of Element 23f in Ground I. Elements 23f and 39f both recite the phrase "generate an output based on the information embedded in the image and the predetermined information;" [Ex. 1001, 17:59-60 and 18:58-59]. However, as discussed above in relation to Ground I, Petitioner has not shown that Wang anticipates Element 23f of the '167 Patent because the barcode information in Wang is not information embedded in an image as required by the

'167 Patent and the private key in Wang is not predetermined information as required by the '167 Patent. Therefore, Petitioner has not shown that Wang anticipates Element 39f in Ground III.

4. Petitioner has not shown that the '167 Patent is obvious over Wang in view of Drummond

163. Petitioner's argument in Ground III relies on Ground I to support the assertion that Elements 19a-f and 39a-f of the Challenged Claims are obvious over Wang in view of Drummond: "[19a-f] See Ground 1, Elements 1a-f analysis" [Pet., p. 52, emphasis in original], "Elements 39a-f See Ground 1, Elements 23a-f analysis" [Pet., p. 53, emphasis in original]. However, Ground I makes no mention of Drummond and as discussed above, Ground I does not show that Wang anticipates Elements 1a, 1b, 1f, 23b, 23c, 23f, of the Challenged Claims. Therefore, Petitioner has not shown that Wang anticipates Elements 19a, 19b, 19f, 39b, 39c, and 39f of the Challenged Claims.

164. Petitioner argues in Ground III that Elements 19g, 19h, 39g, and 39h are obvious if Wang is modified as shown by Drummond. However, Petitioner has not shown that the combination of Wang and Drummond anticipates each and every element of claims 19 and 39 because Petitioner has not shown that Wang anticipates Elements 19a, 19b, 19f, 39b, 39c, and 39f of the Challenged Claims. Therefore, Petitioner has not shown that the claims of the '167 Patent challenged in Ground III

are unpatentable by a preponderance of the evidence.

165. Therefore, Petitioner has not shown that the claims of the '167 Patent challenged in Ground III are unpatentable by a preponderance of the evidence.

D. Ground VI

166. The Petition argues in Ground VI that 1, 4, 5, 7, 23, 26, 27, 29, and 43 are obvious over TAO in view of PTM and Wang. However, Petitioner's analysis of TAO in view of PTM and Wang is deficient, and the claims challenged in Ground VI are not obvious over TAO in view of PTM and Wang, as described in detail below.

1. Petitioner has not shown that capturing an image, the image having information embedded therein is obvious over TAO in view of PTM and Wang

167. Elements 1a, 23b, and 43b of the claims challenged in Ground VI relate to capturing an image, the image having information embedded therein (emphasis added):

Element 1a	Element 23b	Element 43b
an image capture device configured to capture an image, <u>the image having information embedded therein</u> including information relating to a transaction; [Ex. 1001, 16:24-26]	capture an image, <u>the image having information embedded therein</u> , the information embedded in the image including information relating to a transaction; [Ex. 1001, 17:51-54]	capture an image, the <u>image having information embedded therein</u> ; [Ex. 1001, 19:4-5]

168. As discussed in detail above, in the context of the '167 Patent,

information “embedded” in an image refers to information that is hidden in the image and used to provide security for the transaction. The Petition’s argument in relation to Element 1a maps this claim element to the disclosure in TAO of a vendor scanning a product barcode to generate an order for a customer: “A barcode scanner is an image capture device. Ex. 1002 at 59. 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. Id. at 146” and the Petition merely refers to Element 1a in relation to Elements 23b and 43b.

169. There is no evidence in TAO nor does the Petition argue that the barcodes scanned by TAO are anything other than conventional barcodes such as UPC barcodes. In Ground II and as discussed above in relation to Element 1a in Ground I, Petitioner has not shown that the product barcodes in TAO have information embedded therein, where the information in the image is hidden in the image and used to provide security for the transaction as required by the ’167 Patent. Therefore, Petitioner has not shown that capturing an image, the image having information embedded therein is obvious over TAO in view of PTM and Wang.

2. Petitioner has not shown that capturing an image is obvious over TAO in view of PTM and Wang

170. Elements 1a, 23b, and 43b of the claims challenged in Ground VI relate

to image capture (emphasis added):

Element 1a	Element 23b	Element 43b
an image capture device configured to capture an image, <u>the image having information embedded therein</u> including information relating to a transaction; [Ex. 1001, 16:24-26]	capture an image, <u>the image having information embedded therein</u> , the information embedded in the image including information relating to a transaction; [Ex. 1001, 17:51-54]	capture an image, the <u>image having information embedded therein</u> ; [Ex. 1001, 19:4-5]

171. In relation to Element 1a of claim 1, the Petition argues that “TAO discloses an image capture device that captures an image (e.g., a barcode)” [Pet., p. 65] The Petition’s arguments in relation to Elements 23b and 43b merely refer to the argument in relation to Element 1a.

172. TAO describes its barcode scanning capabilities as follows:

Point-of-sale Software for the Palm Computing Platform

Are you selling products at trade shows or expos? Taking orders from customers in their home or office? Submitting bids or issuing quotations in a field situation? Delivering product and need to issue a receipt? For all these situations and more, **Take An Order! is the handheld tool you need.** Combined with any Palm Computing platform handheld device including barcode scanning SPT units from Symbol Technologies and a portable printer like the Canon BJC-55 or Brother MPrint, **Take An Order!** gives you an office that travels with you.

[Ex. 1005, p. 1, red underlining added]

173. However, the SPT units from Symbol Technologies identified in TAO do not have image capture devices. Indeed, the SPT 1800 devices cited by TAO only

had linear scanning capabilities. *See, e.g.*, Symbol SPT 1800 Series Product Reference Guide [Ex. 2009], p. xi. The Symbol SPT 1700 devices cited by TAO [TAO, p. 1] could only scan two-dimensional PDF417 barcodes if the operator “Manually raster[ed] the scan line by slowly moving the scanner up and down so it scans the entire bar code,” thus manually scanning the linear rows of the PDF417 barcode one by one. *See*, Symbol SPT 1700 Series Product Reference Guide [Ex. 2010], pp. 17-8 to 17-9. These linear scanning capabilities, explicitly promoted by TAO, are clearly not capable of capturing an image as required by the ’167 Patent.

174. The Petition’s mapping of “image capture” in Ground VI is deficient because the Petition has not shown that TAO has an image capture device. Therefore, Petitioner has not shown that “captur[ing] an image, the image having information embedded therein including information relating to a transaction” as required by Elements 1a and 23b of the ’167 Patent is obvious over TAO in view of PTM and Wang.

3. Petitioner has not shown that verifying the user is obvious over TAO in view of PTM and Wang

175. Elements 1e, 23e, and 43e of the claims challenged in Ground VI relate to verifying the user:

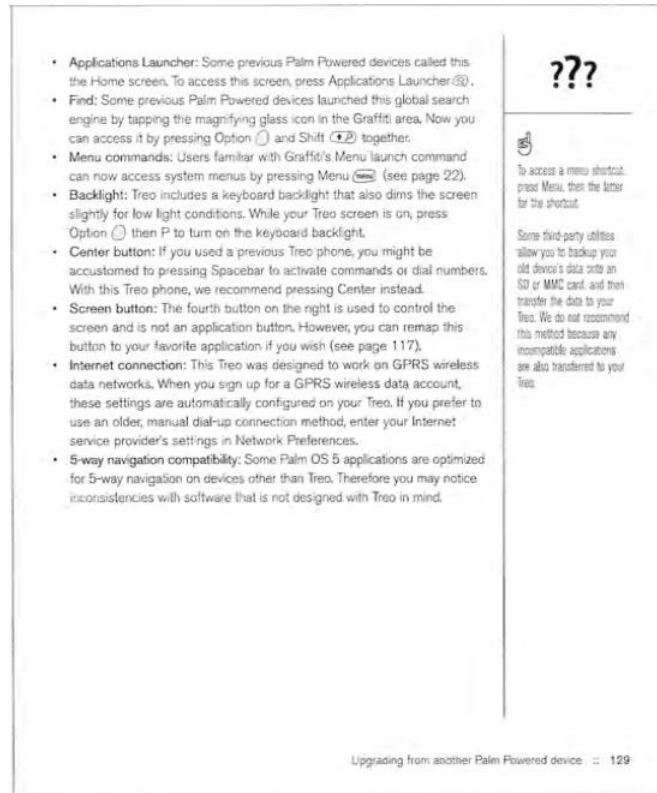
Element 1e	Element 23e	Element 43e
verify the user based on the input information to ensure that the user is authorized to use the apparatus; [Ex. 1001, 16:30-31]	verify the user based on the input information to ensure that the user is authorized to use the portable device; [Ex. 1001, 17:57-58]	verify the user based on the input information to ensure that the user is authorized to use the portable device; [Ex. 1001:8-9]

176. The Petition maps Element 1e to alleged password functionality in the Palm Treo and the Petition’s arguments in relation to Elements 23e and 34e merely refer to the argument in relation to Element 1e:

[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.
---	--

Pet., p. 66

177. Ex. 1006 is the Palm Treo Manual (“PTM”). Page 129 of PTM (reproduced below) has nothing to do with passwords or security and is merely the second half of a section on upgrading from a previous device.



Ex. 1006, p. 129

178. Elsewhere, the Petition cites page 24 of PTM: “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” [Pet., p. 27]. Page 24 of PTM (reproduced below) has nothing to do with passwords or security and is merely a guide to symbols and accented characters.

Symbols and accented characters					
Type...	then press Alt to choose...	Type...	then press Alt to choose...	Type...	then press Alt to choose...
a	á à â ã ä å æ	o	ó ô õ ö ø ò	0	% %0 *
A	Á Â Ã Ä Å Æ	O	Ó Ô Õ Ö Ø Ò	1	¼ ½
b or B	ß	p or P	þ ð	2	²
c	ç è é ê ë	r or R	ŗ ړ	3	¾
C	Ç È É Ê Ë	s	š š Š š		? ! ...
d	đ ð	S	Š š Š š		*
D	Ð ð	t or T	ţ Ț	!	!
e	é è ê ë	u	ú û ü	?	¿
E	É Ê Ë Ì	U	Ú Û Ü	:	: :- (-) :-D
f or F	f	x or X	x ǻ	*	* < > -
i	í î ï	y	ý ŷ	*	* * *
I	Í Î Ï	Y	Ÿ	\$	€ £ ¥ ¢
l or L	ℓ			+	&
m or M	μ			-	- - - - -
n	ñ			/	% \ + /
N	Ñ			#	=
				(	< [(
				)	>])

24 :: Symbols and accented characters

Ex. 1006, p. 24

179. The Petition’s citations to Ex. 1006 have not shown that “The Treo ‘[r]equires a password to see any data...’ indicating that it is secure.” Simply put, the mapping in Ground VI of Element 1e is deficient because the citations to the references provided by the Petition fail to demonstrate any password functionality.

4. Petitioner has not shown that generating an output based on the information embedded in the image is obvious over TAO in view of PTM and Wang

180. Elements 1f and 23f of the claims challenged in Ground VI use the same language in the claim limitations (emphasis added):

Element 1f	Element 23f	Element 43f
generate an output based on the <u>information embedded in the image</u> and the predetermined information; [Ex. 1001, 16:33-34]	generate an output based on the <u>information embedded in the image</u> and the predetermined information; [Ex. 1001, 17:59-60]	generate an output based on the information embedded in the image and the predetermined information; [Ex. 1001, 20:1-2]

181. The antecedents for “information embedded in the image” in Elements 1f, 23f, and 43f are in Elements 1a, 23b, and 43b: “capture an image, the image having information embedded therein including information relating to a transaction;” [Ex. 1001, 16:24-26, 17:51-54, and 19:4-5].

182. However, as discussed above, Petitioner has not shown that Elements 1a, 23b, and 43b are obvious over TAO in view of PTM and Wang. And the Petition’s arguments in relation to Elements 1f, 23f, and 43f offer nothing new to correct this deficiency. Without the ability to capture an image, the image having information embedded therein, there can be no ability to generate an output based on the information embedded in the image. Therefore, Petitioner has not shown that generating an output based on the information embedded in the image as required by Element 1f, 23f, or 43f of the ’167 Patent is obvious over TAO in view of PTM and Wang.

5. Petitioner has not shown that the ’167 Patent is obvious over TAO in view of PTM and Wang

183. As discussed above in relation to Ground VI, Petitioner has not shown that Elements 1a, 1e, 1f, 23b, 23e, 23f, 43b, 43e, or 43f are obvious over TAO in

view of PTM and Wang. Therefore, Petitioner has not shown that the claims of the '167 Patent challenged in Ground VI are unpatentable by a preponderance of the evidence.

XIII. Conclusion

184. This declaration represents the opinions that I have formed up to date based on the material currently available to me. I reserve the right to revise, supplement, and/or amend my opinions stated in this declaration based on new information that becomes available to me and on my continuing analysis of the materials available to me.

185. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine, imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: November 20, 2024



Kai Johnson