

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EARLY WARNING SERVICES, LLC,

Petitioner,

v.

INTELLECTUAL VENTURES II, LLC,

Patent Owner.

Case No. IPR2024-01221

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

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

PATENT OWNER’S EXHIBIT LIST	iv
I. INTRODUCTION	1
II. SPECIFICATION OF '167 PATENT.....	1
A. Background.....	1
1. The Use Of Static Information Such As A Personal Identification Number (PIN) Was Only Of Nominal Effectiveness In Reducing Payment Card Fraud ..	1
2. Non-Static Systems Which Required Synchronization Were Inefficient	2
3. Portable Devices That Presented Bar Codes With Encrypted Strings For Security	3
B. Detailed Description Of The Invention	5
1. General Embodiment - Figure 2	6
2. Authentication Embodiment - Figure 3	7
3. Embodiment For Secure Access To Physical Structures	12
4. Alternate Authentication Embodiment - Figure 4	13
5. Authorization Embodiment - Figure 5.....	16
6. Alternate Authorization Embodiment - Figure 6.....	19
7. Embodiment With Authorization Involving Multiple Parties	20
8. Authorization With Offline Digital Signature - Figure 7	21
9. Secure Document Distribution - Figure 8.....	22
10. Digital Rights Management.....	23
11. Conducting Transactions	24
12. Checkout Process - Figures 10 and 11.....	25
13. Defending Against Phishing Attacks - Figure 12.....	26
III. CLAIMS OF '167 PATENT	29
IV. Claim Construction.....	32
A. General Principles	32

1. The Construction That Stays True To The Claim Language And Most Naturally Aligns With The Specification Will Be The Correct Construction.....	32
2. Determining The Meaning Of A Claim Term Requires Examination of Terms That Have A Particular Meaning In A Field Of Art	32
B. "The Image Having Information <i>Embedded</i> Therein" (All Claims)....	34
C. "Predetermined Information" (All Claims).....	39
D. "A Digital Signature To Be Used To Signify Authorization By The User With Respect To The Transaction" (Claims 1 And 23).....	41
E. "Image Capture Device" / "Configuring A Portable Device To: Capture An Image" (Claims 1, 23 and 43)	42
V. PRIOR ART RELIED ON IN PETITION	43
A. U.S. Patent Publ. 2002/0023215 (Wang).....	44
B. Take An Order (TAO).....	45
C. U.S. Patent Publ. 2003/0217005 (Drummond).....	45
D. Palm Treo Manual (PTM).....	46
VI. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON THE MERITS	46
A. Ground 1 Does Not Have A Reasonable Likelihood Of Success.....	46
B. Ground 2 Does Not Have A Reasonable Likelihood Of Success.....	49
C. Ground 3 Does Not Have A Reasonable Likelihood Of Success.....	51
D. Ground 4 Does Not Have A Reasonable Likelihood Of Success.....	52
E. Ground 5 Does Not Have A Reasonable Likelihood Of Success	53
F. Ground 6 Does Not Have A Reasonable Likelihood Of Success	53
VII. CONCLUSION.....	58

PATENT OWNER'S EXHIBIT LIST

Ex. 2001	Declaration of Kai Johnson
Ex. 2002	Resume of Kai Johnson
Ex. 2003	" <i>Embedding Of Any Type Of Data In Images Based On A Human Visual Model And Multiple-Based Number Conversion</i> ," Da-Chun Wu and Wen-Hsiang Tsai, Pattern Recognition Letter, Volume 20, Issue 14, December 1999, Pages 1511-1517
Ex. 2004	"Lossless Generalized-LSB Data Embedding," Celik, Mehmet Utku, et al., <i>IEEE transactions on image processing</i> 14.2 (2005): 253-266
Ex. 2005	"Lossless Data Embedding For All Image Formats," Fridrich, Jessica, Miroslav Goljan, and Rui Du. In <i>Security and watermarking of multimedia contents IV</i> (Vol. 4675, pp. 572-583). SPIE, 2002
Ex. 2006	<i>Embedding Data in 3D Models</i> , 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
Ex. 2007	<i>Embedding Biometric Identifiers In 2D Barcodes For Improved Security</i> , Noore, Afzel, Nikhil Tungala, and Max M. Houck. <i>Computers & Security</i> 23.8 (2004): 679-686
Ex. 2008	Data hiding in image and video. II. Designs and applications," Wu, Min, Heather Yu, and Bede Liu. <i>IEEE Transactions on Image Processing</i> 12.6 (2003): 696-705
Ex. 2009	Symbol SPT 1800 Series Product Reference Guide
Ex. 2010	Symbol SPT 1700 Series Product Reference Guide
Ex. 2011	Introduction to Bar Codes for the Automated Laboratory
Ex. 2012	Image Definition - Merriam Webster
Ex. 2013	FDIC Bulletin

I. INTRODUCTION

The Petition (Paper #1) challenges claims 1-2, 4-5, 7-8, 12-13, 17, 19-21, 23-24, 26-27, 29-30, 34, 39-41 and 43 (“Challenged Claims”) of U.S. Patent No. 7,314,167 (“’167 Patent,” Ex. 1001) under six grounds. Petition, at 29-30. The Petition fails to present a reasonable likelihood of success in connection with any of the grounds. This response begins with a discussion of the prior art discussed in the Background of the ’167 Patent, and each of the embodiments disclosed in the Detailed Description of the ’167 Patent. An analysis of the claims and cited references follows.

II. SPECIFICATION OF ’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

The ’167 was filed almost 20 years ago, 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 including use of a personal identification number (PIN) to reduce payment card fraud. Ex. 2001, ¶27. 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.* *Id.*, 1:29-38 (emphasis added).

2. Non-Static Systems Which Required Synchronization Were Inefficient

As explained in the '167 Patent, systems where dynamic (non-static) information was used for security also existed, but 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." *Id.*, 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. *Id.*, 1:56-63; 3:11-13; Ex. 2001, ¶28.

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." *Id.*, 2:17-22. Again, this system suffered from the drawback that "[s]ynchronization between the card and the computer is required," which was inefficient. *Id.*, 2:17-22; 3:11-13; Ex. 2001, ¶29.

In a still further prior art system used for managing financial data, a PDA was provided in which the user stored his financial and personal information. *Id.*, 2:29-30; Ex. 2001, ¶30. This system was further described in the '167 Patent 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. *Id.*, 2:30-38.

A still further 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." *Id.*, 2:61-66. Again, this system suffered from the drawback that it required "time-dependent synchronization." *Id.*, 3:9; Ex. 2001, ¶31.

3. Portable Devices That Presented Bar Codes With Encrypted Strings For Security

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. *Id.*, 2:39-44; Ex. 2001, ¶32. 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." *Id.*, 2:44-49. In connection with the transfer of a token to the verification system, the mobile device included a display that displayed a bar code containing the token. The verifying system (e.g., a point of sale device) could include a scanning or image capture device for reading the bar code displayed on the mobile device, and decrypting the encrypted string using a shared secret key. *Id.*, 2:51-59. In connection with obtaining the benefit, right, or product associated with the token, the mobile device in the token-based system did not capture an input image but instead generated and displayed an image captured to be captured by the verifying system. Ex. 2001, ¶32. In addition, the information in the image generated by the mobile device was readable by a conventional bar code scanner. Ex. 2001, ¶32.

In summary, 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. Ex. 2001, ¶33. 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. Ex. 2001, ¶33.

B. Detailed Description Of The Invention

The specification of the '167 Patent disclosed a portable secure device, and the use of the portable secure device to provide a secure transaction. *Id.*, 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. Ex. 2001, ¶34. 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); Ex. 2001, ¶34. As discussed more fully in Section IV(B), 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, at 2 ("Data embedding in images is an application that hides secret messages in digital images."); Ex. 2001, ¶34.

The '167 Patent discloses a number of 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. Ex. 2001, ¶35.

1. General Embodiment - Figure 2

Figure 2 describes operation of 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.

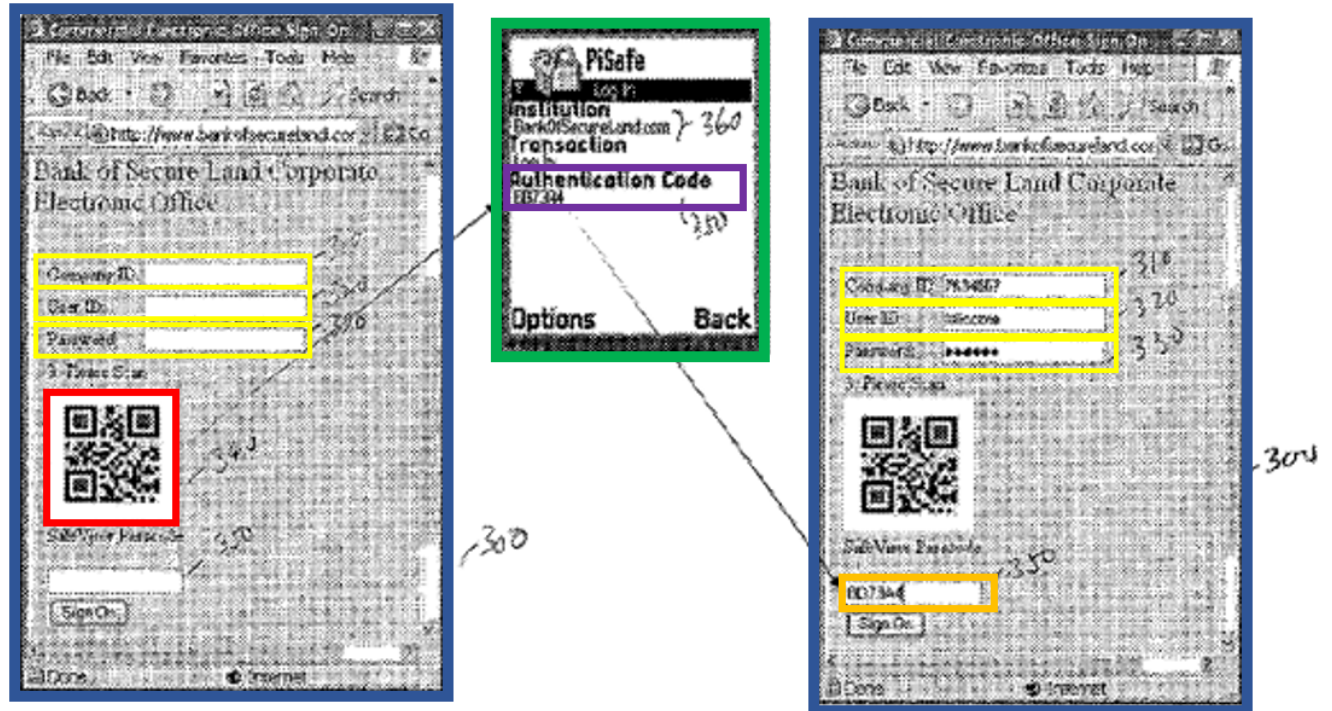
At block 230, upon successful verification of the user's identity and decoding of the captured image, the secure device 100 generates the appropriate instructions or information for the user. Ex. 1001, 5:47-6:28 (emphasis added).

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." Ex. 2001, ¶37. 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; Ex. 2001, ¶37.

2. Authentication Embodiment - Figure 3

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; Ex. 2001, ¶38. 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

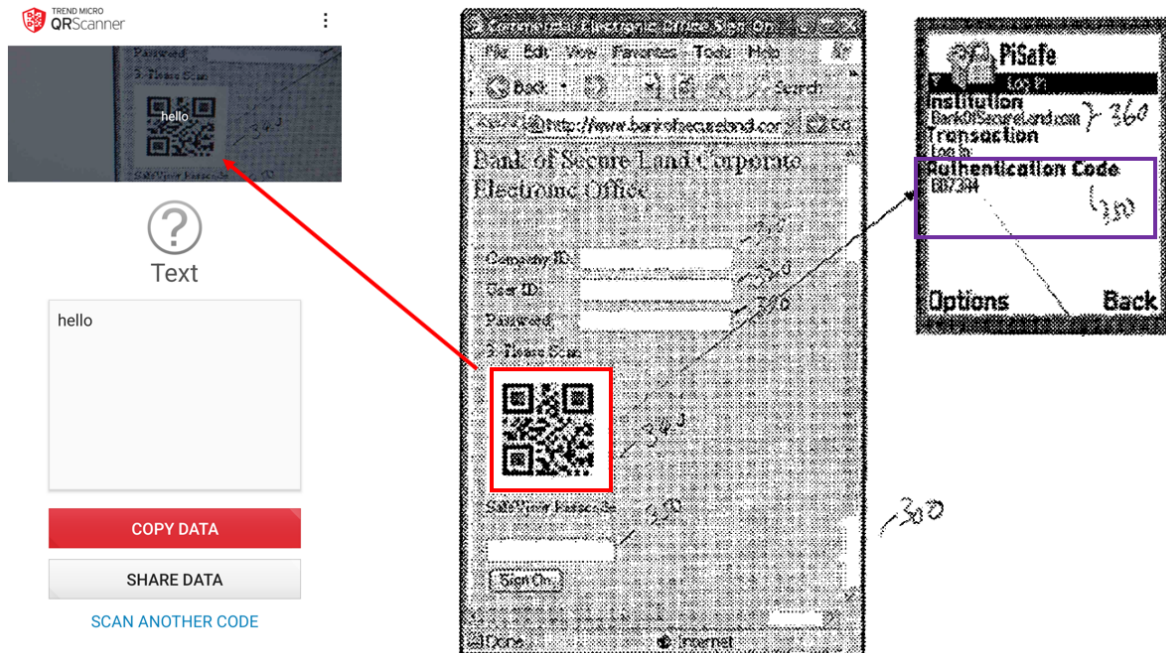
requiring user authentication, while the green box in the center depicts the display of the portable secure device.



By way of overview, in the embodiment of Figure 3, "a user visits a website and is presented with a log-on screen 300" (blue boxes). *Id.*, 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." *Id.*, 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]. *Id.*, 6:49-54; Ex. 2001, ¶39. As explained 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 and other relevant information 360 based on the embedded information stored in the scanned image or video 340 [red box] 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 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, the website also has knowledge regarding the correct authentication code 350 corresponding to the information embedded in the image or video 340. *Id.*, 6:55-7:14 (emphasis added).

Focusing on the 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:



Ex. 2001, ¶40. 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." Ex. 2001, ¶41. 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. Ex. 2001, ¶41. 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"), is able to derive the authentication code from the image. Ex. 2001, ¶41. As explained in the '167 Patent, in the authentication embodiment of Figure 3, the embedded information in the image is decoded using "an encryption, a decryption or a message authentication algorithm," and 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. 2001, ¶41.

In contrast to the embodiment of Figure 3 where information is embedded in the image (using an encryption, decryption, or 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. Ex. 2001, ¶42.

Notably, the predetermined information in the embodiment of Figure 3 is not the private key used to derive the embedded information from the image, but rather is characterized as falling within "other types of information" stored in the secure device. Ex. 2001, ¶43. "[I]dentification information¹ provided by the user" is described as 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

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. Ex. 2001, ¶43, note 1.

information including, for example, predetermined information stored in the secure device 100 and identification information provided by a user.") As was the case with the general embodiment of Figure 2 where the predetermined information was not the private key but rather "other information" like "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; Ex. 2001, ¶43.

3. Embodiment For Secure Access To Physical Structures

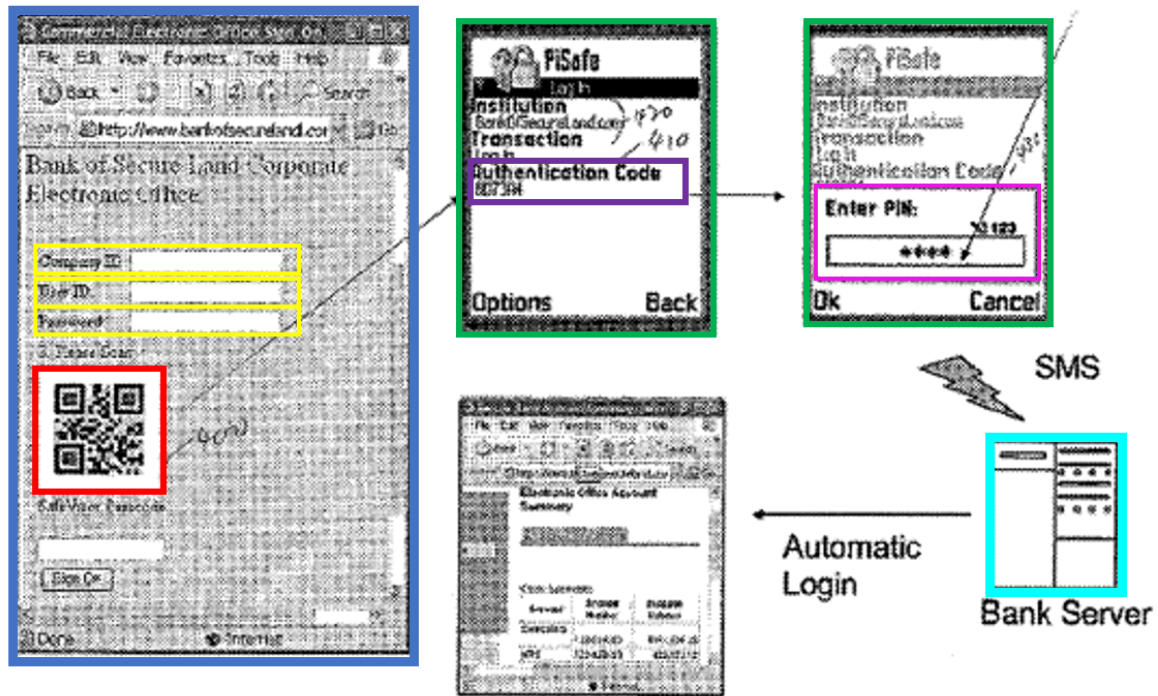
After describing the scanning and extraction of embedded information from an image in connection with Figure 3, the '167 Patent explained that "[t]he secure device 100 may also be used to identify or authenticate persons for physical access to structures and/or vehicles through entry points, such as, doors and gates." Ex. 1001, 7:24-26; Ex. 2001, ¶44. 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)." *Id.*, 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." *Id.*, 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." *Id.*, 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." *Id.*, 7:55-59.

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. Ex. 2001, ¶45.

4. Alternate Authentication Embodiment - Figure 4

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. 2001, ¶46. 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]." *Id.*, 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]." *Id.*, 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." *Id.*, 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." *Id.*, 8:62-67; Ex. 2001, ¶47.

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" (*id.*, 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." Ex. 2001, ¶48.

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." Ex. 2001, ¶49. 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. Ex. 2001, ¶49. Rather, only the secure device (which "has knowledge of the encryption algorithm that is used to create the

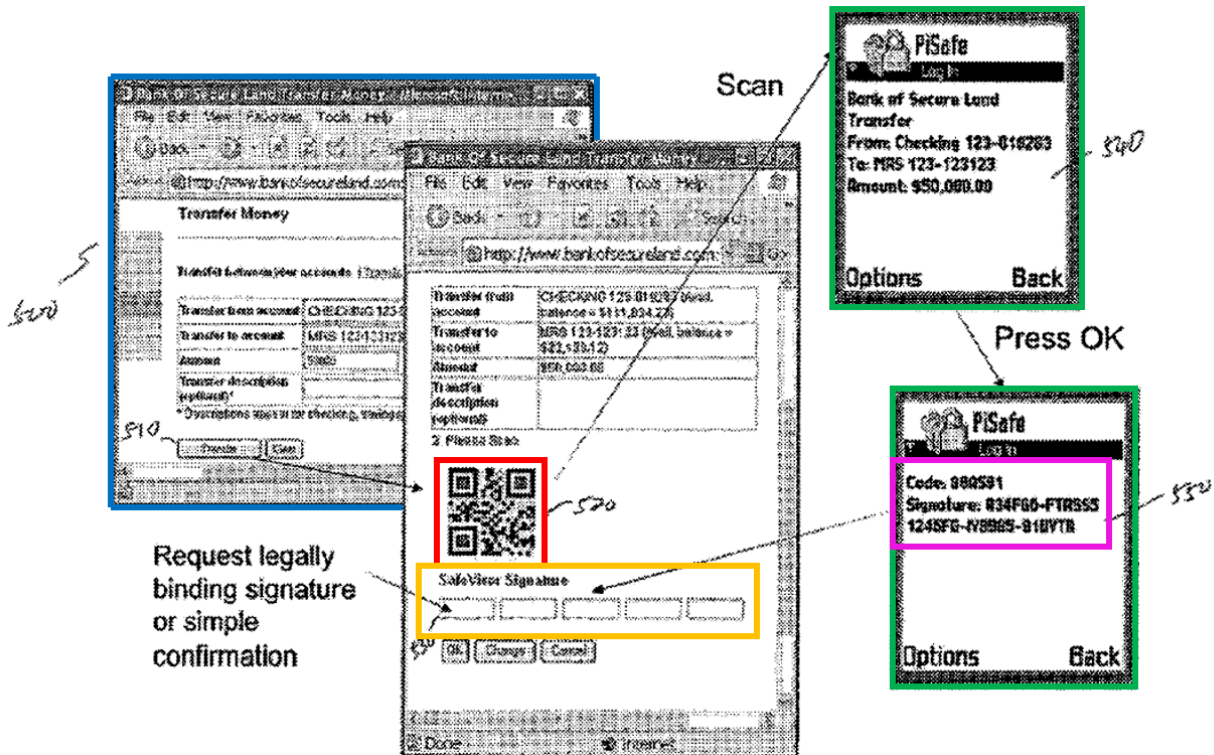
image"), is able to derive the authentication code from the image. Ex. 1001, 6:10-14; Ex. 2001, ¶49.

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 system that relied on static information that was disparaged in the Background of the '167 Patent. (Id., 1:37-38); Ex. 2001, ¶50.

5. Authorization Embodiment - Figure 5

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); Ex. 2001, ¶51. 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. *Id.*, 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." *Id.*, 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.



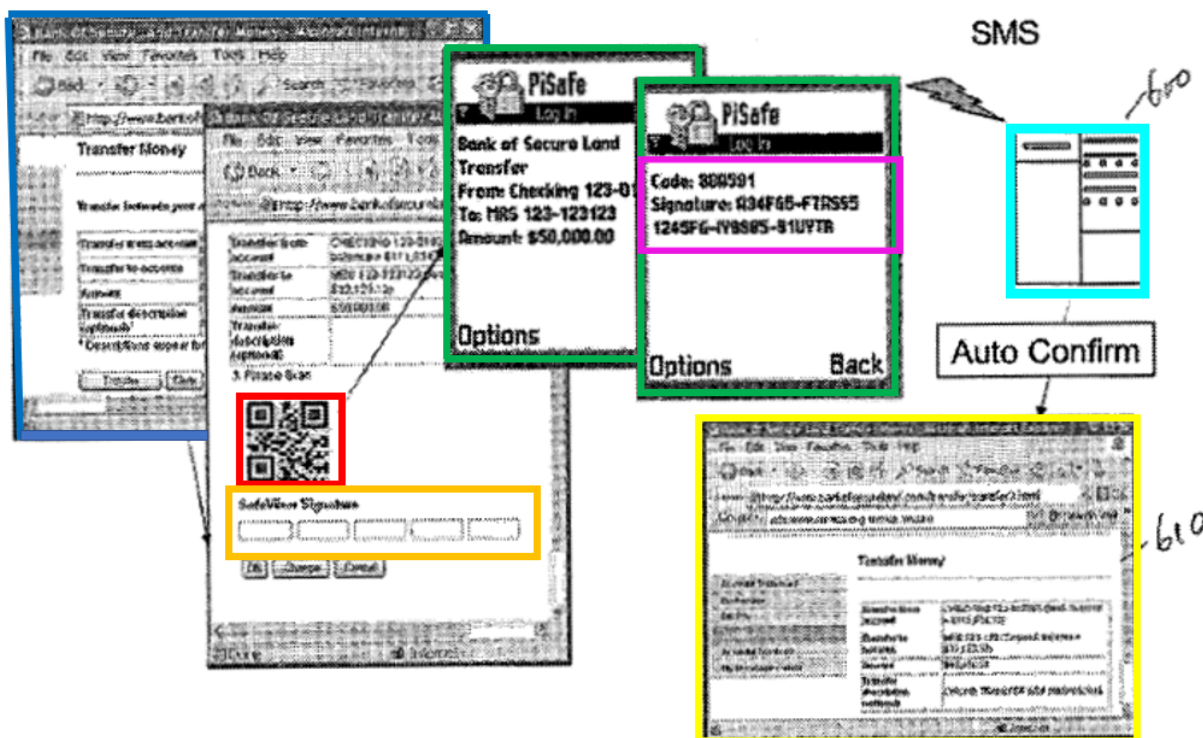
Ex. 2001, ¶51. In the embodiment of Figure 5, the user completes a form 500 [blue box] to effect transfer of money between accounts. "Upon hitting the "transfer" button 510, the website, terminal, server or device displays an image or stream of images 520 [red box] and a blank designated entry 530 [orange 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." *Id.*, 9:18-20 (emphasis added); Ex. 2001, ¶52. 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. *Id.*, 9:27-54 (emphasis added).

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. Ex. 2001, ¶53. 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 not what it says), 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." Ex. 2001, ¶53.

6. Alternate Authorization Embodiment - Figure 6

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; Ex. 2001, ¶54. Figure 6 (reproduced below with colored boxes added by Patent Owner) depicts this alternative authorization process:



Ex. 2001, ¶54. "[U]pon the secure device 100 generating the confirmation signature or authorization code [as discussed in connection with FIG. 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." *Id.*, 9:63-10:13 (emphasis added).

Like the embodiment of Figure 5, it is clear that the information used for secure authorization in the image in Figure 6 is hidden (or embedded) in the image. Ex. 1001, 10:7-11. Ex. 2001, ¶56.

7. Embodiment With Authorization Involving Multiple Parties

The '167 Patent also includes an embodiment where authorization "involving multiple parties" is achieved. Ex. 1001, 10:14-16; Ex. 2001, ¶57. 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." *Id.*, 10:16-24 (emphasis added); Ex. 2001, ¶57.

8. Authorization With Offline Digital Signature - Figure 7

Figure 7 depicts an embodiment where "the secure device 100 can be used to provide offline digital signature to effect authorization." *Id.*, 10:29-30; Ex. 2001, ¶58. 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 [that] 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." *Id.*, 10:31-62.

Again, it is clear that the information used to secure the transaction is embedded (hidden) in the image. Ex. 1001, 10:46-49; Ex. 2001, ¶59.

9. Secure Document Distribution - Figure 8

In the embodiment of Figure 8, the secure device 100 is "used to provide secure document distribution." Ex. 1001, 10:63-64; Ex. 2001, ¶60. Here, "a document is created and secured using a password." *Id.*, 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. Ex. 2001, ¶60. The information embedded in the image or stream of images can be created using public keys that are stored locally or centrally managed." *Id.*, 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. *Id.*, 11:25-28. Upon opening

the message, the recipient uses the secure device 100 to scan the image and then "derive the embedded information" from the image which is then displayed to the user. *Id.*, 11:28-35. The user then uses the displayed information to access the secured document. *Id.*, 11:35-36; Ex. 2001, ¶60.

Again, it is clear that the information used to secure the document is embedded (hidden) in the image. Ex. 1001, 11:30-34; Ex. 2001, ¶61.

10. Digital Rights Management

In another embodiment, "the secure device 100 can be used to effect digital rights management." Ex. 1001, 11:49-50; Ex. 2001, ¶62. 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." *Id.*, 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. *Id.*, 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. *Id.*, 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." *Id.*, 12:1-11.

Again, in the digital rights management embodiment, it is clear that information used to effect digital rights management is embedded (hidden) in the image. Ex. 1001, 11:60-63; Ex. 2001, ¶63.

11. Conducting Transactions

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). If "there 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 secure device 100 can capture the image or stream of images and decode its embedded information.

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. Ex. 2001, ¶64, note 2.

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." *Id.*, 13:16-33 (emphasis added); Ex. 2001, ¶64.

Again, it is clear that information used to secure the transaction is embedded (hidden) in the image. Ex. 2001, ¶65.

12. Checkout Process - Figures 10 and 11

In further embodiments, "the secure device 100 can be used in a checkout process." Ex. 1001, 13:40-41; Ex. 2001, ¶66. "[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." *Id.*, 13:42-

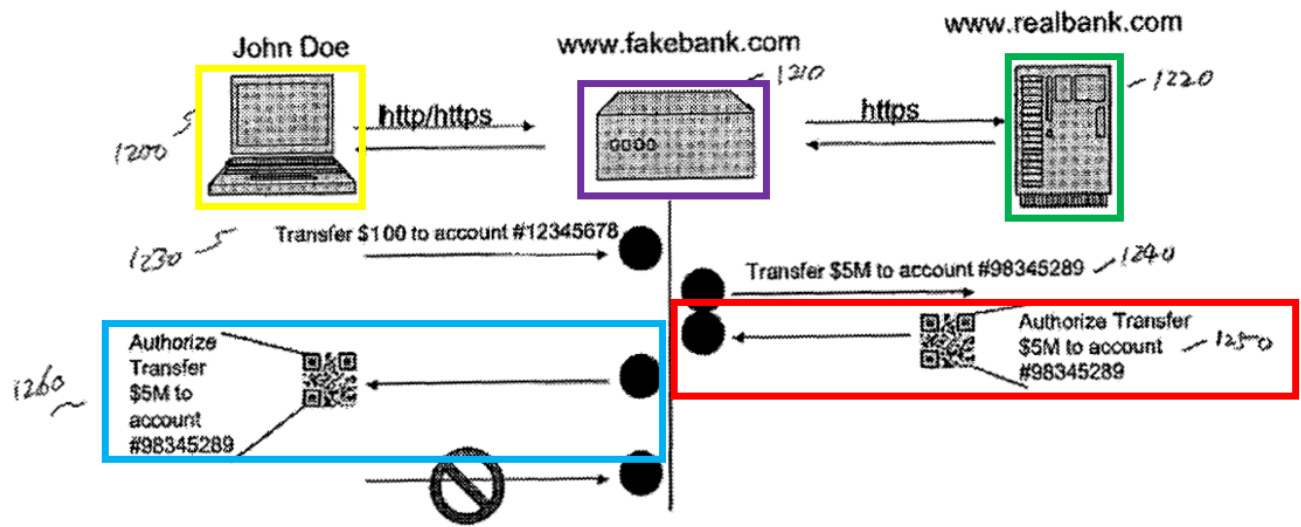
53 (emphasis added). The check-out embodiment of Figure 11 is described similarly. *Id.*, 14:6-23; Ex. 2001, ¶66.

In this embodiment, the merchant is verified using information embedded (hidden) in the image. Ex. 2001, ¶67. 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.³ Ex. 2001, ¶67.

13. Defending Against Phishing Attacks - Figure 12

"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; Ex. 2001, ¶68. Figure 12 (reproduced below with colored boxes added by Patent Owner) depicts this embodiment:

³ See, e.g., *SciMed Life Sys. v. Advanced Cardiovascular Sys.*, 242 F.3d 1337 (Fed. Cir. 2001), *citing*, *Tronzo v. Biomet, Inc.*, 156 F.3d 1154, 1159. 47 U.S.P.Q.2D (BNA) 1829, 1833 (Fed. Cir. 1998) (specification distinguished prior art as inferior and touted advantages of a conical shaped cup for use in an artificial hip device; "such statements make clear that the '589 patent discloses *only* conical shaped cups and nothing further"); *Ekchian v. Home Depot, Inc.*, 104 F.3d 1299, 1304, 41 U.S.P.Q.2D (BNA) 1364, 1368 (Fed. Cir. 1997) ("Since, by distinguishing the claimed invention over the prior art, an applicant is indicating what the claims do not cover, he is by implication surrendering such protection.")



Ex. 2001, ¶68. "Phishing attacks involve fraudulently capturing information from a user, for example, via a fake website, and then using such information to conduct unauthorized transactions." Id., 14:44-47. In a phishing attack, a user [yellow box] unknowingly provides information to a fake website [purple box] to transfer money to account #12345678, thinking that s/he is 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]). In order 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. Ex. 2001, ¶69. 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." In the example, the information displayed on the secure device of the user will indicate that the unconfirmed transaction seeks to transfer money to account #98345289 (as opposed to account #12345678 designated by the user). Ex. 2001, ¶69. "The user may then terminate any connection to the fake website." Ex. 1001, 14:62-63.

Again, it is clear that the defense against the phishing attack is based on information that is embedded (hidden) in the image. Ex. 2001, ¶70. 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. Ex. 2001, ¶70.

In summary, the '167 Patent discloses numerous embodiments. In every embodiment, the embedded information corresponds to information that is protected at least in part by being hidden in the image. Ex. 2001, ¶70. As explained above, if the information necessary to effect a secure 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). Ex. 2001, ¶71.

III. CLAIMS OF '167 PATENT

Claim 1 of the '167 Patent recites as follows:

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.

Independent claim 1 recites an image having "information embedded therein."

As noted above, in every embodiment disclosed in the specification, such embedded information corresponds to information that is hidden in the image. Ex. 2001, ¶73.

All other independent claims in the '167 Patent identically recite: "the image having information embedded therein."

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 (emphasis added); Ex. 2001, ¶74. 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; Ex. 2001, ¶74. The '167 Patent also explains that predetermined information is not "identification information" ⁴ 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"); Ex.

⁴ 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. Ex. 2001, ¶74, note 3.

2001, ¶74. All other independent claims in the '167 Patent identically recite storage of "predetermined information."

Independent claim 1 also recites that an output is generated "based on the information embedded in the image and the predetermined information." Thus, the 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; Ex. 2001, ¶75. 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."

Finally, independent claim 1 recites that "the output includes a digital 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 (discussed in Sections II(B)(5) and II(B)(6) above), where the confirmation signature is necessary for the transaction to be effectuated. *Id.*, 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"); Ex. 2001, ¶76. 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."

IV. Claim Construction

A. General Principles

1. The Construction That Stays True To The Claim Language And Most Naturally Aligns With The Specification Will Be The Correct Construction

Claim limitations are construed under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). Claim language is not read in isolation. *Id.*, 415 F.3d at 1315. "Ultimately, 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. The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Id.*, 415 F.3d at 1316, *quoting*, *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998).

2. Determining The Meaning Of A Claim Term Requires Examination Of Terms That Have A Particular Meaning In A Field Of Art

In many cases, "determining the ordinary and customary meaning of the claim requires examination of terms that have a particular meaning in a field of art."

Phillips, 415 F.3d at 1314. As the Federal Circuit has made clear, that "the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art." *Id.*, 415 F. 3d at 1312. It is "well-settled" that "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." *Id.*, 415 F. 3d at 1313 (citations omitted). "It is the person of ordinary skill in the field of the invention through whose eyes the claims are construed. Such person 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." *Id.* (emphasis added), citing, *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1477 (Fed. Cir. 1998).

Because the meaning of a claim term as understood by persons of skill in the art is often not immediately apparent, and because patentees frequently use terms idiosyncratically, the court looks to 'those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean.'" *Phillips*, 415 F.3d 1314, citing, *Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004). Those sources include "the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles,

the meaning of technical terms, and the state of the art." *Phillips*, 415 F.3d 1314 (citations omitted).

B. "The Image Having Information Embedded Therein" (All Claims)

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. Ex. 2001, ¶81. This is the correct construction for at least three reasons.

First, as discussed in detail 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. Ex. 2001, ¶82. Thus, Patent Owner's construction aligns with the specification.

Second, each independent claim recites that it is an apparatus or method "for providing a secure transaction."⁵ 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).

Ex. 2001, ¶83. As explained in *Pacing Techs., LLC v. Garmin Int'l, Inc.*, 778 F.3d 1021 (Fed. Cir. 2015), "[w]hen a patentee "describes the features of the 'present

⁵ 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"

invention' as a whole," he alerts the reader that "this description limits the scope of the invention." Thus, both the claim language and specification demonstrate that the claims are limited to techniques for providing a secure transaction. Ex. 2001, ¶84. Patent Owner's 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.

Third, the '167 Patent is directed to the field of secure transactions,⁶ 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. Ex. 2001, ¶85. As one author writing at the time 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

⁶ 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).

codes (Koch and Zhao, 1995), the wavelet-based embedding methods (Ohnishi and Matsui, 1996, Chae and Manjunath, 1998), the secure spread 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)(emphasis added).⁷

Another author writing at the time 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 (emphasis added).⁸

A further author writing at the time 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

⁷ "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, Ex. 2003, 1-2.

⁸ "Lossless Generalized-LSB Data Embedding," Celik, Mehmet Utku, et al., *IEEE transactions on image processing* 14.2 (2005): 253-266, Ex. 2004, at 1.

a close relationship to the cover image. The message supplies additional information 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. (emphasis added).⁹

Yet a another author writing at the time also referred "data embedding" in images 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. (emphasis added).¹⁰

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

⁹ "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, Ex. 2005, at 1-2.

¹⁰ *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, Ex. 2006, at 1.

watermarking technique. ... This paper proposes a novel approach to embed uncompressed 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. (emphasis added).¹¹

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, at 1 ("*Index Terms*—Arithmetic coding, conditional entropy coding, context modeling, data embedding, data hiding, least significant bit (LSB) modification, watermark"); Ex. 2008, at 1 ("*Index Terms*—Data hiding, digital watermarking, multilevel embedding, video data hiding.") Ex. 2001, ¶90.

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

¹¹ *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, at 1.

time of the '167 Patent used to describe hiding data or information in the image. Ex. 2001, ¶91.

C. "Predetermined Information" (All Claims)

The specification compels departure from the plain meaning of a claim term when the specification disavows or disclaims a particular feature. *Pacing Techs.*, 778 F.3d 1021, 1024, *citing*, *SciMed Life Sys.*, 242 F.3d 1337, 1341 ("disavowal requires that 'the specification [or prosecution history] make[] clear that the invention does not include a particular feature.'") Here, 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. Ex. 2001, ¶92. 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).

Here, the '167 Patent clearly distinguishes a "private key" from "other" information, such as "predetermined information" which may includes "address information, personal profile information and payment account information." Ex. 2001, ¶93.

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; Ex. 2001, ¶94. 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).

In referencing "predetermined information" and "identification information provided by a user," the '167 Patent refers to them as "other types" (plural) of information, which makes clear that "predetermined information" is a separate and distinct type of information than "identification information." Ex. 2001, ¶95.

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." Ex. 2001, ¶96.

D. "A Digital Signature To Be Used To Signify Authorization By The User With Respect To The Transaction" (Claims 1 And 23)

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 effectuated. 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 effectuate (or complete) the transaction. Ex. 2001, ¶97.

E. "Image Capture Device" / "Configuring A Portable Device To: Capture An Image" (Claims 1, 23 and 43)

The Petition asserts that the term “image capture device” should be construed as “any device that could capture an image, such as a barcode scanner.” Pet., 15. The problem with this proposed construction is that many barcode scanners are only capable of decoding the information in one-dimensional barcodes and cannot capture an image at all. Ex. 2001, ¶78.

At the time of the patent, linear barcode scanners could not 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 bar codes, matrix codes must be read with an image-based reader. They cannot be decoded by a laser scanner.” Ex. 2001, ¶79; Ex. 2011, 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. Ex. 2001, ¶79. 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.” Ex. 2001, ¶79. Decoded barcode data is merely the characters or numbers encoded in the barcode, and not a visual

representation of the barcode. Ex. 2001, ¶79. 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. Ex. 2001, ¶79.

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.” Ex. 2001, ¶80.

V. PRIOR ART RELIED ON IN PETITION

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 is discussed below.

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

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).

In contrast to earlier devices, in Wang such "identification data" remains within 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].

In one embodiment (the one relied on in the Petition), the PEAD is used as a "self-checkout terminal." Ex. 1004, [0115]; Pet., 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).

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]; Ex. 2001, ¶102.

B. Take An Order (TAO)

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, 1. Certain PalmOS devices compatible with the TAO software included a bar code scanner that the vendor could use to scan items to generate an order. *Id.* The software includes a popup which lets the vendor key in the customer's name, credit card number and expiration date. *Id.*, at 2. The software includes the capability to print receipts, quotations, invoices and delivery reports by connecting to a variety of printers. *Id.*, at 3. The reference does not disclose that the information stored in the bar codes is secured in any way. Ex. 2001, ¶103.

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

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., 28; *citing* Ex. 1008, [0246]-[0251], [0301] and [0307].

D. Palm Treo Manual (PTM)

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., 27, *citing*, Ex. 1006 at 24, 97, 109, 112, 129 and 173.

VI. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON THE MERITS

A. Ground 1 Does Not Have A Reasonable Likelihood Of Success

In Ground 1, the Petition alleges that independent claims 1, 23 and 43 are either anticipated by Wang, or obvious over Wang in view of Drummond. Pet., 29. For at least three reasons, the mappings in Ground 1 fail to demonstrate that all of the elements of independent claims 1, 23 and 43 are met by Wang alone or in combination with Drummond.

First, independent claims 1, 23 and 43 each recite: "the image having information embedded therein" (element [1a]). 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. *See*, Section IV(B), *supra*; Ex. 2001, ¶111. The Petition maps this claim element to the UPC barcode scanned by a user implementing Wang's self-checkout embodiment. *See*, e.g., Pet., 33, 38 and 43 (mapping elements [1a], [23a] and [43a] to Wang at [0115] which describes "scanning in the UPC code or barcode.") UPC codes (or

other bar codes used for store checkout) do not include information "embedded" in an image, i.e., information that is hidden in the image and used to provide security for the transaction, as required by independent claims 1, 23 and 43. Rather, the data stored in such bar codes can be decoded by anyone with a conventional barcode scanner using the public UPC standard. Ex. 2001, ¶¶113-114. For this reason alone, Ground 1 must fail.

Second, independent claims 1, 23 and 43 further recite a memory configured to store "predetermined information" (element [1b]) As explained above, the specification of the '167 Patent expressly disavows or disclaims a private key from the scope of "predetermined information," making clear that "predetermined information" corresponds to "other" information, such as, ... address information, personal profile information and payment account information." Ex. 1001, 6:8-22; Ex. 2001, ¶116. The mappings in Ground 1 are deficient because they purport to map the "predetermined information" to a private key - the very item which was disclaimed in the specification. See, e.g., Pet., 33-34 (mapping of element [1b]), 39 (mapping of element 23[b]) and 43 (mapping of element [43[b]), in each case asserting that Wang's "private key is predetermined information"); Ex. 2001, ¶¶117-121.

Third, 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" (element [1h]). 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 effectuate (or complete) the transaction. Ex. 2001, ¶131. In Ground 1, the Petition maps this limitation to a digitally signed receipt - but does not explain how a digitally signed receipt is to be used to signify authorization by the user of the transaction. See, e.g., Pet., 34 and 41 (stating only that "The PEAD user can sign the receipt electronically" but failing to explain how a signed receipt meets the claim language); Ex. 2001, ¶128. A digital signature created by a user would signify nothing more than that the user signed the receipt and that the receipt had not been modified since the signing. Ex. 2001, ¶131. However, it does not follow from the fact that the user has a signed receipt that the underlying transaction that led to the receipt was in fact authorized by the user, as claimed. 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. Ex. 2001, ¶133. Thus, with respect to independent claims 1 and 23, the mappings in Ground 1 are deficient for the further reason that they fail to demonstrate that Wang's signed receipt meets the claim language.

Each of the remaining claims challenged in Ground 1 depends from either independent claim 1 or 23. Under Ground 1, the Petition has failed to demonstrate a reasonable likelihood of success with respect to any these dependent claims because the Petition has failed to demonstrate a reasonable likelihood of success with respect to the independent claim from which each such dependent claim depends.

B. Ground 2 Does Not Have A Reasonable Likelihood Of Success

In Ground 2, the Petition alleges that independent claim 1 is anticipated by Wang. For at least three reasons, the mappings in Ground 2 fail to demonstrate that all of the elements of independent claim 1 are met by Wang.

First, with respect to the requirement in independent claim 1 that recites "the image having information embedded therein," the Petition simply refers back to its "Element 1a analysis" under Ground 1. *See*, Pet., 45 (mapping for Element [1a]). For the reasons set forth in Section VI(A), *supra*, Wang fails to meet this claim element. Ex. 2001, ¶138.

Second, Petitioner's mapping of independent claim 1 in Ground 2 is deficient with respect to the "predetermined information" recited in the claim. In connection with element [1f], the Petition alleges:

The transaction approval data is also based on predetermined information—specifically “user identification data.” ... The user identification data may include “the user’s name, his birth date, [or] his social security number...” [0045]. Thus, the transaction approval data

(output) is based on user identification data (**predetermined information**). Pet., 47 (emphasis in original).

As explained in Section IV(C), *supra*, the '167 Patent makes clear that "predetermined information" is a different type of information than identification information¹² provided by the user to verify or authenticate the user's identity. Ex. 1001, 6:55-66 ("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 the user.") Ex. 2001, ¶140-141. Simply put, the mapping in element 1[f] in Ground 2 fails because, in the context of the '167 Patent, Wang's "identification data" is not "predetermined information." Ex. 2001, ¶143-145.

In Ground 2, the Petition presents an alternative mapping of limitation "the output includes a digital signature to be used to signify authorization by the user with respect to the transaction" (element [1h]) to Wang's digitally signed receipt. See Pet., 47, Element [1f]. For the reasons set forth in Section V(A), *supra*, a digitally signed

¹² As explained in Section V(A), *supra*, like the '167 Patent, Wang refers to "identification data" as the data used to authenticate the user. Ex. 1004, [0004], [0045]; Ex. 1001, 6:1-7 and 6:22-23.

receipt does not signify that the underlying transaction that led to the receipt was in fact authorized by the user, as claimed. Ex. 2001, ¶150.

Each of the remaining claims challenged in Ground 2 depends from independent claim 1. Under Ground 2, the Petition has failed to demonstrate a reasonable likelihood of success with respect to any these dependent claims because the Petition has failed to demonstrate a reasonable likelihood of success with respect to the independent claim from which each such dependent claim depends.

C. Ground 3 Does Not Have A Reasonable Likelihood Of Success

In Ground 3, the Petition challenges independent claims 19 and 39, alleging that the claims are obvious over Wang in view of Drummond.

For claim elements [19a] and [19b], Ground 3 refers back to the mapping of elements [1a] and [1b] to Wang in Ground 1. *See*, Pet., at 52. For the reasons set forth in Section VI(A), *supra*, elements [1a] and [1b] are not met by Wang. Ex. 2001, ¶157.

For claim elements [39a] and [39b], Ground 3 refers back to the mapping of elements [23a] and [23b] to Wang in Ground 1. *See*, Pet., at 53. For the reasons set forth in Section VI(A), *supra*, elements [23a] and [23b] are not met by Wang. Ex. 2001, ¶158.

Each of the remaining claims challenged in Ground 3 depends from either independent claim 19 or 39. Under Ground 2, the Petition has failed to demonstrate

a reasonable likelihood of success with respect to any these dependent claims because the Petition has failed to demonstrate a reasonable likelihood of success with respect to the independent claim from which each such dependent claim depends.

D. Ground 4 Does Not Have A Reasonable Likelihood Of Success

In Ground 4, the Petition challenges dependent claims 8 and 30, alleging that the claims are obvious over Wang and Denso. Ground 4 is deficient because it fails to explain how the elements in the base claims (i.e., claim 1 is the base claim for claim 8, and claim 23 is the base claim for claim 30) are being mapped to the cited references. For example, it is not apparent whether the Petition is relying on its mapping of claim 1 as set forth Ground 1 or its mapping of claim 1 as set forth in Ground 2 in connection with the mapping of claim 8 in Ground 4. To the extent the Petition intended to rely on the analysis of claims 1 and 23 set forth in Ground 1 for the limitations in the base claim for claims 8 and 30, respectively, in Ground 4, the confusion is further complicated by the fact that the analysis of claims 1 and 23 in Ground 1 relies in part on Drummond, which is absent from Ground 4. Simply put, Ground 4 is deficient because it fails to set forth with sufficient clarity how it is mapping the claims to the prior art.

To the extent that the Petition is using only its citations to Wang (and not Drummond) for claims 1 and 23 from Ground 1 for the limitations in the base claim

for claims 8 and 30, respectively, Ground 4 is deficient because, for the reasons set forth in Section VI(A) above, Wang fails to disclose elements [1a], [1b] and [1h], and [23a], [23b] and [23h].

Claim 23 is not the subject of Ground 2, so there are no mappings to Wang in Ground 2 for the limitations in the base claim (claim 23) for dependent claim 30. To the extent the Petition is using its citations to Wang from claim 1 from Ground 2 for the limitations in the base claim (claim 1) for claims 8, respectively, Ground 4 is deficient because, for the reasons set forth in Section VI(B) above, Wang fails to disclose elements [1a] and [1h].

E. Ground 5 Does Not Have A Reasonable Likelihood Of Success

In Ground 5, the Petition challenges dependent claim 13 as obvious over Wang and Raines. In Ground 5, the Petition appears to rely on its mapping to Wang from Ground 2 for the limitations of the base claim (claim 1) from which claim 13 depends. Pet., at 57 ("As discussed in Ground 2, Wang discloses all of the features of Claim 1.") Ground 5 is deficient because, for the reasons set forth in Section VI(B) above, Wang fails to disclose elements [1a] and [1h].

F. Ground 6 Does Not Have A Reasonable Likelihood Of Success

In Ground 6, the Petition challenges independent claim 1, 23 and 43 as obvious over TAO in view of PTM and Wang. Ground 6 is deficient for at least three reasons.

First, independent claims 1, 23 and 43 each recite: "the image having information embedded therein" (element [1a]). 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. *See* Section IV(B), *supra*; Ex. 2001, ¶168. The Petition maps this claim element to the disclosure in TAO of a vendor scanning a product barcode to generate an order for a customer. Pet., at 65 (element [1a]). Similar to the UPC code scanned by the user in Wang, there is no disclosure in TAO that the product information in the bar codes is "embedded" in an image, i.e., that the information is hidden in the image and used to provide security for the transaction. 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. Ex. 2001, ¶¶168-169. For this reason alone, Ground 6 must fail.

Second, independent claims 1, 23 and 43 each require the capturing of an image. In this regard, claim 1 recites "an image capture device," and claim 23 and 43 recite "configuring a portable device to: capture an image." These limitations are not met by the mappings in Ground 6. In relation to the "image capture device" in element [1a] of Claim 1, the Petition (at 65) relies on TAO's barcode scanning capability, which TAO describes as follows:

Point-of-sale Software for the Palm Computing Platform

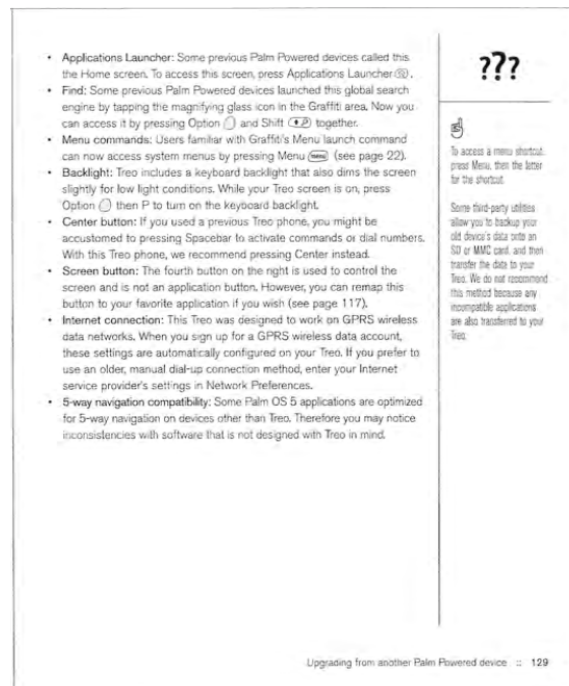
Are you selling products at trade shows or expos? Taking orders from customers in their home or office? Submitting bids or issuing quotations in a field situation? Delivering product and need to issue a receipt? For all these situations and more, **Take An Order! is the handheld tool you need.** Combined 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, at 1 (red underlining added); Ex. 2001, ¶172. In Ground 6, the Petition cross-references the mapping for element [1a] for element 23[a] and element 43[a] See, Pet., 68, 70. The SPT units from Symbol Technologies identified in TAO are not image capture devices. Rather, these devices were limited to linear scanning capabilities. See, e.g., Symbol SPT 1800 Series Product Reference Guide [Ex. 2009], at xi; Ex. 2001, ¶173. The Symbol SPT 1700 devices could only scan two-dimensional 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. Symbol SPT 1700 Series Product Reference Guide [Ex. 2010], at 17-8 to 17-9; Ex. 2001, ¶173. The linear scanning capabilities in the SPT device identified by TAO are clearly not capable of capturing an image as required by claims 1, 23 and 43 the '167 Patent. Ex. 2001, ¶173. Thus, the mapping advanced in Ground 6 is deficient because it lacks an "image capture device" (in claim 1) and "a portable device to: capture an image" (in claims 23 and 43.) Ex. 2001, ¶174.

Third, the Petition's mapping of element [1e] in Ground 6 is deficient. In Ground 6, the Petition (at 66) maps element [1e] to alleged password functionality in the Palm Treo. From the Petition:

[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.
---	--

However, page 129 of the Palm Treo Manual (reproduced below), and makes no mention of passwords:



Ex. 2001, ¶177. Elsewhere, the Petition cites page 24 of the Palm Treo Manual as disclosing certain password functionality. Pet., at 27 ("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.") However, page 24 of the Palm Treo Manual (reproduced below), and makes no mention of passwords:

Symbols and accented characters					
Type...	then press Alt to choose...	Type...	then press Alt to choose...	Type...	then press Alt to choose...
a	á â ã ä å æ	o	ó ô õ ö ø	0	% %%
A	Á Â Ã Ä Å Æ	O	Ó Ô Õ Ö Ø	1	¼ ½
b or B	ß	p or P	®	2	²
c	ç © ª « ¬ ® ¯	r or R	®	3	¾
C	Ç € º » ˆ ˜	s	ß š Š š	.	? ! ...
d	† ‡	S	ß š Š š	,	,
D	† ‡	t or T	™ † ‡	!	!
e	é ê ë ì	u	ú û ü	?	¿
E	É Ê Ë Ì	U	Ú Û Ü	:	: ; - () ~D
f or F	/	x or X	x □	'	' < > -
i	í î ï	y	ÿ ŷ	"	" " " "
I	Í Î Ï	Y	Ÿ Ŷ	\$	€ £ ¥ ¢
I or L	£			+	&
m or M	µ			-	- . = - -
n	ñ			/	% \ + /
N	Ñ			#	=
				(	< [{ .
				)	>] } .

Ex. 2001, ¶178. Simply put, the mappings in Ground 6 of elements [1e], 23[e] and 43[e] are deficient because the citations provided in the Petition fail to demonstrate any that the Palm Treo Device "Requires a **password to see any data ...**," as alleged in the Petition. *See*, Pet., at 66 (emphasis in original); Ex. 2001, ¶179.

Each of the remaining claims challenged in Ground 6 depends from either independent claim 1 or 23. Under Ground 6, the Petition has failed to demonstrate a reasonable likelihood of success with respect to any these dependent claims because the Petition has failed to demonstrate a reasonable likelihood of success

with respect to the independent claim from which each such dependent claim depends.

VII. CONCLUSION

For the above reasons, Patent Owner respectfully requests that the Board deny institution of the Petition.

Respectfully submitted,

Dated: November 20, 2024

By: /Daniel H. Golub/
Daniel H. Golub
Registration No. 33,701
Counsel for Patent Owner
Intellectual Ventures II LLC

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this Patent Owner Preliminary Response complies with the type-volume limits of 37 C.F.R. § 42.24(b)(1) because it contains 13,345 words, excluding the parts of this Patent Owner's Preliminary Response that are exempted by 37 C.F.R. § 42.24(a), according to the word processing system used to prepare this Patent Owner's Preliminary Response.

Respectfully submitted,

Dated: November 20, 2024

By: /Daniel H. Golub/
Daniel H. Golub
Registration No. 33,701
Counsel for Patent Owner
Intellectual Ventures II LLC

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** was served via email (as consented to by counsel) on November 20, 2024 to lead and backup counsel of record for Petitioners as follows:

Justin L. Krieger
Reg. No. 47,719
Kilpatrick Townsend & Stockton LLP
1400 Wewatta Street, Suite 600
Denver, CO 80202
Office: 303.405.1486
jkrieger@ktslaw.com

Darin J. Gibby
Reg. No. 38,464
Kilpatrick Townsend & Stockton LLP
1400 Wewatta Street, Suite 600
Denver, CO 80202
Office: 303.571.4000
dgibby@ktslaw.com

Nicoletta Kennedy
Reg. No. 68,161
Kilpatrick Townsend & Stockton LLP
701 Pennsylvania Avenue NW, Suite 200
Washington, DC 20004
Office: 202.639.4711
nkennedy@ktslaw.com

Torrey Spink
Reg. No. 72,641
Kilpatrick Townsend & Stockton LLP
1400 Wewatta Street, Suite 600
Denver, CO 80202

Office: 303.405.1486
tspink@ktslaw.com

Dated: November 20, 2024

By: /Daniel H. Golub/
Daniel H. Golub
Registration No. 33,701
Counsel for Patent Owner
Intellectual Ventures II LLC