UnifiedPatents

PATROLL Claim Chart Submission

U.S. Patent 7,314,167

U.S. Patent 7,314,167 ("*Intellectual Ventures*" or the "patent-at-issue") was filed on March 8, 2005, and claims priority on the same date. Claim 1 of the patent-at-issue is directed to a method an apparatus for providing secure identification, verification, and authorization. The apparatus includes an image capture device configured to capture an image, the image having information embedded therein, 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 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.

The primary reference, U.S. Patent 2005/0071283 ("*WMR*"), was filed on April 12, 2004, and claims an earliest priority date on May 25, 2000. The patent is directed to a system and method of securely processing an electronic transaction in which an image and data associated with the transaction are separately processed. The system and method includes a legally acceptable substitute record of the transaction being recreated at any step in processing; unauthorized access to the image, data, and/or substitute document being detectable; quality assurance of the image and data being provided; and participants in a network creating additional security for the transactions.

The secondary reference, U.S. Patent 7,207,477 ("*Diebold*"), was filed on March 8, 2004, and claims priority on the same date. The patent is directed to an apparatus and method of wireless transfer of account data and signature from a handheld device to an electronic check generator, for use of purchasing an item via a self-service checkout at a merchant store. The item is associated with a bar code and an anti-theft device. A customer uses their phone to establish communication with the store's transaction host. The phone includes a camera and a programmable memory. The memory includes customer account data. The camera is used to capture and transmit an image of the bar code to the host. The host determines the item's cost from the received bar code image. The customer can wirelessly transmit their account data from the phone to an in-store terminal. The terminal can transmit the account data to the host. The host can accent and use the account data in payment for the item. After customer payment for the item, the host causes the anti-theft device to be neutralized.

A sample claim chart comparing claim 1 of *Intellectual Ventures* to *WMR* and *Diebold* is provided below.

US-7314167-B1 (“*Intellectual Ventures*”)	**A. US-20050071283-A1** (“*WMR*”) **B. US-7207477-B1** (“*Diebold*”)
[1.pre] **An apparatus for providing a secure transaction, the apparatus comprising**:	**A. US-20050071283-A1** “[0002] The present invention relates generally to **electronic transaction processing, particularly to financial instruments and transactions translated into electronic format and associated procedures such as secure**, accurate and verified imaging of financial instruments, check truncation and electronic funds payment, settlement and clearing.” *WMR* at para. 2 “[0076] In an embodiment of the present invention, **the system allows for secure check truncation at the point of presentment or any other step in the item processing chain by creating a file containing an image of the check and a file containing transaction data** related to the paper check…” *WMR* at para. 76 “164. A **secured multi-function shared services network for processing an electronic transaction**…” *WMR* at claim 164 **B. US-7207477-B1** “In an exemplary form of the invention **security measures are provided to assure that only a proper authorized user is enabled to operate the system**.” *Diebold* at col. 11:47-49 “1. **Apparatus comprising…** **…a merchant transaction system**…” *Diebold* at claim 1
[1.a] **an image capture device configured to capture an image**, **the image having information embedded therein including information relating to a transaction**;	**A. US-20050071283-A1** “[0082] As shown in an embodiment depicted in FIG. 2, **a teller comprising an imager and optionally, means to input and view data, captures the check information and image, inputs additional information**, provides image and data quality assurance and exception processing, provides security, provides check and account status, and allow for inquiries, look ups, or recalls of any check image file previously captured at that teller. **The check image file and associated transaction information file and or the reintegrated image/data related to the paper check are all used in check processing**.” *WMR* at para. 82

	B. US-7207477-B1 “**The customer has a camera 302 which can communicate with the phone 300, e.g., the camera may be part of the phone (e.g., videophone)**. After the customer’s phone has established communication (step 400) with the store’s network host 310, **the purchaser points the phone camera at the bar code 320 corresponding to the item. An image of the bar code 320 (or data representative of the image) is captured and sent (step 402) to the transaction system (e.g., host) 310**. **The transaction system can resolve the bar code data and process the data to determine the price of the item corresponding to the bar code (step 404). For example, the transaction system may convert the digital image of the bar code to numerical data, and then make a comparison of this numerical data to price data to determine the item’s price**.” *Diebold* at col. 29:26-39
[1.b] **a memory configured to store predetermined information**;	**A. US-20050071283-A1** “155. A system for receiving and processing an electronic transaction comprising: an application… adapted to… 3) **store the image file and or the file comprising information associated with the document**…” *WMR* at claim 155 **B. US-7207477-B1** “…a portable hand-held customer device including **a programmable memory,** **wherein the memory includes financial account data stored therein,** **wherein the memory includes electronic signature data stored therein,** wherein the customer device is operable by a customer during a transaction with a merchant…” *Diebold* at claim 1
[1.c] **an input unit configured to receive input information provided by a user**; **a processor configured to**:	**A. US-20050071283-A1** “[0081] The depository bank also captures other checks as defined herein, including all documents from a driver’s license to a deposit slip that are also checked for quality and processed. **The collected information may be electronically derived from the imaging and or converted by other methods, such as but not limited to, inputting the information by a human via a computer terminal to create an electronic representation of the information, teller generated, such as creating an electronic deposit slip based on the transaction that is input directly, outputted to a second device, such as a line printer and manually inputted**

	into the imager, or hand written and scanned. Alternatively, the depository bank may transfer the paper check to an intermediary bank or to a payee bank which may gather the information, perform the imaging, and create the electronic data files." *WMR* at para. 81 "[0111] Images that meet the parameters set for image quality are validated 370. A QA digital signature and or watermark unique to the paper check, process, capture environment, and or **processor** is generated and associated with the image file…" *WMR* at para. 111 **B. US-7207477-B1** "The portable terminal also includes **an input device which enables the user to select data from the card memory corresponding to any one of the plurality of the user's accounts**." *Diebold* at col. 4:47-50 "The card memory may also include data representative of instructions which are used by **a processor in the portable terminal for carrying out transactions**." *Diebold* at col. 5:18-22
[1.c.i] **verify the user based on the input information to ensure that the user is authorized to use the apparatus**; and	**A. US-20050071283-A1** "[0225] Security functions implemented by the Integration Node include **1) authentication: PKI Digital Certificates are issued and managed via the integration nodes in the shared services network. All requests and responses from integration nodes are digitally signed and verified with a certificate unique to that integration node; 2) authorization: all integration node request and response activities are verified against a known service definition specific and unique to the participants**…" *WMR* at para. 225 **B. US-7207477-B1** "**It is a further object of an exemplary form of the present invention to provide a transaction apparatus that authorizes operation based on a physical characteristic of an authorized user**." *Diebold* at col. 3:46-49 "FIGS. 89-95 show screens displayed on the portable terminal and associated with the logic flow for **assuring that a user is authorized to use the terminal**." *Diebold* at col. 6:37-39

	"**The user could display a reproduction of their signature on the screen of the terminal so that a merchant could verify the signature**." *Diebold* at col. 18:25-27 "**Such indicia may also be transmitted by the terminal to a remote system and used to verify the authenticity of a transaction or for other purposes**." *Diebold* at col. 21:12-15
[1.c.ii] **generate an output based on the information embedded in the image and the predetermined information**; and	**A. US-20050071283-A1** "[0133] Image Capture Format (ICF) is the image file format used for image capture and manipulation. ICF is specific to the capture device and typically not available to any outside system. **The final output from the image capture device is the same as the image storage format and optionally includes meta data about the image, capture device, operating environment and the like**." *WMR* at para. 133 **B. US-7207477-B1** "**Display component 40 includes display 22 as well as the other hardware and software devices which enable the display to provide visual outputs in response to processor 36**." *Diebold* at col. 8:27-30 "**The processor 36 of the portable terminal 14 carries out instruction steps in response to the inputs provided by the user of the card and portable terminal**." *Diebold* at col. 10:51-54 "**In screen 118 shown in FIG. 28 if the user presses the enter button 28 as schematically indicated therein the terminal next displays screen 120 shown in FIG. 29 in which the terminal outputs an indication that the card has been deleted**." *Diebold* at col. 16:22-26
[1.d] **an output unit configured to forward the output generated by the processor**, wherein	**A. US-20050071283-A1** "…**The central server 240 uses configurable sorting and routing algorithms to forward the transaction file, the image file, and or the reintegrated image/data file to one or more targets, such as a validation service 270**…" *WMR* at para. 196 **B. US-7207477-B1** "As the remote terminal exchanges messages with the remote locations to transfer the funds after the connection has been made, **the display of the remote terminal may present the screen 202 shown in FIG. 70 to indicate that the transaction is going forward**." *Diebold* at col. 23:23-27

	"If the user has first identified themselves with an access code or biometric data to operate the terminal with the card, **the level of security may be considered already sufficient that the PIN may be recalled from memory and forwarded by the terminal**." *Diebold* at col. 24:56-61 "For example, **the neutralizer can have an output device that can display the latest identifier sent from the transaction system (e.g., host)**." *Diebold* at col. 31:21-24
[1.d.i] **the output includes a digital signature to be used to signify authorization by the user with respect to the transaction**.	**A. US-20050071283-A1** "[0111] **Images that meet the parameters set for image quality are validated 370. A QA digital signature and or watermark unique to the paper check, process, capture environment, and or processor is generated and associated with the image file. The QAVC or a derivative is used as the QA stamp of acceptance and may be encoded in the digital signature along with other unique data**." *WMR* at para. 111 "[0196] **The central server 240 validates signature on the file containing digital signature on the transaction file 250 and the digital signature on each item in the file to verify that tampering has not occurred between transmission endpoints**…" *WMR* at para. 196 "…**The application digitally signs each file and or the data, and optionally stores the image file and or the associated information file. The application is capable of sending the separate files to a server in real time or as determined by the synchronization agent. When the files arrive at the server, the digital signatures are validated**…" *WMR* at para. 223 **B. US-7207477-B1** "For example in some embodiments scanner 50 may be a scanner suitable for scanning and **reading written indicia. This may include the signature of an authorized user**. Data representative of such a signature may be input and produced with the scanning device and stored in the programmable memory of the card. **The signature may then be reproduced on the display or transmitted to a remote location for purposes of identifying the authorized user or the authenticity of a transaction**." *Diebold* at col. 9:30-38