

for a transaction, with the transaction requiring a signature, the card reader/writer **174** obtains any necessary transaction information previously written onto the card **184** (i.e. account data, PIN data, and other data, or "obtained data") including the URL of the web encrypted, graphically encoded electronic signature in the database **180**. Preferably, the consumer then enters his/her PIN on a PIN entry keypad **196** of the transaction payment terminal **172** to provide authenticity for the user of the card **184**. A correct PIN allows the transaction payment to proceed, while an incorrect PIN ceases the transaction.

[**0064**] Assuming the correct PIN entry, the obtained data is used to process payment and other functions. The obtained URL allows the transaction payment terminal **172** to obtain the web encrypted, graphically encoded electronic signature from the database **180** via the network **178** (or alternatively, from the database **182**). The transaction payment terminal **172** then de-encrypts and graphically de-encodes the web encrypted, graphically encoded electronic signature to obtain a "reproduced original" of the signature and provides the reproduced original signature on a paper receipt printed by a printer **212** without the user having to provide the signature. In addition, digital receipt program instructions **206** are used to generate a digital receipt that is also stored either in the database **182** or the database **180**, and may be electronically forwarded to the consumer via their e-mail address which may be part of the other data of the card **184**. The digital receipt includes either the web encrypted, graphically encoded electronic signature or the reproduced original.

[**0065**] Referring now to **FIG. 10A**, there is depicted a flow diagram, generally designated **220**, depicting an exemplary manner in which an "initial" phase of an aspect of the present invention is accomplished. In particular, before a consumer can utilize a card as described above with reference to **FIGS. 8 and 9**, the consumer's signature must be obtained. The consumer's signature is obtained on a signature capture device (SCT) such as those shown and described herein, block **222**, in a manner also described herein in conjunction with the description of the SCT. The captured signature is then graphically encoded according to a graphics encoder, block **224**. Thereafter, the encoded signature is encrypted with a web (Internet) encryption method, block **226**.

[**0066**] The encoded and encrypted signature is then stored in a storage device, block **228**. The storage device is preferably a data warehouse that is in communication with the Internet. As such, each storage location in the data warehouse has an Internet address or URL. Once the encoded and encrypted signature is stored at a storage location within the storage device, the address (e.g. URL) of the storage location is obtained, block **230**. Once the storage location is obtained for the encoded and encrypted signature, the address is written onto/into a user's card, block **232**.

[**0067**] Referring now to **FIG. 10B**, there is depicted a flow diagram, generally designated **240** of a manner of using a card onto which the address of the encoded and encrypted signature has been stored. A transaction requiring a signature and/or card is initiated on a transaction payment terminal, block **242**. At the appropriate point in the transaction, the user's card is read by the transaction payment terminal, block **244**. Reading the user's card obtains the address (e.g.

URL) previously stored thereon, in addition to obtaining other data required for the transaction. In order to verify or authenticate the transaction (i.e. whether the cardholder is the owner/authorized user), the user enters his/her PIN, block **246**. Correct entry of the PIN, provides authorization to proceed with the transaction.

[**0068**] The transaction payment terminal logs onto the address obtained during reading of the card, block **248**. The encoded and encrypted signature is retrieved by the transaction payment terminal from the storage location specified by the address obtained from the card, block **250**. Thereafter, the encoded and encrypted signature is decrypted and decoded to obtain the original signature (i.e. an electronic representation of the original signature), block **252**. The original signature is then printed onto a paper receipt, block **254**, when the transaction is complete. In addition, the signature is appended to a digital receipt generated from the transaction that is then stored in a storage device, block **256**.

[**0069**] With reference now to **FIG. 11**, there is depicted another embodiment of a signature capture terminal (SCT) generally designated **260**. In particular, but in general terms, the SCT **260** is operative to accept entry of a PIN for transactions requiring a PIN via a disability access device. The entry of a PIN via the disability access device is preferably accompanied by the production of secure audio. Other data may be entered into the SCT **260**, preferably via the disability access device, in response to menu choices presented by the SCT **260**.

[**0070**] The SCT **260** is characterized by a housing **262** that supports a screen or display **264**. The screen **264** is a touch screen, sonar screen, or the like, in like manner to the screen **34** of the SCT **30**. The screen **264** forms, at least in part, a signature capture area. A stylus for writing onto the screen **262** is provided, retained when not in use within a tray **267**. Raised alignment tabs **268** are disposed on both sides of the screen **264** preferably in the middle (relative to vertical direction) thereof. The alignment tabs **268** include indicia such as Braille for a tactile indication of their presence. The alignment tabs provide boundary markers for the screen/signature capture area **264**.

[**0071**] The SCT **260** includes speakers **270** and an audio jack **272** to which may be coupled a set of headphones **274**. A volume control **276** is provided that is operative to raise and/or lower the volume of the speakers and any headphones connected to the audio jack **272**. A card reader **278** is also provided that is operative to read a magnetic strip type card, a smart card, RFID type card, or the like. In accordance with an aspect of the present invention, the SCT **260** includes either an integral disability access device **280** or an external disability access device **288**. The integral disability access device **288** and external disability access device **288** are the same with the exception that the external disability access device **288** includes an interface cable **290** that is adapted to be accepted (i.e. plug into) the port **286**. Preferably the port **286** is a Universal Serial Bus (USB) port and thus the interface cable **290** is configured accordingly including a USB termination plug (not shown). The integral disability access device **280** includes three (3) buttons, an Up button (an "up" triangle) **282**, a Down button (a "down" triangle) **283**, and an Enter button (a diamond) **284**. In like manner, the external disability access device The disability access devices **280** and **288** are designed to allow a user with a