

## TOUCH PAD THAT CONFIRMS ITS SECURITY

### RELATED APPLICATIONS

[0001] This application claims the benefit of the following application:

[0002] U.S. patent application Ser. No. 60/252,800, entitled, "A Touch Pad that Confirms its Security," filed Nov. 21, 2000, naming G. F. R. Sulak Soysa et al. as inventors, with Attorney Docket No. A-70049/MAK/LM and commonly assigned to @pos.com, Inc. of San Jose, Calif.

[0003] U.S. patent application Ser. No. 60/252,800 is incorporated by reference herein.

[0004] This application is related to:

[0005] U.S. patent application Ser. No. 09/588,109, entitled, "Secure, Encrypting PIN Pad," filed May 31, 2000, naming James C. Lungaro, Susan W. Tso, Llavanya Fernando and Simon Lee as inventors, with Attorney Docket No. A-68938/MAK/LM and commonly assigned to @pos.com, Inc. of San Jose, Calif.

[0006] U.S. patent application Ser. No. 09/588,109 is incorporated by reference herein.

[0007] This invention relates to the touch pads, display, touchscreens and secure data entry. More particularly, the invention relates to confirming to the user the security of data to be entered on a touch pad during, for example, a consumer transaction.

### BACKGROUND

[0008] All of the credit- and debit-card companies are experiencing high levels of fraud, including Visa International, MasterCard International, American Express Company and Discover Bank. The ease of circumventing the hardware or software security of a PIN entry device has contributed to this fraud over the last ten years. Visa and MasterCard project an increase of annual losses on credit and debit cards of \$843.2 million in 2001 to \$2.13 billion by 2010. Accordingly, the payment companies are requiring stricter security—both physical and logical—for payment devices.

[0009] Older conventional devices for debit transactions are physically and logically secure. Tamper-detect switches inside a device including a casing erase valuable information if the casing is broken. Security grids and ruggedized security shrouds prevented drilling into the device. Logical security measures manage cryptographic keys (to encrypt PIN numbers) and transaction data within the device. Additionally, the logical security ensures message authentication coding during message transit.

[0010] The advent of reliable and less expensive LCD and touchscreen technologies brought the corresponding evolution of newer payment devices that incorporated the technologies—payment terminals, personal digital assistants (PDAs), and Internet appliances, for example. These newer devices enable customers to interact with the devices during transactions. However, the transactions from such devices are not as secure (physically or logically) as those from the older devices.

[0011] One such newer device is the iPOS TC transaction terminal available from the Assignee of the instant invention. The iPOS TC is a web-enabled payment device for secure debit and credit transactions. Dual channels securely simultaneously transmit electronic transaction and signature data on one channel and advertising and promotional media from the World-Wide Web (the web), on the other.

[0012] These newer devices are more programmable and have more functionality than the older conventional devices. Because of their status on the web, however, they are increasingly susceptible to attacks by hackers. These malfeasants may re-program the device, for example, to make information normally encrypted appear in the clear or to display rogue keypads, thus compromising security.

[0013] Accordingly, there is a need in the art for a payment device that protects against a user entering information on a rogue keypad, thus reducing the chances of fraudulent activity from the device.

[0014] These and other goals of the invention will be readily apparent to one of ordinary skill in the art on reading the background above and the description below.

### BRIEF DESCRIPTION OF THE DRAWINGS

[0015] **FIGS. 1 and 2** illustrate the touch pad of a payment device, according to one embodiment of the invention.

[0016] **FIG. 3** illustrates the circuitry of a payment device, according to one embodiment of the invention.

[0017] (The drawings are not to scale.)

### DESCRIPTION OF THE INVENTION

[0018] **FIG. 3** illustrates the circuitry **3** of a payment device according to one embodiment of the invention. The circuitry **3** includes a microprocessor **31**, an encryption circuit **32**, a MSR circuit **33**, a signature-capture circuit **34**, first and second display controllers **35**, **3B**, a touch-pad controller **36**, a security-icon display **37**, a touch pad **1** and a (general) display **39**.

[0019] The microprocessor **31** communicatively couples to the encryption circuit **32**, the MSR circuit **33**, the signature-capture circuit **34** and the display controller **35**. The encryption circuit **32** communicatively couples with the display controller **3B** that itself communicatively couples with the security display **37**. The display controller **35** and the (general) display **39** communicatively couple. The encryption circuit **32** communicatively couples with the touch pad controller **36** that itself communicatively couples with the touch pad **1**.

[0020] U.S. patent application Ser. No. 09/588,109 describes an encryption circuit **32**. That encryption circuit **32** may include a CPU, a memory, a touch-pad interface and a POS-system interface (all not shown here). The memory of the encryption circuit **32** may be programmed to perform the invention as described herein, including receiving, converting and encrypting input from the controller **36**. Alternatively, the encryption circuit **32** may include an application-specific integrated circuit (ASIC) or other hardware for performing encryption.

[0021] The controllers **32**, **33**, **34**, **35** and **36** are preferably within a single chip **3A** (which also has a microprocessor as