

**SYSTEM AND METHOD FOR PROTECTION
AGAINST SKIMMING OF INFORMATION
FROM CONTACTLESS CARDS**

CROSS-REFERENCE TO RELATED
APPLICATION

[0001] This application claims the benefit of U.S. provisional patent application No. 60/667,864 filed on Apr. 1, 2005, which provisional patent application is hereby incorporated by reference herein in its entirety.

BACKGROUND OF THE INVENTION

[0002] This invention relates to payment cards that are used for making contactless payment transactions. In particular, the invention relates to techniques for fraud prevention in proximity, contactless or smart card payment systems.

[0003] Proximity payments are used in situations where, although the purchaser is present, it is useful or at least more convenient to be able to make a payment without having to make physical contact with the vendor/payee. The purchaser, for example, may use a contactless "smart card" to make a proximity payment without having to manually swipe a card through a conventional point-of-sale device (i.e., a magnetic strip card reader). An exemplary contactless smart card is MasterCard PayPass™ card. This card is an enhanced payment card that features a hidden embedded microprocessor chip and antennae (i.e. a miniature Radio Frequency (RF) transceiver chip and an antenna). The MasterCard PayPass provides a purchaser with a simpler way to pay. The purchaser can simply tap or wave his or her MasterCard PayPass payment card on a specially equipped merchant terminal that then transmits payment details wirelessly using radio frequency signals, eliminating the need to swipe the card through a reader. Account details are communicated directly to the specially equipped merchant terminal and are then processed through MasterCard's highly trusted acceptance network. Moments after the purchaser taps the terminal with his or her MasterCard PayPass card, they receive payment confirmation and are on their way.

[0004] Proximity payment systems based on smart cards (such as MasterCard PayPass) may be advantageously implemented in traditional cash-only environments where speed is essential, (e.g., quick serve and casual restaurants, gas stations and movie theaters). Purchaser information, which may be stored in a microchip on the smart card, is sent directly from the microchip to a point-of-sale (POS) device or other wireless reader device, which may be up to about 10 cms away. Proximity payments also may be made using other payment devices (e.g., a mobile phone, PDA, or handheld computer), which are suitably configured to carry a microchip that stores and retransmits stored or processed account information when required. Common industry infrared or wireless protocols (e.g., Bluetooth) may govern communication between the payment device and the vendor/payee's wireless reader or POS device.

[0005] As with electronic payment transactions conducted over the Internet and other e-commerce transactions, both parties to a proximity payment transaction will have security concerns. Payers need reassurance that the vendor/payees are not unscrupulous criminals who will misuse payer information, the vendor/payees need to know that the payers are legitimate and both parties need to know that unauthorized third parties cannot intercept the transaction information. A

number of techniques, which address at least some of these security concerns, are available. Data encryption techniques, for example, can be used to secure transaction information during transmission.

[0006] The proximity and smart card payment systems take advantage of the new on-card chip technology to deploy cardholder verification methods to make secure transactions. Purchases made with the cards can be verified, for example, uses of a personal identification number, or PIN. The proximity and smart cards aim to cut fraud by including an on-card microchip, which can store more information than the usual magnetic strips, and also by having users verify transactions by keying in a personal identification number (PIN) rather than signing a receipt. However, as with any technology, the security provided by on-card chip technology is not infallible. Fraudsters can find new ways of illegally accessing cardholder information to breach security.

[0007] Consideration is now directed toward improving schemes for safeguarding cardholder information to prevent, for example, fraudulent use of stolen or lost payment cards. In particular, attention is directed to securing the information contained in proximity, contactless or smart payment cards.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Further features of the invention, its nature, and various advantages will be more apparent from the following detailed description and the accompanying drawings, wherein like reference characters represent like elements throughout, and in which:

[0009] FIG. 1 is an illustration of an exemplary mailer having RF-shielding material, which is designed to interfere with intruding RF-signals from communicating with an enclosed payment card having an on-card microchip, in accordance with the principles of the invention.

DESCRIPTION OF THE INVENTION

[0010] In accordance with the present invention, a system and a method are provided for safeguarding cardholder information stored in proximity, contactless or smart cards. The system and a method involve transporting the cards in RF-shielded environments that prevent unauthorized RF intrusion or access to the on-card chip circuits. The invention advantageously further reduces opportunities for fraud in payment-by-card systems.

[0011] The advantages of the invention may be understood with reference to counterfeiting, which is a type of card fraud that is prevalent with current electronic or paper payment systems that are based, for example, on plastic cards in which magnetic stripes or embossed structures contain cardholder information. A counterfeit card is one that has been printed, embossed or encoded without the consent or knowledge of the card issuer, or one that has been validly issued but has then been altered or recoded. A common method of counterfeiting is called skimming, in which the counterfeiters copy the information stored in the magnetic stripes on plastic cards. The counterfeiter copies the information stored in the magnetic stripe, for example, by swiping it through a small card reader. Armed with this information, the counterfeiter can then produce counterfeit cards and use them to carry out fraudulent transactions.

[0012] Proximity, contactless and smart cards in which computer chips are embedded hold more information, but in a more secure environment, than can be stored magnetic