

## FIGHTING IDENTITY THEFT: LESSONS FROM THE UNITED KINGDOM

### Introduction

Credit card fraud is the most common identity theft complaint reported to the Federal Trade Commission (FTC).<sup>1</sup> AARP analysis of previous FTC complaint data found that complainants age 50 and older were more likely to report being victimized by this form of identity theft than those under the age of 50.<sup>2</sup> For this reason, finding new techniques to combat credit card fraud is an important step in protecting older consumers from identity theft.

APACS, the United Kingdom (UK) payments association representing card issuers, established a new industry standard in 2004 to reduce the amount of “plastic card” fraud in the UK.<sup>3</sup> This standard, called “chip and PIN,” involves embedding a microchip inside credit and debit cards and requiring that consumers use a secret four-digit personal identification number (PIN) to complete a transaction. Previously, credit cards in the UK were similar to those used in the United States, consisting of a magnetic strip that is swiped through a magnetic reader during a transaction, after which the consumer signs his or her name on a receipt to verify the transaction.

Early indications suggest that the chip and PIN method has resulted in substantially less card fraud in the UK.<sup>4</sup> Similar technology used in France has been credited with reducing card fraud in that country by 80 percent.<sup>5</sup> While these results have been encouraging, a number of concerns remain about the chip and PIN system.

<sup>1</sup> Federal Trade Commission. Consumer Fraud and Identity Theft Complaint Data January–December 2005 (January 2006).

<sup>2</sup> N. Walters. “Identity Theft: An Update on the Experience of Older Complainants.” AARP Public Policy Institute. DD 102 (October 2004).

<sup>3</sup> Plastic card fraud is a term used in the UK to refer to fraud involving both credit and debit cards.

<sup>4</sup> APACS. “UK Card Fraud Losses in 2005 Fall by £65m—to £439.4m from £504.8m in 2004” (March 6, 2006). <http://www.apacs.org.UK>

<sup>5</sup> BBC News. “‘Chip and PIN’ Security Warning.” (December 18, 2004).

### The Chip and PIN System

To use a card containing chip and PIN technology, a consumer places the card into a reader (often called a PIN pad), which accesses the embedded microchip on the card. The card reader verifies the card as authentic, and the consumer then inputs his or her four-digit PIN, which is checked against the PIN stored on the card. If both PINs match, the transaction is completed. This method does not work for transactions carried out over the telephone or Internet, or for mail order purchases where the consumer is not present at the point of sale.

Introduction of the chip and PIN system is credited with the decline in several types of credit card fraud in the UK, including counterfeit card fraud and account takeover fraud.<sup>6</sup> On the other hand, “card not present fraud” (that is, credit card fraud through the Internet, phone, or mail order) has seen a substantial rise since the introduction of chip and PIN (Chart 1).

**Chart 1:**  
**Change in Card Fraud Losses on UK-Issued Cards between 2004 and 2005**

Fraud Type	Change from 2004 (£)
Counterfeit card fraud (skimmed/cloned)	-25%
Fraud on stolen/lost cards	-22%
Card not present fraud (Internet, phone, mail)	+21%
Fraudulent applications <sup>7</sup>	-5%
Account takeover	-24%
<b>Total</b>	<b>-13%</b>

Source: APACS. “UK card Fraud Losses in 2005 Fall by £65m—to £439.4m from £504.8m in 2004” (March 6, 2006)

<sup>6</sup> Startups.co.UK. “Fraud Falling Under Chip and PIN.” *The Register* (March 14, 2006). <http://www.theregister.co.UK>

<sup>7</sup> Providing fraudulent information when applying for a card.

## Concerns about Chip and PIN

Critics of the chip and PIN system in the UK have expressed a number of concerns about the system. One is that thieves will “shoulder-surf” to collect PINs of consumers entering their PIN information during a transaction. Because many PIN pads are placed in a position that makes them easy to see, critics worry that it will be easy to ascertain a consumer’s PIN as he or she completes the transaction. Further, cameras commonly used by store security can view these transactions. Because some consumers may use the same PIN for more than one card, discovering the consumer’s PIN could compromise more than one of the consumer’s financial accounts.

For this type of theft to occur, the thieves would then have to steal the actual card containing the microchip from the victim. Some fear that this could result in physical harm to the consumer. However, because most card counterfeiters rely on technology to commit fraud on a large scale, they are probably unlikely to resort to physical confrontations with individual cardholders.<sup>8</sup> Further, such theft would likely be reported immediately and result in the card’s being reported as stolen and deactivated before a thief would have had time to use it.

Another concern is the security of the data the PIN pad machines gather. Some PIN pads (such as mobile PIN pads, often used at restaurants) are wireless, since the pad must be brought to the customer; these PIN pads transmit transactional data over wireless networks, which are vulnerable to eavesdropping. In the United States, this problem is believed to be responsible for leaking card information and PINs in several retail stores.<sup>9</sup> While the cards involved did not have embedded microchips as they do under the chip and PIN system, the incident highlights the

vulnerability of data transmitted over wireless networks.

A final concern is that the chip and PIN system will not reduce fraud, but simply redirect thieves into different types of fraud. Indeed, there was a significant increase in card not present fraud after deployment of the chip and PIN system in the UK (see Chart 1). It is possible that reductions in the amount of card fraud will result in increases in other types of non-card-based identity theft. Because card fraud tends to be the easiest for consumers to deal with, an increase in other types of identity fraud could result in consumers being exposed to frauds that are more difficult to address (such as opening new accounts or loans using a victim’s name).

## Summary

The chip and PIN system has been effective in reducing several types of card fraud in the UK and other countries where similar technology is used. Despite the concerns about this technology, reducing the amount of card fraud may also reduce the number of identity theft victims in the United States. While the chip and PIN system is not a comprehensive solution to the threat of identity theft, the United States should monitor the progress of this technology in other countries as it seeks to craft new privacy solutions to address identity theft.

*Written by Neal G. Walters  
AARP Public Policy Institute  
601 E St., NW  
Washington, DC 20049  
202-434-3910; E-Mail [ppi@aarp.org](mailto:ppi@aarp.org)  
June, 2006  
© 2006 AARP <http://www.aarp.org/ppi>  
Reprinting with permission only.*

<sup>8</sup> A. McCue. “‘Shoulder-surfing’ Chip and PIN Fraud Fear Dismissed: Card Counterfeiters Won’t Turn to Mugging Old Ladies, Claims APACS.” Silicon.com (November 8, 2004).

<sup>9</sup> B. Sullivan. “ATM Theft Investigators Eye Software Flaw: Hackers May Have Plucked PIN Codes, Encryption Key Out of Thin Air.” MSNBC.com (March 22, 2006).