

White Paper

Examining cardholder authentication via ATMs and EFTPOS systems

by **Steve Gold**

Author	Steve Gold
Date	27 February 2008
Copyright	© Gridsure 2008



Gridsure Limited
Orchard House, Heath Road
Warboys, Cambs PE28 2UW

■ T: +44(0)870 7741404
■ e: info@gridsure.com
■ www.gridsure.com

Registered in England and Wales
No. 6018375
VAT No. 904250068



The latest European ATM Crime report¹ claims to show that, across Europe as a whole, ATM fraud dropped 55 per cent during the second half of 2006, compared to figures a year earlier. The driving force behind the significant reduction in fraud is the increasing adoption of EMV smart card standard at a growing number of ATMs, but delving into the report reveals that fraudsters are now diverting their efforts to physical attacks on ATMs, which are up by 60 per cent, and those ATM families/countries that continue to use magnetic stripe technology. More than anything, the report highlights the often-repeated assertion that card fraudsters tend to favour those frauds which require less preparation and have a lower chance of their being caught.

This perhaps explains why three recently reported card scams – on the London Underground; at a cluster of Liverpool garage forecourts; and a rash of ATM skimming in Ireland – have centred on the use of automated technology to harvest the required card details and their associated PINs.

A range of scams

In the London Underground scam of November 2007², fraudsters were found to have fitted more than 50 skimming devices – which harvest card and associated PIN details – to various Transport For London Oystercard/Travelcard machines across the `tube' network.

Police discovered that around 58 ticket machines had been tampered with and 27 skimming devices were recovered from several tube lines, notably the busy Piccadilly (for London Heathrow) and District (covering the more affluent areas of London).

Police are reported to have arrested two people installing a skimming system on a tube ticket machine during October, following which a raid on their address generated a haul of skimming machines and card reading equipment.

Earlier in November³, police discovered a network of tiny cameras hidden in the ceilings of a number of BP garages across the Wirral, one of the more affluent areas of Merseyside.

Police started investigating the large-scale fraud after they received reports of numbers of cards being `skimmed' at a shop in Greasby in June, 2007. The fraud trail quickly led them to a local BP garage.

Four people have been arrested and bailed in connection with the fraud technique which is reported to have been used a number of garages in the area.

After harvesting card details from the relevant machines and videoing PIN pad usage, the fraudsters are said to have withdrawn money and made purchases using cloned cards in London, Thailand and across the Far East.

In late October in Nenagh, Co. Tipperary, meanwhile⁴, Irish police say that thousands of euros were stolen from at least 40 credit and bank card accounts of customers after an ATM there was fitted with a skimming unit.

¹ www.eas-team.eu.htm

² <http://www.thisislondon.co.uk/standard/article-23421006-details/Fraudsters%20use%20Tube%20machines%20to%20clone%20bank%20cards/article.do?expand=true>

³ <http://www.liverpoolecho.co.uk/liverpool-news/local-news/2007/11/08/cameras-used-in-garage-cash-scam-100252-20078632/>

⁴ <http://www.kilkennyadvertiser.ie/index.php?aid=8196>

Police, who say that the details of 40 cards used at a Bank of Ireland ATM were recorded and used for cloning purposes in a 37-minute period on October 13, 2007, report that the professional criminals performing these types of fraud tend to originate from Eastern Europe and African nations.

Common denominator

The common denominator amongst these frauds is the fact that customer card details were lifted from the magnetic stripe of the cards concerned and PINs, where appropriate, were recorded by a skimming device and/or a video camera.

Whilst the banks and other institutions are busy upgrading ATMs and retail EFTPOS devices to use the EMV smart chip identifiers from relevant plastic cards, rather than the older magnetic stripe technology, the process will take several years to extend to all retailers and cash machines across Europe.

And that is before the roll-out of the technology is considered for other areas of the world, notably North America and the Far East, where smart card usage at EFTPOS terminals, let alone ATMs, remains in the minority.

Because of this, it is clear that the anti-card fraud efforts by the relevant authorities must concentrate on the customer authentication side of the transactions, which include checking signatures, PINs and other information.

It is now well known in the card industry that signatures can be forged, but PINs are arguably less secure, as witnessed by the three recent card frauds identified earlier. As long as the industry has to rely on legacy magnetic stripe technology, the customer authentication side of the transaction, whether at an ATM or using a retail EFTPOS system, remains a weak link.

Anecdotal evidence compiled from various photocard technology schemes around the world, notably by the Royal Bank of Scotland in the UK over the last two decades, suggests that retail staff rarely check the holder's on-card photo with that of the user.

Perhaps worse, because many retailers no longer handle a customer's card when they visit their establishment and make a purchase, staff cannot even verify the sex of the customer with the name on the card.

Against this backdrop, the ATM and card processing industries are busy implementing a number of new technologies to counter fraud within specific card usage segments. Diebold, for example, has released a new ATM card skimming technology⁵ for its Opteva range of cash and associated ticket dispensing machines.

The firm says that the fraud-deterrence technology centres around the use of a SAFE (Secure Anti-Fraud Enhanced) sensor that can detect a skimming attachment placed in front of a card slot. Coupled with environmental factors and cardholder activity analysis, the company claims the system is proof against triggering false alarms and automated ATM shutdowns.

⁵ <http://www.diebold.com/news/newsdisp.asp?id=3354>

VeriFone is also joining the technology bandwagon to beat the fraudsters, unveiling a new solution for card 'payments at the pump' that meets the latest PCI (Payment Card Industry) security standards.

Known as Secure PumpPAY⁶ this has already been deployed at initial test sites across Europe, the Middle East, Asia and the Far East with, says Verifone, considerable success in reducing fraud.

Sales of the new technology are reported to be brisk, especially since the major card issuers have mandated that starting on Jan 1, 2009, all new self-service pumps must feature PCI-approved PIN-entry devices.

And from July 1, 2010, all card transactions at pumps must be protected with advanced Triple DES encryption technology.

Conclusions

It is clear that the ATM and EFTPOS industry is doing its utmost to reduce fraud in specific sectors of the market. Coupled with the increasing deployment of EMV smart card technology, the security of most transactions, whether for cash (or its equivalent) or retail purchases, can only improve over time.

The bad news, however, is that card fraudsters are likely to concentrate their activities on the weakest points in the card transaction chain, namely on the need for legacy compliance with magnetic stripe technology and the industry's reliance on the use of a four digit PIN as a means of identifying the cardholder.

Supporting the former technology is a given requirement for the industry, therefore it stands to reason that steps must be taken to increase the cardholder authentication side of a given transaction.

Given the inherent weakness of the PIN element of Chip & PIN, it is clear that other technologies such as biometrics and pattern recognition systems need to be deployed, if not in all transactional environments, but in high-risk areas such as ATM usage and garage forecourts. Reliable and economic biometric verification of cardholders is still several years away, and even when it does become available, there will be a legacy gap in many countries and/or industries. It is for this reason that interactive pattern recognition systems are almost certain to come to the fore.

Not only are they secure against the interceptive fraud weaknesses that are inherent in PINs and other fixed-string identification systems, but their ease of use and economic deployment to an ATM environment means that the cost-benefit side of the equation is a given.

⁶ <http://www.petro-c.verifone.com/securepumpay/>

Steve Gold

Widely regarded as a leading authority on communications and IT security, Steve Gold has been a journalist for 22 years, 18 of them full-time. He has specialised in IT security and communications for most of that time.

Former news editor (for 12 years) for SC Magazine and Info Security News, the magazine's online newswire service, Steve is also a former UK bureau chief (1984 to 2002) for Newsbytes News Network, one of the pioneering online newswire services, which he and his colleagues sold to the Washington Post in the late 1990s.

A qualified accountant and formerly an auditor before taking up journalism full-time, Steve has also authored and co-authored several books, including the Hacker's Handbook, The Good Software Guide and The Good Hardware Guide.

