

### Smart Card & Identity News

Is published monthly by  
Smart Card News Ltd

**Head Office:** Smart Card Group,  
Columbia House, Columbia Drive,  
Worthing, BN13 3HD, UK.

**Telephone:** +44 (0) 1903 691779

**Fax:** +44 (0) 1903 692616

**Website:** [www.smartcard.co.uk](http://www.smartcard.co.uk)

**Email:** [info@smartcard.co.uk](mailto:info@smartcard.co.uk)

### Editorial

**Managing Director** – Patsy Everett

**Technical Advisor** – Dr David Everett

**Production Team** - Lesley Dann, John Owen

**Contributors to this Issue** –  
The Squeakers, Tom Tainton,  
David Lock, Stephane Fymat,

**Photos** - Grazvydas Januska & Edyta Pawlowska (Dreamstime.com )

**Printers** – Hastings Printing Company Limited, UK

**ISSN** – 1755-1021

### Disclaimer

Smart Card News Ltd shall not be liable for inaccuracies in its published text. We would like to make it clear that views expressed in the articles are those of the individual authors and in no way reflect our views on a particular issue.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means – including photocopying – without prior written permission from Smart Card News Ltd.

© Smart Card News Ltd

## Our Comments

Dear Subscribers



*Patsy Everett*

The ID card is back in the news again, there are still more protests the latest being from the British Airline Pilots Association (BALPA) who are complaining that their members are being targeted as guinea pigs in an experiment that is unlikely to improve security. However on this one I can see what's happening, it's all those UFOs reported this month being spotted from airplanes. If you are going to meet up with some extra terrestrial being then presenting your ID card will probably be an expected form of introduction.

More seriously let's look at the report of the Identity Fraud Security Committee, which now shows that ID fraud is apparently affecting the UK economy to the tune of £1.2 billion. This new fraud figure apparently includes the costs of the Identity and Passport Service (IPS) because the Home Office figures include 'prevention' as a cost of fraud. At £300 million it was the second biggest contributor to the fraud figures, this will get a few people excited.

Also reported this month is the news that the UK government is going to require the use of an ID card (or passport) to buy a mobile phone. Now this is pretty standard practice in Europe (although they have already better adopted ID cards than the UK) and one wonders whether anybody actually cares. I would need some convincing that the criminal fraternity won't find a way around this little impediment and I can't help think that it won't be long before there will be a big market in identity documents, enough to convince the cashier in Tesco anyway.

One figure that came out this month in all the kafuffle was the fact that 72% of Vodafone subscribers are pay as you go. I had never realised it is this large and helps to explain the distribution of phones. We were doing a study in the office as to how many people have smart phones, taking our own circle of friends as the basis for the survey. Some 12 months ago our survey showed a very small percentage of people with smart phones (e.g. Symbian, Microsoft, etc) but now it is all changing and we have concluded that the iPhone has brought that degree of 'want to have' to the marketplace. Out of the original 100 phone customers 5 had smart phones but now we are up to 40. The other thing we have noticed is that the Blackberry is also on the up, always an executive want to have but now it's starting to penetrate down the chain to people not normally associated with living in their email box. Sexy little things with a keyboard that you can actually use to send texts and short emails, for those of you not yet decided this is one of the problems with the iPhone, no keyboard!

You are probably wondering where all this is leading, well NFC of course. At Cartes this year there is going to be an NFC zone, which clearly reflects the perceived interest in this market. Well the bit that still interests me is whether every phone will have NFC or whether I'm going to have to select from a much smaller number of phone





options. Most of the people I have spoken to accept that NFC will be a niche market albeit in their view a large one and at the moment it seems to me that there is only one Nokia phone that is available with NFC and that is some 5 years or more after I was told it will soon be in every phone. Will it come to the iPhone or the Blackberry? I'm still not convinced but I'm looking forward to seeing all those enthusiastic faces I'm sure I will find in the NFC Zone – see you there!

Just before I sign off I wonder how you are finding the identity checks in UK airports. I have discovered that I can fly from Gatwick to Manchester without ever having to produce any ID, I just need the boarding pass that I printed at home. I've done a couple of such trips this year which just seems to be inconsistent with the total surveillance policy I've been hearing about this month. How are other people finding the need for identity?

See you at Cartes,

Patsy.

## Contents

### Regular Features

Lead Story – ID Card Needed to Purchase Mobile Phones.....	1
Events Diary .....	3
World News In Brief .....	5,10,14,17,19

### Industry Articles

Fraud Prevention Week is a Timely Reminder we're all at Risk.....	9
Collaborate to Innovate	
– the key cornerstone in today's evolving payments industry .....	12
Avoiding a 'Keys to the Kingdom' attack	
-without compromising security .....	15
California becomes second state to ban skimming	
– but is it too little too late? .....	18

## Events Diary

### November 2008

- 4-6 Cartes 2008 - Paris, France
- 10-11 Mobile Money Transfer 08 - Dubai, UAE
- 11-13 7th Asian High Security Printing Conference - Bangkok, Thailand
- 18-20 ID World International Congress - Milan, Italy

### December 2008

- 1-4 Prepaid Commerce Europe 2008 - Stockholm, Sweden
- 2-3 ISNR (International Security & National Resilience) - London, UK





### .... Continued from page 1

their car registration number, the Police database to track the movement of the car using the automatic number plate recognition system currently installed on all major roads in the UK. And of course you could track all associated people through their mobile phones and have a look to see what they are up to.

Just in case you had forgotten the state can also track a citizen's activity by their use of financial payment cards, travel cards, close circuit TV cameras (4.2 million in the UK) and their travel records as per the new e-Borders database. It sounds just like a Sci-Fi film from the 70's yet today this is where we are in the UK and yet we need to know is this a step too far?

If there was a totally trusted body with totally trusted employees, a totally trusted way of accurately acquiring the data and a totally trusted database handling all this data by totally trusted users then I guess few people would complain. In fact the only time you would hear about it is when some criminal or terrorist is brought to judgement or even better when some atrocity has been avoided. The trouble is we don't actually have any confidence in any of these parameters.

Nobody really trusts the Government and in fact they have arguably badly impeached their reputation by using the terrorism laws to freeze the bank accounts of the Icelandic banks in the UK this month. It makes the actions of local authorities look like trivia in their spying on citizens to check their dog walking habits and to see where they are habiting/cohabiting or what have you in terms of rights for schools placements. This is not a good start for a new national database.

Does anybody seriously believe you can have totally trusted employees? Whether for personal gain or to protect their current status or possessions people can always be motivated to take unlawful actions. Remember the 600 people disciplined in DWP for having a look at records not required as part of their work tasks, similar things are known to happen in the NHS and probably just about any other office you can think off – the tax office for example. It doesn't stop there because people also make mistakes (yes, all of us) which can lead to the compromise of confidential data. It's now almost a daily occurrence to see who the latest guilty party is. Not only the government off course but often their advisors, PA Consulting, EDS and Deloitte have all recently made the front page with lost laptops, disks or memory sticks.

Then you have the matter of accurately and securely acquiring the registration data. Now with ID cards and e-Passports there are biometrics designed to stop multiple and false applications. The trouble is that this doesn't work too well in the field when you don't do a similar biometric check because bogus cards or passports will not be detected particularly when the terminals are incapable of checking the digital signatures. I can't imagine the local supermarket having a biometric reader in order to sell a mobile phone. And one thing you can bet on is that criminals and terrorists will be the experts at knowing how to get by with false identity documents.

In terms of the security of the database itself and more particularly the access control to the data in the database. If you have a large number of authorised users then you immediately have a problem controlling authorised access. One imagines that for this sort of planned database there will be a large number of users across multiple departmental/organisational boundaries. Perhaps we could mandate 2 Factor authentication, a good use of smart cards and one that we might well expect to see on the increase. But then we have yet another registration problem of identifying the users and managing the authentication system and its database, no mean feat.

In fact we can almost certainly conclude that any database of this scale with its myriad of users is going to result in breaches to user privacy. Worse it may even be by design, the deep packet content filtering system being tested by BT (PHORM) as part of a new targeted advertising scheme is sort of in the middle of all of this, look at what the user is doing on the internet and target the advertising accordingly – pretty invasive stuff particularly if you can't opt out.

So the question is will all this really happen? Well it has already started with GCHQ reportedly being given £1 billion to set up a network of black boxes on the internet to monitor traffic with total project costs estimated at £12 billion. Remember ECHELON, the signals intelligence collection and analysis system developed under the UK-USA Security Agreement to monitor fax, emails and other data communications. Apparently this was not capable of really doing the job and that this new approach is designed to correct the shortcomings.

As for the new National Database well that seems less likely, I can't imagine the privacy bodies letting this one go by without a fight.





## World News In Brief

### UTC Withdraws Offer For Diebold

United Technologies Corp. this week informed Diebold Inc, by letter of the withdrawal of its February 29, 2008 acquisition offer. The following is the letter's complete text.

"We have seen Diebold's financial restatements recently filed with the SEC and note that you have scheduled your annual meeting for November 12. In light of your extended refusals of UTC's requests for management discussions and due diligence, we are withdrawing our offer of February 29 to purchase any and all Diebold common shares at \$40 per share. We had hoped we could negotiate a transaction that would have created substantial value for both your and our shareholders. It's unfortunate this won't happen."

Diebold, Incorporated provides integrated ATMs and other self-service solutions as well as security systems and services. Diebold employs more than 17,000 associates.

### Thales Completes nCipher Acquisition

Thales announced that its acquisition of nCipher PLC, purchased for £50.7 million in cash, became effective on Friday 10 October.

nCipher is delivering solutions in the fields of key management and cryptographic hardware. nCipher operates a network of partners and offices in the UK, Europe, the Asia Pacific region and the USA, with customers including government, financial institutions and enterprises.

The acquisition is to further develop Thales's information and communications systems security business by combining the expertise of the two companies. Thales will also add nCipher's network of regional offices to Thales's international network, thereby creating a wider distribution base.

### L-1 Identity Solutions Receives \$5.9 Million Driver's License Contract

L-1 Identity Solutions, Inc., a provider of identity solutions and services, announced that the L-1 Secure Credentialing Division received a three and a half year, \$5.9 million contract expansion from the state of Mississippi.

The state of MS uses an over-the-counter secure

credentialing production system that processes and issues driver's licenses on the spot at bureau locations. The integrated workstations from L-1 include L-1 ImageCams for digital portrait capture, personal computers, driver's license\ID card printers, fingerprint scanners, flatbed document scanners and signature pads and will help MS to quickly and securely process and issue valid driver's licenses.

### XIRING And SCM Microsystems Jointly Develop Mobile Terminals For German eHealth Market

XIRING, and SCM Microsystems, have announced their collaboration to develop mobile eHealth smart card terminals for the new generation German healthcare system. Beginning in late 2008, new electronic health insurance cards will be distributed to 82 million German citizens, creating a market for compatible mobile eHealth terminals that facilitate at-home patient consultation and treatment by Germany's 310,000 healthcare professionals and 130,000 physiotherapists. With this agreement, the two companies aim to achieve a leading share of this new market. SCM will sell the mobile terminals in Germany through its existing distribution channels and Value Added Partners.

### ICMA Survey Shows Continued Growth In Card Manufacturing Industry

The International Card Manufacturers Association (ICMA), a global non-profit association for card manufacturers, personalisers and suppliers, announced this month the results of its Annual Card Manufacturing Global Market Survey. The survey measured results from 2007 and revealed that factors such as inflation and the decline of the value of the dollar have affected the value of the overall global card market. However, North America remains the #1 unit producer of cards with the Asia Pacific region retaining its second position in card production after out-producing Europe for the first time in 2006.

In 2007 the unit market reached 19.2 billion cards, which represents a 12 percent, increase over 2006. North America remains the largest card unit market with more than 9.1 billion cards manufactured in 2007.

Asia Pacific manufactured 4.5 billion cards. Europe



remained in the #3 position with just over 4 billion cards manufactured. Latin America reached the 1 billion mark in 2007 and Middle East/Africa manufactured 489 Million cards last year.

The regions surveyed were North America, Europe, Asia Pacific, Latin America and Middle East/Africa. The products surveyed were plastic cards of all thicknesses including traditional cards-with and without magnetic stripe, and chip cards that include contact, contactless and combi-cards for diverse applications such as financial hologram cards, ID cards, telecom cards, gift cards, transit cards and more.

### **INSIDE Contactless And TIEMPO Partner On Next Generation Chip**

INSIDE Contactless, and TIEMPO, a company specialized in the design of asynchronous ICs, have announced a partnership for the design of a next generation chip product that incorporates asynchronous design technology.

The new chip will be designed using TIEMPO clockless and delay insensitive technology.

As the first step of this partnership, INSIDE and TIEMPO have engaged in a collaborative project that will include expert designers from both companies, TIEMPO providing INSIDE with its asynchronous IPs and with the expertise of its engineers in the design of low-power asynchronous chips.

### **Oberthur Technologies Gets FIPS Certification New Java Card**

Oberthur Technologies announced that it has obtained the new FIPS140-2 Level 3 certification for its Large memory Java card platform generation. Internationally designed and recognized, the FIPS certification enables to verify that products meet the cryptography claims by vendors.

This new platform is compliant Java Card 2.2.2 and Global Platform 2.1.1, the new Java card is the first to be FIPS certified with full support for Elliptic Curve cryptography.

### **Giesecke & Devrient Launch Volume Production of Hot-laminated Display Cards**

Giesecke & Devrient (G&D), announced a new display card capable of being manufactured on a high-volume industrial scale. The six-digit display is incorporated in the card during the normal hot-lamination process, thereby augmenting its

resistance to mechanical wear. G&D's GDC4000 display card can be used to display one-time passwords (OTPs) for secure authentication during access to IT networks, or transaction numbers (TANs) for online banking.

G&D has chosen Aveso, a specialist in flexible displays, to supply the display technology. Aveso will provide the display that will then be embedded together with various electronic components, a battery and a button in different layers of the card using a hot-lamination process. The finished card corresponds to the standard ISO ID1 format and is not thicker than usual types of credit card.

The use of a dynamically generated one-time password in conjunction with static customer data such as account number, user password and personal identification number (PIN) significantly enhances the security of online authentication. The display card makes it possible to add a supplementary, bi-directional identity check that protects users and providers of online banking services against the theft and fraudulent misuse of passwords and TANs. This additional verification works as follows: When the bank's background system receives the one-time password generated by the card, it responds by transmitting a second one-time password that appears on the customer's computer screen. When the customer now presses the button on the card, the password it displays must match that shown on the computer screen. This provides secure confirmation that the password was indeed sent by the bank.

### **Stagecoach Begin Paypass Roll-out**

Bus passengers in Liverpool (UK) are to be the first in the UK to be able to use a bankcard to make on-board payment for travel, Stagecoach, MasterCard and The Royal Bank of Scotland (RBS) announced.

A one-year trial will see the major roll-out of the technology in the second quarter of 2009 on around 200 Stagecoach buses in Merseyside, allowing passengers to make fast, convenient and safe payments simply by tapping their card on a dedicated reader.

MasterCard PayPass and Maestro PayPass allows holders to make payments under the value of £10 and will be a direct alternative to cash, saving customers fumbling for cumbersome coins or waiting for change. Customers will still be given a bus ticket as proof of purchase.

It is the first ever use of contactless bankcard payments on public transport in the UK and the first significant extension of the 'Tap & Go' way to pay.





## MIFARE Classic Hacks Revealed At ESORICS 2008

In March 2008 researchers at Radboud University Nijmegen, led by Professor Bart Jacobs, demonstrated that the Mifare Classic Chip, as used in the London 'Oyster' card has shortcomings.

Publication of the scientific article was published on Monday at the European Symposium on Research in Computer Security (Esorics) 2008 security conference in Malaga on the 6-8 October, 2008.

Since then Smartex a smart card technology club has distributed the university publication as a PDF entitled "Dismantling the Mifare Classic".

In a statement, NXP Semiconductors said it "regrets that the Radboud University Nijmegen has revealed just yet details of the protocol and the algorithm of Mifare Classic as well as some practical attacks on Mifare Classic infrastructures"

"NXP has an open dialogue with the University Nijmegen and other researchers on the security of Mifare Classic and has taken the lead in communicating the effects of attacks and possible countermeasures to industry partners who need to know. Nevertheless, NXP would like to point out that a broad publication of detailed information to carry-out attacks with limited means is, at this moment in time, contradictory to the scientific goal of prevention and the responsible disclosure of sensitive information."

"Security upgrades, whether still based on Mifare Classic or migrating to a different card format, are complex system modifications which may involve a combination of hardware and software in the cards as well as in the infrastructure and back-end equipment. As these upgrades can - based on the particular system security requirements - take up to a number of years, it is not conceivable that all Mifare Classic infrastructures have their security upgraded to the necessary level yet."

At the same day that Henryk Plotz, a PhD student at Humboldt University in Berlin, published his master thesis (PDF) that includes the full implementation of the algorithm used in the Mifare Classic. (<http://sar.informatik.hu-berlin.de/research/publications/>)

NXP Semiconductors, will launch its new Mifare Plus IC at Carte's 2008, 4-6 November in Paris, France. MifarePlus is the latest addition to NXP's Mifare family of chips, and will combat the Mifare classics failures.

At CarteS, NXP will demonstrate multiple levels of enhanced security available to customers with Mifare Plus, including 128-bit Advanced Encryption Standard (AES) and the easy migration path from existing Mifare Classic implementations.

## Oyster & Oyster Brand Could Be Lost To New Technology, Assembly Hears

Transport for London is considering replacing Oyster with new ticketing systems operated through mobile phones or bankcards, the London Assembly heard.

At a meeting of the Assembly's Budget and Performance Committee, TfL representatives said they were looking at various technologies and providers to take over from Oyster in 2010. TfL announced in August that they were terminating early the current contract with TranSys for delivering Oyster ticketing.

Will Judge, Head of Future Ticketing at TfL said they wanted the new ticketing system to be contactless, fast and convenient. He added that with new advances in technology, the system could be delivered on a smartcard - like the Oystercard - or on a phone or bankcard.

Mr Judge also said that when TfL considers the new technology, they would not try to do it in-house, but would take advantage of good practice elsewhere.

TfL told the Committee they were investigating whether Oyster - and its successor - could be integrated with other parts of London transport. It is hoped that Oyster will be available on the capital's riverboat services next year.

Commenting on the decision to terminate the contract with TranSys, Mr Judge said that TfL believed it would save millions of pounds by moving to a more conventional - not PFI - contract.

He said TfL intended to break the new contract up into modules and let each bit individually - much like the Congestion Charge contract.

Assembly Members also heard that the new ticketing system could have a different name and that the Oyster brand could be lost forever.

John Biggs AM, Chair of the London Assembly Budget and Performance Committee, said: "This Committee is interested to hear about the new technologies that TfL is exploring for the delivery of their new ticketing system. We will look with interest during our examination of TfL's business plan to see what level of savings is achieved."





## Smart Card Alliance Paper Addresses Why Smart Cards Are Secure

Smart card technology is becoming an important part of everyday life in the United States and throughout the Americas. Now the preferred technology for securing personal digital devices, it is used in electronic passports, contactless payment cards, transit fare cards, SIMs for cell phones, new ID cards issued to government and non-government employees-the list goes on and on. But are they really secure? The Smart Card Alliance addresses this question with a new report that explains what makes smart cards secure in a white paper released today entitled "What Makes a Smart Card Secure?".

<http://www.smartcardalliance.org/pages/publications-smart-card-security>

"Our newest report details how smart card technology uses secure integrated circuits as the core of the technology, and explains the unique security benefits this provides to personal secure devices such as cards, USB tokens, SIM modules or embedded chips. Readers will also learn how smart card technology and secure microcontrollers enable additional system-level security measures, and how these multiple layers work together to better protect the system and its information from unauthorized users."

## Consumers Trust Online Payment Providers More Than Traditional Banks

Important consumer segments such as baby boomers, trust online payment providers more than they trust traditional banks, according to a survey on retail financial services recently conducted by the Cisco Internet Business Solutions Group (IBSG). Consumers are demanding the same convenience they receive online when shopping in a brick-and-mortar environment. This dramatic shift in consumer expectations presents a considerable market opportunity for financial institutions that embrace connected commerce. The average incremental value of connected commerce for the top 20 U.S. banks is estimated to reach more than \$100 million yearly by 2015.

The research reveals that evolving customer preferences among all age groups represent both a challenge and an opportunity for financial institutions. As consumers increasingly use the Internet and mobile devices to make purchases and payments, banks are subject to both customer attrition and revenue loss. The research also shows,

however, that banks can reverse this trend and use their connections to merchant and consumer payment data to create new revenue models from advertising, cross-selling and value-added services surrounding points of sale.

Historically, the online shopping experience was designed to imitate the brick-and-mortar experience. The Cisco IBSG survey results show that now, coming full circle, the brick-and-mortar experience must resemble the online channel to meet the shifting expectations of consumers.

## Pilot's Targeted As UK ID Card Guinea Pigs

From 2009 the UK Home Office plans its second phase of the UK ID card roll-out by issuing ID cards to British and foreign nationals working in sensitive roles or locations, starting with airport workers.

Jim McAuslan, general secretary of the British Air Line Pilot's Association (BALPA) told the UK 'Observer' newspaper that "Our members are incensed by the way they have been targeted as guinea pigs in a project which will not improve security.

BALPA is among the world's largest flight crew associations - second in size only to the U S Air Line Pilots' Association. As a specialist organisation we protect and improve the professional status, pay and conditions of our members. BALPA's membership is currently more than 9,000.

Jim continued; "We will leave no stone unturned in our attempts to prevent this, including legal action to force a judicial review if necessary."

## Giesecke & Devrient To Supply Austria's e-card For A Further Five Years

The Main Association of Austrian Social Insurance Institutions has extended its contract with Giesecke & Devrient (G&D) for an additional period of five years. Under the terms of the new contract, worth approximately 20 million euros, the Munich-based company has been entrusted with the production, personalization and delivery of a total volume of around nine million electronic social insurance cards (the e-card) from 2010 onward. Deliveries of the latest-generation Austrian e-card, which combines the functions of a health insurance card and a citizen card for e-government applications, will commence in early 2010.





# Fraud Prevention Week Is A Timely Reminder We're All At Risk

By Tom Tainton, Smart Card & Identity News



*Tom Tainton*

The UK's fourth National Identity Fraud Prevention week, a partnership between the Metropolitan police and various organisations including Experian, Fellowes and Equifax took place earlier this month. The awareness campaign educates consumers about the threat of identity fraud as well as offering advice to prevent it happening to consumers and businesses. Fronted by the BBC's Adrian Chiles, the nationwide event aims to tackle the problem of identity theft, one of Britain's fastest growing crimes. According the government estimates, the annual cost of identity fraud is more than a staggering £1 billion. It is therefore little surprise that a Populus poll revealed that 81% of British people were concerned about becoming a victim of stolen personal data, that's more than the worry expressed towards burglary, mugging and pickpocketing.

The survey also showed that a fifth of the British public access their bank details at work or at internet cafes, putting them at risk of identity fraud. And don't worry, even if you don't share your personal data across the net you're still just as vulnerable to attack. Perhaps most alarmingly, a bin-raiding survey conducted by Fellowes exposed that over half of all UK household waste contained one or more items, which would give a potential fraudster everything needed to steal an identity. That's more than 18 million homes across the country. To make matters worse, research carried out by credit reference agency Experian found that it takes an average of 467 days for someone to discover they are a victim of identity crime.

To combat this, MPs called for Brown to appoint an ID fraud tsar – a central figure to coordinate efforts and reduce the potential knock-on effects to businesses and consumers alike. An All Party Identity Fraud Group spokesman said, "Appointing a single person to work across the government and private sector would certainly create a more unified approach to the problem. We believe a national strategy for fraud should be established, and sooner rather than later."

However, the calls were received with mixed reviews from the industry. Some critics believe an appointed figure would just be a case of the government bailing out private firms unwilling to review their own security processes. Instead it was argued that educating staff more efficiently and investing in secure technology will help to stem the flow of identity fraud in the UK, which already has the highest rates in Europe, with four million British adults falling foul of identity crime last year. One reason for the soaring rates is the difficulty in reporting computer crime. Because it doesn't have to be reported to the police, organisations now just alert their banks who have no incentive to publish damning figures that reflect negatively on their business. It's not going to get any easier either. Over the next few years the average person will have ten times the current amount of personal information in the public domain and fraudsters will be licking their lips at the prospect.

In October alone, there have been a vast number of identity crimes affecting businesses and individuals across Britain. Facebook, the world's most popular social networking site, was hit with an IM-based spam campaign aiming to steal a user's log-in details. The scam worked when a member clicked on a site link promising a 'hot date'. When the member clicks on the link the virus obtains personal credentials using a php script, giving the fraudster access to passwords, email and even financial data.

In addition to this, a number of malicious PDF files were discovered in Adobe Acrobat Reader. The PDF's had been created to exploit security flaws in the software and to install malware in vulnerable applications. More than 25,000 attacks were recorded in just two weeks. The Home Office's incredible ability to lose vital information continued when Ministry of Justice sheepishly announced the loss of 3,500 security passes for prisons. On average, one employer loses their security pass every day suggesting an inexcusable culture of carelessness. The problem isn't just confined to British shores. French President Nicolas Sarkozy recently revealed his bank account had been breached and small sums of money had been stolen, after hackers had obtained entry details to the President's account. France has seen a 9% increase in online theft prompting the government to warn citizens of their own online vulnerability.





There are ways to prevent identity fraud. By managing personal information carefully the risk of crime can be substantially reduced. There are various ways to do this. Be vigilant when asked to give account details, and pay attention to billing cycles. Use strong passwords, and various email addresses if necessary. Most importantly, invest in up-to-date anti-virus software and the latest security patches. Believe me; it'll be worth it in the long run.

## World News In Brief

### Research Highlights Need For UK Central e-crime Body

Research carried out by Infosecurity Europe has shown that 95 per cent of people would prefer to report online fraud directly to a dedicated e-crime agency, rather than having to go through APACS and/or the financial services firm with whom the fraud took place.

The research by the Infosecurity Europe show - which took in online responses from 359 visitors to the site - follows on from a debate in the House of Lords on e-crime and IT security issues.

In that debate, their Lordships noted it was anomalous for UK banks not being obliged - in law - to refund account holders who have been electronically defrauded.

Lord Broers, the Chairman of the House of Lords Committee on Science and Technology, said that the current situation is that account holders are only being refunded under a voluntary code, noting that that in today's environment, this is scarcely appropriate.

In addition, Lord Broers said, whilst customers currently report their e-frauds to the banks, it is not in the banks' interests to draw attention to the fact that their anti-fraud systems have failed.

Against this backdrop, their Lordships concluded there is a need for specific legislation - similar to the Bills of Exchange Act 1882 - which specified that if a bank honoured a forged cheque, the bank, not the customer upon whose account the cheque had been drawn, was liable.

The Earl of Erroll, a cross-bench member of the House of Lords, said that he was not surprised that 95 per cent of people would like to be able to report online fraud directly to a dedicated body.

"I think that people instinctively realise that you cannot expect people or organisations to report their own shortcomings reliably," he said, adding that the industry must always have independent bodies looking after our interests."

### Home Office Accounts For One Quarter Of ID Fraud

The latest estimate of the cost of identity fraud to the UK economy is £1.2bn. The figure was developed by the Identity Fraud Steering Committee and key industry stakeholders and is based on a new methodology agreed by the committee. (<http://www.identitytheft.org.uk/>)

The new identity fraud figure is actually the direct cost of the Identity & Passport Service, because Home Office figures include anything they deem to be "prevention" as part of the cost of fraud.

The new - but as yet unexplained - methodology actually eliminates over half a billion pounds of activity that the government previously claimed as 'identity fraud'.

Analysis of the current estimates reveals that a large part of the stated 'cost' of fraud is, in fact, the cost of bureaucracy. The activities of the Identity and Passport Service make it the second largest item in the list.

Phil Booth, NO2ID National Coordinator said:

"NO2ID has called the ID scheme a fraud many times but, by counting the cost of its own activities to boost fraud figures, the Identity and Passport Service has confirmed it.

"On this logic, the more the Home Office spends on identity control, the more "fraud" there is. It is more than just circular logic. The Home Office is now, by its own estimate, the country's single biggest fraudster - taking the public for nearly £300 million a year and rising."





## UK Home Office Employees Lose Security Passes Once A Day

The UK political party, the Liberal Democrats have revealed that staff at the Whitehall departments responsible for the nation's internal security have lost nearly 3,500 security passes since 2001. Staff at the Home Office and the Ministry of Justice are losing their passes at a rate of over one per day. Since 2001, 3,492 security passes have gone missing, and the rate at which passes are being lost has risen by 300% in the last six years.

The research shows that:

- Between 2001 and July 2008, Home Office and Ministry of Justice staff lost or had stolen 3,492 security passes.
- Between 2001 and 2007, they lost or had stolen 3,241 passes, at a rate of 463 a year, 9 a week, or over one a day.
- Home Office staff were nearly twice as careless as Ministry of Justice staff, losing 2,039 passes between 2001 and 2007, compared to 1,202.
- Their carelessness appears to be on increase. In 2007, the combined staff of both departments lost or had stolen 675 passes (nearly two a day), compared to just 169 in 2002 - a 300% increase.

Commenting, Liberal Democrat Shadow Home Secretary, Chris Huhne said:

"Everyone understands that things can go missing, but these figures suggest a culture of carelessness among the people responsible for our safety and security. On average, one of their employees loses their security pass every day.

"This Government wants powers to build a database of every phone call and email, but the evidence of lost security passes suggests they could not be trusted to run a nightclub door.

"They must scrap ID cards before they are allowed to treat our most sensitive data in the same slapdash manner."

## Identity Theft Three Times More Likely In The UK

One in seven online shoppers (14%) in the UK, has fallen victim to identity theft, around three times the number in Germany (3%), Spain (5%) and France (6%). The findings come from PayPal's 'Global

Trust and Safety Report', which surveyed 6,000 people from the United States, Canada, France, Germany, Spain and the United Kingdom.

The report examined online security fears and habits and found that half (49%) of online users in the UK are 'very concerned' about identity theft and when people are victims of this crime they often have no idea how it occurred.

Fears of identity theft may be widespread, yet online users are underestimating their own role in preventing it happening with many choosing weak or obvious passwords for accounts; more than half (53%) of users across all six countries admit to using important personal dates or names. However the report did find that attitudes to password security do vary between different cultures. Over four in 10 (42%) people in the UK use an important date or name for their password, compared to only 35% of Spaniards. The French came out as taking the most risks with their password with 63% choosing a password that could be easily guessed.

Michael Barrett, chief information security officer for PayPal said, "This survey shows that while concerns about ID theft form a universal language, more identity theft tends to occur in countries where a higher percentage of e-commerce is concentrated. But e-commerce is growing in prominence around the world, and fraudsters will likely follow the money. Consumers everywhere can stay one step ahead and better protect themselves online by following a few simple tips."

However, choosing stronger passwords may not help in some situations, as the report found online consumers are willing to divulge their password information to others. More than a third of online shoppers in the U.K (35%) have shared their password information with a family member compared to just over a quarter (25%) in Germany admitting to telling a family member their password.

Online security is also being undermined as details are displayed on popular social networking site: one in seven (14%) 'social networkers' in the UK admit to displaying password related information on a social networking page, which could ultimately lead to identity theft.

The PayPal study also found that a number of identity theft victims say they have no idea how the theft occurred, with 40% in the UK are clueless as to how their information was obtained. In fact, more than half of identity theft victims in the UK (52%) had to be contacted by their bank or credit card provider before they were even aware their identity had been stolen.





# Collaborate To Innovate

– the key cornerstone in today’s evolving payments industry

By David Lock, Business Consultant at ACI Worldwide



*David Lock*

The payments industry is continually evolving with new technologies bringing more competition and innovation to the payment services market. However, there has been a subtle change of focus in recent years. While previously innovation in card technology was driven mainly by the fight against fraud, today consumers are in the driving seat dictating how card and payment technology should evolve. In June this year, the GSMA - the global trade body for the mobile industry - and the European Payments Council agreed to accelerate the deployment of services that enable consumers to pay for goods and services in shops, restaurants and other locations using their mobile phones. Integrating payment applications onto the mobile phone satisfies consumer appetite for using this single device to conduct every aspect of their life. But, how will financial institutions and other parties, such as retailers and mobile phone operators, benefit from these developments in payment technology and also overcome the associated challenges ahead?

The mandatory introduction of EMV cards in Europe in 2006 is one of the most recent innovations in card technology, ensuring that cardholders are able to conduct face-to-face transactions in a more secure manner. By the end of 2007, half of all MasterCard-branded cards were EMV chip enabled and EMV acceptance penetration stood at 68 per cent of all Point-of-Sale terminals and well over half of all ATMs in Europe. Yet consumers are demanding more from their banks in terms of payments services. Increasingly technology-savvy consumers are keen to have instant access to the full range of banking services and do not see why the mobile phone cannot be used as a payment device as well as their main communications, banking and travel device.

From the early introduction of magnetic strip cards through to the more security focused implementation of EMV smart cards, a revolution in payments is now underway. Instead of implementing new technology that is purely driven by fraud concerns, the financial services industry is responding to consumer demands for more innovative products that work in conjunction with everyday gadgets such as mobile phones. With the advent of phone-based payments a new range of payment channels will be available to the customer. This provides many opportunities to implement additional services such as location-based coupons, instant redemption of loyalty, and car parking with expiry time reminders. However, in order to drive uptake of mobile payments forward, the industry has to find a way to collaborate to be able to provide customers with efficient and secure offers.

## Widespread mobile phone uptake: what are the challenges?

Enabling widespread mobile payments is no mean feat as there are numerous hurdles to overcome along the way. In fact, it could be argued that contactless card payments must first become mainstream before mobile payments can seriously be considered as a replacement for cards or cash. In the UK, Barclaycard’s OnePulse card became the UK’s first integrated travel and payment contactless card enabling purchases of everyday items under £10 and acting as an Oyster travel pass to access the London transport network. Barclaycard is exploiting the currently unique nature of its product to attract new customers from the ten million Oyster card holders in London. Contactless also brings opportunities for other banks to increase their share of the UK card market in what is a very competitive industry.

However, it remains the case that, a major challenge to overcome is the issue of security. The proportion of contactless transactions that come online for authentication is much lower than with contact EMV, making them more attractive to fraudsters. In addition, issuance systems must also evolve to support contactless while maintaining competent identification of risk and revenue profiles of potential cardholders. Banks need to decide if they would prefer to only issue contactless cards when the customer’s existing cards expire; when replacing lost or stolen cards or if requested by the customer well before his current expiry date. Such complexities are compounded by the fact that it is not yet clear exactly what functionality, such as debit, credit or transit, will be offered on the cards once full roll-out starts. The London trials cannot be used as an exact blueprint for large-scale roll-out. London is unique as regards its existing infrastructure and transport network, and the notion of contactless is already culturally ingrained in the local population through the use of Oyster cards. However,





Oyster does not work on many train lines into London and there are a myriad of transit organisations in the UK – which suggests that a less proprietary option for contactless will be required in the long-term.

Once again there is also the concern of how criminals will attempt to exploit this new technology and all parties must ensure that fears relating to security and personal privacy do not jeopardise uptake. Aite Group has suggested that this new payment channel with inexperienced users of mobile payments, little technological standardisation, millions of transaction-enabled mobile devices and the global reach of the mobile internet provides an opportunity for organised crime gangs to exploit these weaknesses. With the overlap of mobile banking with internet banking, it is likely that many of the threats prevalent in the online world could cross to the mobile domain.

The adoption of pan-European standards, which currently do not exist yet as most mobile payment initiatives are being implemented at a national level is an additional stumbling block. Cross-border standards will be important to ensure that the various business relationships continue to be successful after the pilot phase is complete.

Co-branding could also provide a potential challenge for more widespread uptake of mobile payments. As mobile payments become a reality, unique co-branded products will appear providing new revenue streams and opportunities for those involved. However, inevitably, these agreements will be time-limited contracts which could lead to a whole host of problems when the business relationships come to an end.

Ultimately, as during the roll-out of EMV cards, all parties involved have to collaborate, at least to some degree, to identify and implement the possible solutions.

### **Near-Field Communications (NFC) – what's next?**

Despite the challenges outlined above, it is likely contactless card payments will gradually become a way of life, and we are already beginning to see the move from card to NFC-enabled mobile phones that can leverage the existing infrastructure. RBS and Barclays are again leading the way as both launched pilots of NFC phone technology in London in late November last year. Across the Channel, six major French banks and four mobile operators joined forces in cooperation with MasterCard Worldwide and Visa Europe to launch mobile payments at the end of November 2007. The large-scale field trial to test mobile contactless payments involved 1,000 customers and 200 sales outlets located in the cities of Caen and Strasbourg. The trial was based on a payment application embedded in the customer's SIM card and on the NFC technology.

This UK pilot is, however, still in its infancy without an imminent industry-wide roll-out date. As with cards, contactless mobile payments raise a number of issues such as merchant service charges for retailers, points of interaction for customers and security risks when phones are lost or stolen. However, the biggest stumbling block in ensuring the long-term success of NFC technology is building and maintaining cross-industry relationships. The involvement of mobile operators means that the mix of relationships required for NFC is even further complicated than the transit-bank relationships evidenced in scenarios such as OnePulse. It is an unbalanced business ecosystem with many more banks in Europe than telcos and handset manufacturers. This complexity is compounded by the fact that banks and telcos have very different views on the level of security required for payment applications residing on a mobile phone. Finding a viable commercial model that fits all parties' requirements and that is affordable for consumers is the priority.

More recently, in August 2008, electronic payments provider NETS, SingTel and United Overseas Bank in Singapore rolled out a six-month NFC pilot, enabling users to make payments from their mobile phone.

Due to the number of different providers that NFC draws together, there is a very clear need for technology that reflects this complexity and enables customers to manage their bank accounts, card accounts, mobile wallets, loyalty applications, transport and ticketing applications, while maintaining usability and security.

### **Supporting Technology**

With the changes to the customer experience, the business model and conditions in the financial markets, there is uncertainty as to what this means for the technology infrastructure of the financial institutions. However, what is clear is that there will be a requirement for more flexibility and openness not envisaged when most closed cards systems were conceived.





For both issuers and acquirers, the fee structures will require greater flexibility. The revenue model will need to cater for complex differential fees based on the use of technology that will be required to charge merchants. New events and services with new value chains will need to be generated for issuers. In addition new players in the business model will require both fees and a share of revenue which will require amendments to existing systems.

The technology supporting new applications and channels will also require new openness. One of the complaints of users in London NFC and contactless trials is that there is not one common place to go to for information. Customers demand a single point of contact which will require combining data from banks, mobile companies, transport and other third parties into a single user experience. The ability to provide technology to all partners that allows them to combine all data will be key.

### Looking ahead

Banking is all about risk, and banks will not innovate without a business case, particularly in the current economic climate. Yet, even when margins are tight, financial institutions cannot afford to stand still and take their foot off the pedal when it comes to payment innovation. Banks are constantly vying for the best customers available and those banks which move first with the right product will create the market and own the lion share. Unlike the introduction of Chip and PIN in the UK which was driven by a desire to reduce card present fraud collaboratively across the industry, contactless and mobile payments are purely marketing-led and therefore by definition more competitive. The more savvy financial institutions recognise that in order to differentiate their services and steal a march on the competition, now is the right time for innovation in payments to ensure future survival and prosperity. Collaboration between all parties involved, however, is key to turning this innovative concept into mainstream reality.

## World News In Brief

### ID World International Congress

18th - 20th November 2008, Milan, Italy.  
This year's ID WORLD International Congress will take place in Milan at the Milanofiori Congress Center on November 18th to 20th and explore the fundamental issues associated with automatic identification in a variety of market segments via three cornerstone initiatives: the Conference, the Exhibition and the Exchange.

ID WORLD International Congress, is the annual world summit on automatic identification. It is a comprehensive showcase of RFID, biometrics and smart card technologies, and is the only international forum that looks at the auto ID industry as a whole, rather than focusing on a specific technology.

Last year ID WORLD attracted around 2,500 individual visitors.

### CARTES & IDentification 2008

The Paris event on digital security and smart technologies will bring together all the international players of the sector who will present their innovations to the 20,000 expected visitors. In complement, the Congress offers the opportunity to update knowledge on current topics with the most

well-known specialists of nowadays.

For this 2008 edition, United States will be the guest of honour. An exposition on smart devices and a 'NFC Zone' will also be organised. Finally, highly awaited by the professionals of the sector, the Sesames Awards will be awarded on the eve of the exhibition in a prestigious venue in Paris.

### BMX & NXP Reveal Multifunctional Car Key

BMW Group Research and Technology and NXP Semiconductors, have unveiled a prototype of the world's first multifunctional car key. The prototype features contactless payment, personalised access control, and advanced functionalities including public transport e-ticketing, to deliver an enhanced mobility experience.

In the future, car owners may benefit from the ease-of-use of contactless payments for ad-hoc transactions including general shopping, paying for your petrol, public transport, parking and road tolls, replacing the need for cash or additional cards.





# Avoiding A 'Keys To The Kingdom' Attack Without Compromising Security

By Stephane Fymat, VP of Business Development and Strategy at Passlogix



*Stephane Fymat*

In Europe, very few people have heard of Terry Childs. In California, everyone has. Childs is the City of San Francisco's disgruntled network manager who reset all administrative passwords to the routers for the city's FibreWAN network and held the city administration to ransom. He refused to hand over the passwords which effectively gave him complete control of the network, locking out all other employees and preventing anyone else from administering it.

As legal teams try to get to the bottom of how Childs was able to gain so much control, IT managers around the world are working out how to prevent the same thing happening to them.

The complexity of corporate IT systems requires users to memorise more and more passwords: surveys have found that 36 per cent of users have between six and 15 passwords to remember; a further 18 per cent have more than 15 unique identifiers to memorise. Research from Burton Group, suggests that the average user can spend up to 15 minutes every day logging on to separate application – which adds up to 65 weekday hours spent entering user IDs and passwords each year.

Almost everyone has personally experienced password frustration: the inability to remember the details for an important application when they needed it and the delay in getting the password reset by the IT help desk. Gartner estimates that 25 to 35 per cent of calls made to IT helpdesks are password related at an estimated cost of around £15 - £20 a call, adding millions to the support bill at larger companies.

Aside from lost productivity, the excessive administrative overhead and the user frustration, passwords can actually present a significant security risk. In an effort to jog their memories, users will often create passwords that are easy-to-figure out - such as derivatives of names and birthdays - making it all-too-easy for hackers to gain access to enterprise applications and data.

Concerns about ineffective password systems and lax password security that enables unauthorised users to breach enterprise networks have caused corporate regulators to take a tougher stance on password security. The Sarbanes Oxley Act for example, includes specific clauses on password security. Nonetheless, there are people, including Bill Gates, who question their benefit and long term future.

But the problem doesn't lie with passwords themselves – it's how they are managed and the lack of best practice in how they are deployed. The latest generation of enterprise single sign-on technologies (ESSO) overcomes the inherent weaknesses of passwords. ESSO eliminates the need to remember - and therefore the risk of forgetting - and is the most effective antidote to the problem of password overload.

ESSO enables users to sign in once with a single password and access all their applications, databases and systems. They no longer need to remember or enter individual passwords for all those applications, so they gain immediate access to corporate information in a more secure, controlled environment. ESSO automates the process of password entry by responding to each log-in prompt without user intervention. New passwords can be automatically generated when old ones expire, and the user ID and password for every application can be stored in a secure central repository.

Quite aside from the very quantifiable savings that can be made in help-desk costs, the benefits of ESSO to the enterprise include simplified administration, improved enterprise security and greater user productivity, all while retaining the ability to achieve compliance with regulations on data protection, privacy and corporate governance.





So why isn't it more widely used?

ESSO has often been seen as too costly and labour intensive to ever be truly attainable. But the latest advancements in the technology mean that its time may finally have come.

Traditionally, one of the biggest criticisms of ESSO has been that it makes an organisation vulnerable to a single point of attack. The reality is that ESSO provides a higher degree of security. There is no user involvement so password quality rules can be more easily enforced, for example. Password length and complexity and the frequency at which they are changed can be greatly increased making them much more difficult for a hacker to decipher. Since users don't need to remember each password, unique, complex alpha-numeric combinations of any length, case or format can be created for each application, database or account log-in. Mathematicians have proved that if the length of a password is increased from 8 to just 9 characters, the time to crack the password is increased to 447 years.

Even in the unlikely event of a hacker cracking the password, they would still need access to a workstation with ESSO software on it, or alternatively install software on a workstation themselves. Even then it would require specific knowledge about how to install and configure the ESSO software with the target organisation's directory.

But the problems associated with passwords aren't limited to the fallibility of users' memories and the determination of hackers. The Childs incident illustrated another problem that has passed under the radar at most companies, who place an enormous amount of trust in their IT staff and system administrators. There was only one administrative account on many systems at San Francisco. Childs had open access to system passwords, and so was able to change them without authorisation and lock out his colleagues. It's not an uncommon scenario – but it is an unavoidable and unnecessary one.

The most advanced ESSO software now includes shared and privileged user management capabilities. This enables all administrative passwords to be encrypted and stored in the enterprise's central directory. Administrators must check out a password from the directory in order to use it - and can be approved or denied based upon the administrator's role and manager's approval within an identity management system. If approved, the software will log the administrator on to the network device and check the password back in automatically – the administrator never knows the password.

The software will also keep a history of passwords for each network device. So if network devices must be restored from backup, the then-current password can be retrieved. Had this system of shared management capability been in place at the City of San Francisco, Childs would never have been able to hold the City administration to ransom in the way that he did.

The lesson from San Francisco is that an effective alternative to basic password systems, is needed which offers much greater control and security around access to enterprise networks. The number of application passwords that must be managed in many enterprises today is untenable, undesirable and unsafe. The bottom line is simple: passwords no longer provide adequate protection. ESSO is a proven solution that removes the burden from both end users and administrators, and simultaneously hardens the network against attack through strengthened password policies.

The Childs incident highlights the need for greater control over administrative passwords – and the role that ESSO can play in protecting organisations against sabotage by insiders. If we are to avoid a repeat of what happened in San Francisco, widespread adoption of ESSO with shared and privileged user management needs to be seriously considered.





## World News In Brief

### **SAFRAN To Acquire Motorola's Biometrics Business**

Safran an ID solutions based on biometrics company, this month announced that it has entered into a definitive agreement to acquire the biometric business unit within Motorola Inc. The acquisition has been approved by Motorola and SAFRAN.

Motorola's biometric business unit, headquartered in Anaheim, California, USA, designs, develops, integrates and maintains automated fingerprint identification systems ("AFIS") for law enforcement, civil and commercial customers around the world. The firm serves national, state, county and municipal agencies internationally, and provides integration solutions and systems for more than 300 customers in 40 countries in North America, Europe, the Middle East and Asia.

Jean-Paul Herteman, CEO of SAFRAN said, "This acquisition enables Sagem Securite to strengthen its position in the US market for homeland security where it is already committed to offer world-class identification solutions to government, state and local markets. This acquisition is a continuation of SAFRAN's long history of investing in the US. It is also an important step in our plan to improve our product offering, expand production in the US, and reduce costs."

The transaction is targeted to close first quarter of 2009 at the latest and is subject to customary closing conditions and regulatory approvals.

### **Data Theft Dating Back To 2006 Continues To Concern Deutsche Telekom**

According to the magazine Der Spiegel, a storage device with 17 million mobile telephone data records is still in the hands of unknown parties. The stolen records contain names, addresses and cell phone numbers, and in some cases, date of birth of customers of Deutsche Telekom.

In spring 2006, Deutsche Telekom immediately reported the theft to the public prosecutors office. Within the scope of their investigations, the public prosecutors office was able to recover storage media. Extensive research conducted over several months on the Internet and in data trading places could not reveal any clues indicating that the data had been offered or disseminated on the black

market. Owing to this, Deutsche Telekom assumed that there would be no dissemination of the data. However, Der Spiegel was apparently able to access the data in question via third parties.

"We are very concerned by the fact that the incident from 2006 is relevant once again. Until now, we were under the assumption that the data in question had been recovered completely as part of the investigations of the public prosecutors' office and were safe," said Philipp Humm, Managing Director at T-Mobile Deutschland. "Notwithstanding the fact that the culprits have been at work with a tremendous criminal potential, we earnestly regret to say that we have not been able to protect our customer data in line with our standards."

### **UK MoD Computer Hard Drive Missing**

Computer hard drive containing personal details of about 100,000 of the Armed Forces has disappeared. The information was being held by EDS, which is the Ministry of Defence's main IT contractor.

It is thought to contain more than 1.5m pieces of information, including the details of 600,000 potential recruits and details of passport numbers, addresses, dates of birth, driving licence details and telephone numbers.

### **UK Police To Carry Mobile Fingerprint Scanners**

UK Police could soon be armed with mobile fingerprint scanners as part of the police initiative named Project MIDAS (Mobile Identification At Scene).

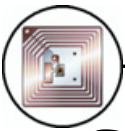
The scheme will be managed by the National Policing Improvement Agency and the hand-held devices are to be rolled-out in 2010.

The Fingerprint scanners will allow police officers to check suspects against the polices's IDENT1 biometrics database.

"It is estimated the mobile fingerprinting system saves about 67 minutes per search and if it were scaled to a national level, as planned under Midas, it would be equivalent to having an extra 336 officers on the beat" said the NPIA.

Tenders are still open for the Mobile Identification At Scene (Midas) scheme.





# California Becomes Second State To Ban Skimming – but is it too little too late?

By Tom Tainton, Smart Card & Identity News



*Tom Tainton*

Earlier this month California became the second state to pass a law making it illegal to steal data from RFID (radio frequency identity) cards. It is hoped the new legislation will help to deter fraudsters from conducting identity theft such as skimming, a practice that is becoming increasingly common among fraudsters and organised gangs. The bill stipulates that anyone found guilty of stealing information from RFID tags can be 'punishable by imprisonment in a county jail for up to one year, or face a fine of not more than \$1500.

There are security mechanisms that issuers can employ to make it more difficult for a fraudster to steal data stored on RFID cards. Unfortunately many don't or do so poorly, so it's hoped the laws could help serve as a deterrent against would-be hackers. But is this really enough to tackle a growing problem? It's unlikely that a criminal will be discouraged by the prospect of a four-figure penalty, an amount of money that pales in comparison to the lucrative benefits of identity scams. In a nutshell, the potential amounts of cash waiting to be snaffled overshadow the tame punishments put in place.

Nevertheless, when the California state governor Arnold Schwarzenegger signed the 'SB31' law he drew support from a number of groups and organisations including the Republican Liberty Caucus, the American Civil Liberties Union (ACLU), the National Organisation for Women (NOW) and the Privacy Rights Clearinghouse. Nicole Ozer, technology policy director for the ACLU of Northern California praised Arnie saying, "By signing SB 31, Governor Schwarzenegger has taken an important step to safeguard the privacy, personal and public safety, and financial security of millions of families."

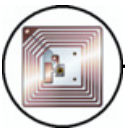
Schwarzenegger had vetoed another related bill also introduced by Simitian. The bill would have required schools to obtain written consent from parents before issuing RFID-enabled cards to students. RFID tags could be used for recording attendances and tracking student whereabouts. The legislation was drafted after controversy erupted at a Californian school regarding student privacy but was eventually barred due to 'parental opposition.'

The most common users of RFID tags are the healthcare and pharmaceutical industry. The technology is used for tracking drugs and equipment as well as identifying patients on health insurance cards. Used in a growing variety of applications, RFID chips store small amounts of data which can be read from a nearby device. Although this provides a great number of benefits it's also easier than ever to steal someone's personal information. A recently published paper in the Stanford Law Review underlined the frailty of RFID tags and the alarming simplicity involved in exploiting the technology. The paper detailed a case in which researchers at the John Hopkins University (a world leader in science and engineering research) cracked the encryption code on chips used in Exxon Mobil gas cards. Armed with this information, and an unauthorised reader, they were able to fill up their tanks with free petrol.

Unlike most, an RFID card does not need to be swiped but can be read automatically without the card-bearer even batting an eyelid. Some cards with RFID capabilities can be read from over several yards making it easier to surreptitiously obtain personal information without their prior consent or knowledge. Of course, RFID technology is not the issue. The chips have enabled customer data to be stored on credit cards, and created 'keyless' entry systems allowing millions of Californians to open locked offices, apartments or car doors. Even passports now carry built-in RFID allowing personnel to be scanned and cross-referenced with other databases.

The issue is identity theft, a crime that is on the rise particularly in California. According to the Federal Trade Commission, there were 45,175 victims reported in the state last year. With 125 victims per 100,000 population, California ranked third in the entire country behind Nevada and Arizona. State Senator Joe Simitian, a Palo Alto Democrat first introduced the bill in 2006, before the proposed law was finally passed in recent weeks. He said, "The problem is real. Until now there haven't been any laws preventing skimming your information, and millions of Californians are at risk."





The legislation makes exemptions for certain emergency situations, such as allowing health care workers to scan an unresponsive patient's health card without permission, in order to help that person. In addition police authorities would be able to view information held on an RFID card if in possession of a warrant. Earlier this year Washington became the first American state to pass a law against stealing RFID data. Any identity theft for the purpose of fraud is classed as a level C felony. That means a criminal convicted in Washington could receive as much as a \$10,000 fine and five years in prison in comparison to just one year and a \$1500 penalty in California.

It's heartening to see positive reactions to the issue, and others are sure to follow suit. There is no doubt that the only way to prevent identity fraud is to introduce harsher penalties for those convicted, and if the problem persists then the severity of the punishments will only increase too. Whether the Californian bill will deter criminals remains to be seen. Until identity theft is taken seriously and stricter legislation is put in place, I very much doubt it.

## World News In Brief

### Warnings Over WiFi Security Is No Longer Secure

Global Secure Systems, an IT security consultancy, announced that a Russian's firm's use of the latest NVidia graphics cards to accelerate WiFi "password recovery" times by up to an astonishing 10,000 per cent proves that WiFi's WPA and WPA2 encryption systems are no longer enough to protect wireless data.

According to Hobson, companies can no longer view standards-based WiFi transmission as sufficiently secure against eavesdropping to be used with impunity, so the use of VPNs is arguably now mandatory for companies wanting to comply with the Data Protection Act.

This is, he said, an interesting step in the evolution of WiFi security, as, it may actually trigger a move back to hard-wired connections in financial institutions who are concerned about data privacy.

"The \$64,000 question, of course, is what happens when hackers secure a pecuniary advantage by gaining access to company data flowing across a WPA or WPA2-encrypted wireless connection. Will the Information Commissioner take action against the company concerned for an effective breach of the Data Protection Act," he said.

However renown cryptographer Bruce Schneier on his blog comments; "just because they can speed up brute-force cracking by 100 times using a hardware accelerator. Why exactly is this news? Yes, weak passwords are weak -- we already know that. And strong WPA passwords are still strong. This seems like yet another blatant attempt to grab some press attention with a half-baked cryptanalytic result.

### TSSA Calls For Urgent Inquiry Into Deloitte Stolen Laptop

UK Transport Salaried Staffs' Association (TSSA) rail union called for an urgent inquiry after a laptop containing personal details of 150,000 workers in the industry was stolen.

The computer was in a bag taken from an employee of Deloitte which until recently was the external auditor for rpm, which administers railway pension schemes.

Deloitte Services include; risk management, security, data quality & integrity and IT control assurance.

Gerry Doherty, general secretary of the Transport Salaried Staff Association, said there should be an inquiry because of the large number of people whose personal details have been lost.

"We are extremely concerned that this personal information affecting well over 100,000 people has gone missing. There will be a lot of worried railway employees who will be concerned about where this information will eventually end up. We need to know precisely what information has gone missing and how security will be sharpened in the future."

The Laptop also contained all the details including names, National Insurance numbers, dates of birth, pensionable salary, earnings and contributions from all UK Vodafone staff.

Vodafone said: "Vodafone is extremely concerned about the breach in security of our employees' personal information and we take the matter very seriously.

