January 2010

Volume 19 • Number 1

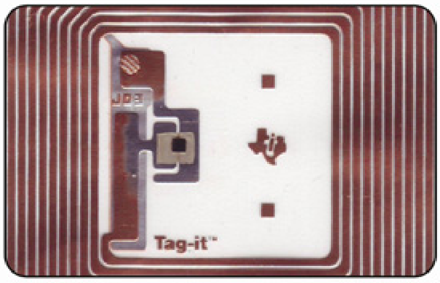
Smart Card & Identity News

Smart Cards, SIM, Payment, Biometrics, NFC and RFID

www.smartcard.co.uk

7 • *Payments security takes centre stage as we head into a new decade*

11 • *Interview with Dr. Jack Pan, Watchdata*



13 • *RFID Accomplishments: From Public Transport Ticketing to Personal Wireless Devices*

18 • *Reducing Merchant Acquirer Fraud in a Changing Payments Landscape*

Gemalto Counts Cost of New Year Bug

"Late Millennium bug" hits Germany leading to over 30 million debit and credit cards damaged and incapable of transactions.

The mishap was reported to have occurred as a result of a programming failure, which left the German credit and automated teller machine (ATM) cards unable to deal with the change in year from 2009 to 2010. About 20 million debit cards known as Girocards or EC cards in Germany and 3.5 million credit cards, were affected by this "Y2K"-like computer bug or a version of the millennium bug 2010 (reports The German Savings Banks and Giro Association or DSGV - Deutscher Sparkassen- und Giroverband).

The bug has left cardholders unable to use their payment cards in drawing cash from the cash machines or make payments throughout Germany and abroad. People were in a state of 'shock' when ATM machines refused to pay-out, as they rejected the plastic money.

Gemalto, the Amsterdam-based giant in security and smartcard solutions, has taken the blame, which apparently will cost around £270 million to put right. The smartcard blunder even caused Gemalto's shares to immediately drop by 3.3 percent.

Continued on page 4….

Smart Card & Identity News
Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group,
Suite 3, Anchor Springs, Duke Street,
Littlehampton, BN17 6BP

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen, Lesley Dann, Suparna Sen

Contributors to this Issue – Suparna Sen, Steve Brunswick, Tom Tainton, Walt Bonneau Jr., Michelle Weatherhead

Photographic Images - Nejron - 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.

Our Comments

Patsy Everett

Dear Subscribers

Well now that Xmas is over it's interesting to talk to friends to see how much shopping they actually did over the internet. Hands up I did about half my shopping on the internet, gadgets for guys are best bought this way far less hassle and nowhere near so boring. I just can't believe how excited these men get over toys (I can't call them gadgets) that seem to have no other purpose in life than making strange noises or flashes. I got a Cajon drum from Father Xmas which I'm sure was negotiated over the internet but I've no idea what happened to my leather boots that I was rather hoping for? Perhaps they're not so easy to buy on the internet.

Anyway the general consensus seems to be that most people are doing a large part of their shopping on the internet, probably more than me. So the question is 'are you worried about the security?' do you have a moment to hear the results?

In every case they were using either a credit or debit card but often with the card information stored at the seller (e.g. Amazon) but nobody was using the security widgets discussed in the Newsletter this month. So the first question surrounded the choice of card,

Would you prefer to use a credit or debit card for your purchases on the internet? The answers were all about the free credit with a credit card or the financial planning offered by a debit card. Nobody seemed to think about the fact that your current account is effectively exposed by the use of a debit card as we discussed last month, I really must get my friends reading this blog!

Do you have any reservations about the merchant holding your card information? Again it was interesting, just about everybody was happy with Amazon. They really do have an enviable reputation probably better than any bank. Also they clearly are a (the?) major player in the internet.

I couldn't resist it so I had to ask 'do you use eBay and how do you pay?' Pretty unanimous again and as for payment it was of course PayPal. So clearly people don't mind PayPal holding their card or bank account information.

So back to the core subject 'are you happy to pass your card details over the internet to an unknown merchant?' Again it was interesting, just about everybody was a little concerned but they all do it.

Pursuing this further what became clear was that people (my friends at least) were confident that in the event of fraud that they would be covered by the bank who would sort everything out. Interesting to note here that a few people thought the credit card company would sort it out, they hadn't fully appreciated that the cards are issued by some bank that is responsible for any problems with the card. An interesting brand discussion could be had here but we'll leave that for another day.

Identity theft was a big issue, people were concerned about some villain using their identity in some fraudulent way but that wasn't directly associated with using the debit or credit card, not until you point out of course that large merchants have been known to lose this information

on rather a large scale which can be used for more than just fraudulent payments on the card, more on this in the Newsletter.

Well we've got there, how about the widget I said, you know the calculator type device that makes your payments more secure like when you are doing electronic banking? You know when you have said something particularly boring when people's eyes glaze over and they immediately change the subject. I had several goes at this but the best I got was what a jolly good idea but perhaps I won't need to use it!

Now we all know the problem is getting worse but who is going to blink first? There are two approaches, either we have to have a more secure way of accessing the internet with software or we have to insert a security widget into the payment chain that the consumer finds effectively transparent. There's an opportunity here for someone. Just as a note one friend has a service from his bank that sends him an SMS when he makes a payment over £25, he loves it and I think I could become quite attached.

See you in Barcelona at the Mobile conference.

Patsy

Contents

Regular Features

Industry Articles

Events Diary

February 2010

2 The Card Awards, The Grosvenor House Hotel, London - www.thecardawards.com

8-10 Security Document World 2010, The Queen Elizabeth II Conference Centre, London

- http://www.sciencemediapartners.com/

9-11 EurasiaRail 2010, Hilton Istanbul, Istanbul, Turkey

- http://www.terrapinn.com/2010/raileurasia/

15-18 GSMA Mobile World Congress, Barcelona, Spain - http://www.mobileworldcongress.com/

24-26 European Card Acquiring Forum 2010, Grand Hyatt Berlin, Berlin, Germany

- http://www.europeancardacquiring.com/

25-26 3rd Annual Card Acquiring Summit, Vienna, Austria

- http://www.jacobfleming.com/jacob-fleming-group/conferences/financial/3rd-annual-card-acquiring-summit

Source: www.smartcard.co.uk/calendar/

March 2010

1-5 RSA Conference 2010, San Francisco, USA

- http://www.rsaconference.com/2010/usa/

3-4 Border Security 2010, Crowne Plaza Rome St. Peter's Hotel & Spa, Rome, Italy

- http://www.smi-online.co.uk/events/overview.asp?is=1&ref=3192

15-19 Cards Africa, Johannesburg, South Africa

- http://www.terrapinn.com/2010/cardsza/

15-16 CEE Cards Market 2010, Radisson SAS Béke Hotel, Budapest, Hungary

- http://www.smi-online.co.uk/events/overview.asp?is=8&ref=36

Source: www.smartcard.co.uk/calendar/

A Cry for Cash in a Cashless Society. . . .Continued from page 1

As per addressing the problem, Gemalto wish to update the faulty cards in the field. It has started distributing a corrective software fix to banks. First the software is installed on their ATM machines. Once a faulty card is inserted into a modified ATM the card is automatically updated with the card fix.

The DSGV approved Gemalto's software fix on January 7, although it might take several weeks for the software to be fully installed by the German banks. The solution would hopefully avoid the need to replace cards that would otherwise be very expensive and time-consuming for the banks, thereby saving up to 263,567,210 GBP ($430 million) of additional cost.

At this stage, according to ZKA (Zentraler Kreditausschuss - the German Central Credit Committee), acceptance of the concerned cards by the ATM and point of sales terminals is widely re-established in the country.

Gemalto has estimated that the whole payment card fiasco could cost between €6 million to €10 million (US$8.7 million to $14.5 million) or 53,326,389 GBP to 88,877,315 GBP to place things right.

ATMs and payment terminals in shops have been reprogrammed so that only the magnetic stripe of the card can be read. According ZKA, approximately 60,000 ATMs in Germany have already started working again, with fewer than 64, 0000 machines yet to start functioning, as per the latest updates.

Gemalto's rival, Oberthur Technologies, whose chips are also fitted in German bank cards, said it had not been affected by Gemalto's hitch.

The BVR group of cooperative banks said the faulty software had affected about 4 million of the debit cards issued by its member banks, amounting to 15 percent of the total payment cards.

The private bank association BDB also reported problems with its 2.5 million cards. A spokeswoman with the privately-held Commerzbank said some of its cards had been affected but again many of its terminals had already been configured to accept the questionable cards.

Postbank, Germany's largest bank and the owner of the country's biggest retail banking network, however, did not disclose whether its cards had been impacted or not, the AFP reports.

According to a Deutsche Bank spokeswoman, its customers remained unaffected by the faulty payment card issue.

Ironically, the bug issue seems to cause damage to more recently-issued cards, which contain a computer chip designed to provide extra security, while the older cards with magnetic strips on the back seem to be unaffected.

Problems remain mainly with credit cards, so the customers are advised to use their debit cards for the time being. At present, there are about 93 million EC cards in circulation in Germany.

There has been a deep concern among German retailers about how the system failure will affect the broader economy. Many people are still unable to withdraw cash or pay, and some have even had their cards 'eaten' by the ATM, which declared the smartcards had expired. Now the German retail industry is calling on banks to compensate traders for lost earnings.

However, smartcard experts believe that on the whole retailers will not be affected as most of the systems that are running in the retail sector are still using the magnetic stripe instead of the microchip, which got corrupted.

It's the dominant public-sector savings banks and cooperative banks of Germany that were worst hit by this sudden glitch.

Other 2010 bugs!

SpamAssassin which included all versions of cPanel, started blocking huge amounts of legitimate email due to a bug in the spam detection rules with the 2010 date.

Just after midnight on New Year's Day, Symantec's Endpoint Protection Manager caused the next big storm, as it stopped working, stopped updating, and started acting weirdly, after been hit by its own 2010 date bug.

Even Kaspersky software experienced massive update problems on December 30th, according to support forums.

Thus all the above incidents highlight the big loophole of the computers to properly handle the 2010 date.

I really wonder how many other pieces of software are currently malfunctioning, and how many are still waiting to be reported! Computers perhaps need more sophisticated technology to bring in smooth online operations, with each passing year.

Gemalto will continue to re-program in the field some 30 million payment cards, using specially modified ATM machines, and although it appears to be a Herculean task, this solution would negate the need for card replacement and offer a ready answer for any similar future problem.

By Suparna Sen, Smartcard & Identity News

World News In Brief

Trade Association Gains Momentum

Smart Card and Identity News can confirm that the AIDC Centre in Barnsley is setting up a trade association on behalf of the smart card and secure eServices industry. This is as a result of senior industry figures privately expressing concerns about being able to deal effectively with apparently conflicting requirements across various public sector organisations. Perhaps the time is now right for the smart media and eServices industry to come together with a unified voice. AIDC (www.aidc.org) is an independent, not-for-profit body and has experience of governmental liaison through its various EU projects. Interested businesses are invited to contact Peter Collins, Marketing Director, on 01226 720780 or by email peter.collins@aidc.org, to discuss the way forward for the supply sector.

$51 Million Awarded in Anti-Piracy Case

Dish Network, EchoStar and NagraStar have been awarded $51 million by a federal court in Florida relating to TV anti-piracy.

The judgment has been made against Robert Ward, who posted pirate software on the internet, which enabled people to receive satellite TV without paying any monthly subscriptions. The court upheld that the posting of the pirate software violated the Federal Communications Act, and that damages should be calculated on how many individuals downloaded the software.

Contactless Payment Terminals at 2010 Winter Olympic Games

US-based global payments technology company, Visa, has entered an agreement with the Canadian subsidiary of beverage company Coca-Cola to equip 550 Coca-Cola vending machines with Visa payWave contactless payment terminals in the Vancouver 2010 Olympic and Paralympic Winter Games. The majority of the Visa payWave enabled vending machines will be located in official venues for the 2010 Games, including the Olympic and Paralympic Villages in Whistler and Vancouver and two Vancouver training centres.

Massachusetts Residents at risk of Online Security Breaches

One in six Massachusetts residents has had credit card numbers, medical records or other personal information leaked or stolen over the past two years, according to records provided to the Globe by state officials.

Thousands of leaks were reported, especially between June and November 2009, occurring in a variety of forms. For example, a laptop theft at the Chicago headquarters at the Blue Cross and Blue Shield Association led 39,000 at risks in Massachusetts.

EMV Authentication Program for Mobile Phones

Arcot announced a new EMV authentication solution for cardholders to authenticate "Card Not Present" transactions using their mobile phones. This new solution 'ArcotOTP' lowers the cost of providing EMV authentication and increases the convenience for cardholders on the go.

ArcotOTP can be used by the hundreds of millions of EMV cardholders, which allows them to use their mobile phones to secure e-banking, e-commerce, telephone orders or a whole host of other transactions where the customer is not face-to-face with the bank or merchant. The new ArcotOTP mobile application, combined with the Chip Authentication Program (CAP) solution from MasterCard, increases security, reduces the risk of fraud, thus making it easier for cardholders to shop or bank online anywhere.

Fines of up to £500,000 for Data Loss!

The Information Commissioner's Office will be able to issue fines of up to £500,000 for serious data security breaches. The new rule is expected to come into force in the UK on 6th April 2010, after getting approved by Jack Straw MP, the Secretary of State for Justice.

The size of the fine will be determined after an investigation to assess the gravity of the breach. Other factors will include the size and finances of the organisation at fault. Individual cases will also be assessed on whether the breach was accidental or deliberate, and how much distress the leak of information caused.

Germany Suspends its £1.5bn Invested E-Health Card Project

The roll-out of Germay's national e-health smart card has been put on hold, as the country's new health minister, Philipp Rösler, has decided a review to be carried out of security and confidentiality.

The national e-health project is one of the largest in Europe and intended to eventually provide every German citizen with an electronic card carrying their health data, medical history, prescriptions, and insurance status.

The e-health card had been planned to be used mostly to simplify health insurance transactions and claims, providing proof of eligibility and in its later phases for medical data and prescription information.

New Mobile Device Payment Technology in Market

XA Worldwide, a leading provider of electronic payment and risk management solutions, has announced the launching of its MobileXR mobile device payment technology in conjunction with its partner technologies, Pago Kiosks and Pago Pass.

MobileXR is the payment processing software within the PaGo kiosk and PaGo mobile application that ensures a secure and safe payment solution without using cash. MobileXR is also available for POS payment infrastructures, call centre environments, ATM/kiosk networks and e-commerce websites. This technology provides electronic payment solutions across unbanked financial businesses, B2B vertical marketplace services and B2B customer services.

Payments security takes centre stage as we head into a new decade

By Steve Brunswick, Strategy Manager at Thales Information Systems Security

Steve Brunswick

As the first decade of the new millennium ends, payments look set to take centre stage in 2010. In spite of the economic downturn, electronic transaction volumes have continued to rise and, as the recession eases, volumes will only increase. At the same time however, the opportunity for fraud grows too. To address this potential threat, the financial services community has been implementing measures to combat the risk of fraud, which seem to be paying dividends. For example, card fraud in the UK decreased by 23 percent during the first half of 2009 when compared to the same period in 2008. However, as the industry continues to strive to retain customer trust it cannot settle for the results achieved to date. The article examines the fraud and security trends in 2009 and discusses what is in store for 2010.

Face to Face Card Transactions

One of the main trends of 2009 is the significant decline in UK face-to-face payments fraud. This trend can be traced back to the UK's adoption of EMV or Chip and PIN in 2003, which had an immediate impact on fraud reduction. According to the UK Payments Administration, the losses on UK high street transactions reduced by 55 percent between 2004 and 2008, from £218.8m to £98.5m respectively. While 2008 figures increased in comparison to the previous year, first half 2009 figures show an encouraging return to the trend of declining levels of fraud.

EMV is mandated across the entire Eurozone as part of the SEPA Cards Framework. Equally, Australia has stepped up its migration to Chip and PIN cards and will ban signature transactions by April 2013 while Canada will not be accepting magnetic stripe transactions beyond 2015. As criminals move away from countries with secure Chip and PIN payment systems, countries that continue to use magnetic stripe technology, such as the US and parts of the Middle East, are likely to be seen as an increasingly attractive target. These regional disparities in face-to-face payment security are unlikely to change significantly in 2010, so countries with magnetic stripe cards could come under increasing attack by fraudsters.

Card Not Present (CNP) Fraud

Strong Authentication

UK banks have spearheaded the fight against CNP fraud through the roll out of two-factor authentication technologies. In 2007, banks rolled out smart card or CAP readers to provide two-factor authentication for their online banking customers and, according to APACS, online banking fraud losses reduced by 33 percent between 2006 and 2007. As a result, Barclays, Nationwide and RBS have all distributed card readers to customers. By making customers strongly authenticate themselves using an unconnected smart card reader and their bank card for online banking, the banks have the identity confirmation required before transfers are initiated. In fact, an announcement by Barclays stated that customers using two-factor authentication for online banking experience no fraud whatsoever.

Despite the initial decline in fraud following the roll out of card readers in 2007/2008, 2009 has seen an increase in fraud. Financial Fraud Action UK suggested that online banking fraud had actually risen by 55 per cent in the first half of 2009. As with the migration to EMV by some regions, the adoption of two-factor authentication by some banks may have left those without this technology more vulnerable to fraud as criminals now know who to target. As a result, attacks can be focused on those customers without access to two-factor authentication technology and this may have resulted in an increased number of successful attacks.

Without two-factor authentication technology, consumers are left open to phishing and other malware attacks that target vulnerabilities in customers' PCs. Which? Computing judged banks without this technology, such as Abbey and Halifax, as having "poor" online security. Both banks require three pieces of information to be entered in full at log-in, making the information vulnerable to a simple keylogger that captures keystrokes or even characters picked from a drop down list to be used later by the fraudster to gain access to the account. One way for all banks to protect their customers and stem the rising tide of fraud would be for them all to roll out two-factor authentication technologies to their customers in 2010.

Securing e-commerce

While 2009 has seen growth in UK online banking fraud, there has been a significant decline in CNP fraud during this time. Much of this is due to increased e-commerce security. So what was done to achieve success in 2009? To date, card schemes have led the charge in initiatives that address e-commerce fraud. Verified by Visa and MasterCard SecureCode encourage customers to register in order to protect transactions with an additional password. The systems allow financial institutions to confirm a cardholder's identity to the online retailer, thus making transactions more secure against fraudsters.

To make e-commerce even more secure, banks should consider extending two-factor authentication to the e-commerce environment. The fact that the infrastructure for two-factor authentication has already been put in place for online banking means that there is a strong business case to employ two-factor authentication more broadly online. With few opportunities to differentiate services, banks should seize the opportunity to extend their security offering to e-commerce and demonstrate to customers that they are reacting to the threat of fraud, improving customer retention as a result.

Protecting cardholder data

2009 also saw increased momentum behind protecting cardholder data as it is stored and processed by banks, payments institutions and merchants. While card scheme mandates require PINs to be protected through encryption, cardholder data has not had the same protection and is vulnerable to fraud. The focus on protecting cardholder data is in large part due to the impact of the Payments Cards Industry Data Security Standard (PCI DSS). This standard aims to prevent any information that could be used to make a counterfeit card or a fraudulent online transaction from falling into the wrong hands and applies to every acquiring bank, merchant and third party that accepts or processes payment cards. It is now mandatory for businesses with over 100,000 transactions a year to either be PCI DSS compliant or be able to demonstrate plans to become so. Furthermore, the European Commission is considering implementing data protection regulation for all companies that accept payments. As a result, 2009 has seen an increased focus on compliance with data security mandates within the payments industry. As requirements will become more stringent over time with the PCI already discussing the new version of its data security standard, meeting regulatory requirements will continue to be a focus for all parties involved in processing payments throughout 2010.

In the last year, U.S. merchants and processors in particular have been extremely active in pursuing end-to-end encryption projects to protect cardholder data throughout the payments network. The Accredited Standards Committee X9 (ASC X9) is working on end-to-end encryption standards, but many organisations have chosen to go ahead with their projects now, with the goal of improving PCI DSS compliance. In the US, PIN debit is another means of improving transaction security, requiring cardholders using their debit card for purchases to enter their PIN, which is validated with the issuer. Like the roll out of Chip and PIN in EMV territories, this does require a Point of Sale terminal upgrade, which can be a barrier to adoption for smaller merchants, or those with integrated tills.

2009 has also seen increased buzz around the use of tokenization as a key way to help secure card data and comply with PCI DSS. Projects using this technology are now being pursued by numerous large merchants. However, there has, up until now, been relatively low awareness of what tokenization is and how it can add to the security mix. Tokenization involves substituting card details (which can be used for fraud) with random numbers (which are useless to a fraudster). So, when an organisation processes a given transaction, instead of tracking the transaction using card details, it uses a random number or token that has been allocated to represent the card. The card details are encrypted and, as tokens are used instead of card details to record and track transactions, far fewer locations use card numbers. Consequently, the opportunity for data spillage or fraudulent interception is significantly reduced.

In 2009, the payments industry put protection of cardholder data firmly on the agenda and efforts to increase security will only escalate next year. End-to-end encryption and tokenization are keys to tackling this issue and 2010 will see more widespread deployment of both these technologies throughout the industry.

The uptake of contactless payments

The adoption of new payment methods will significantly impact upon the payments landscape in 2010. The biggest change is likely to result from the greater adoption of contactless payments. This is due in large part to a series of initiatives from card companies, mobile phone operators and big retail groups. Uptake is likely to be driven by certain players, for example, Barclays has said its plans model a migration of 26 per cent of cash transactions to contactless cards by 2016, which it predicts will double card transaction volumes for UK acquirers.

2009 has seen much talk of the roll out of contactless payments on the mobile and the buzz around this innovation will continue in 2010. Further trials have been recently announced, and more are expected in 2010. However, it is unlikely that it will be rolled out for a few years yet. In terms of deployment in 2010, the focus will remain firmly on contactless cards.

When developing contactless cards, security has been a top priority. The payments industry has added security on both the contactless devices and in the processing network and security measures includes generating a unique Card Verification Value or CVV for each transaction. Additionally, and unlike traditional payments, with contactless it is possible to detect repeat attacks. A 'repeat attack' is where the fraudster obtains all the information from a real transaction and then conducts the same transaction many times over. The fraudster relies on the system that they are trying to attack not realising that it is receiving the same instances of the real transaction. However, the added network security in contactless means that transactions can only be processed once. Consequently, this type of fraud will be more difficult to commit. Furthermore, the processing of some contactless payments does not require the use of the cardholder's name and some cards do not even include the cardholder's account number. This means that there are no card details available for a fraudster to steal. It is clear that contactless payments are relatively robust in terms of security and this bodes well for fraud reduction in 2010.

In summary, the payments industry has seen real progress in security during 2009. Regrettably the battle against fraud is ongoing. We expect to see increased momentum behind the roll out of technology such as end-to-end encryption and tokenization combined with two-factor authentication. These technologies are critical to increasing the security of payment transactions and it would be beneficial to the industry to see their increased uptake next year. As financial institutions come to realise the growing importance of payments, 2010 could see payment security leading the agenda of those financial institutions interested in making the most of the opportunities while minimising the risks.

UK Payments Administration http://www.ukpayments.org.uk/media_centre/press_releases/-/page/732/

World News In Brief

SMARTRAC Producing 500,000 RFID Inlays a Month

SMARTRAC N.V., announced reaching a production milestone in its certified high security production facility in Chanhassen, Minnesota. In December 2009, production of RFID components from SMARTRAC's production location in the U.S. reached 500,000 highly secure ePassport inlays in one single month for the first time. The majority of RFID inlays caters towards high security applications such as ePassports and eID Cards and is manufactured with SMARTRAC's advanced and proprietary wire-embedding technology.

UniRush Introduced Unique Card-To-Card Funds Transfer Feature

US card issuing company UniRush has launched first-time card-to-card funds transfer feature to the RushCard prepaid card. RushCard, a prepaid card business of UniRush, has reported that the new card-to-card funds transfer feature will allow the cardholders to make instant transfers of money via mobile phones. This kind of credit transfer can be made at a fraction of the cost compared to the movement of money through leading wire transfer services.

ACS Launches its New ACOS7 Dual-interface Smart Card

Advanced Card Systems Ltd. has launched its new ACOS7 dual-interface Smart card for the world Automatic Fare Collection (AFC) market.

"All-in-One Card" is a single smart card being used within a city for multiple applications, both for transit and for non-transit payment. ACOS7 supports both contact and contactless interfaces and is complaint with ISO7816-4 and supporting secure e-purse, e-deposit and transactions. ACOS7 can be applied to transportation, retail, property management, car parking, utility supply, etc.

Bill Payments Easier with new iPhone Credit Card Reader

The US iPhone accessory company Mophie has introduced the new iPhone credit card payment accessory and complementary application that makes possible to take credit card payments using the handset.

The peripheral card reader developed by Mophie has been launched at the 2010 International CES consumer technology tradeshow in Las Vegas between 7 and 10 January. The accessory is to be plugged into the iPhone terminal, allowing users to swipe credit cards. The card details can then be processed by an iPhone app that handles the payments.

$30 Million win of Contracts for National eID Program

On Track Innovations Ltd. announced that it had signed contracts relating to a national eID program with total consideration that exceeds $30 million. Revenues from this Project in 2010 are expected to be over $20 million. An advance payment has been received to support the initial stages of the project, which have already commenced.

The award of the project follows a successful completion by OTI of a pilot program and provides for the supply of new biometric-based electronic ID cards and other official documents (relating to birth, death, marriage, etc.), as well as the equipment required for the setup of the document issuing stations country-wide.

LaserCard Corporation Wins Secure Professional Drivers License Project in Hungary

LaserCard Corporation has announced that it has been awarded the contract to supply highly secure International Certification cards for professional drivers by Hungary's Public Transportation Authority. The special five-year certification cards will be issued by the Hungarian government to professionals, like bus drivers, truck drivers, ship captains and airline pilots, who drive or pilot Hungarian registered commercial vehicles internationally. The cards feature LaserCard's tamperproof and highly counterfeit-resistant optical security media, which is intended to store the holder's facial image, biometrics and demographics.

Oxford heading for Historic £2 Million Multi-Operator Smartcard Ticketing System

Bus companies are to sign a ground-breaking deal that will cut the numbers of buses in central Oxford by a quarter, paving the way for the pedestrianisation of the city centre. Another key element of the scheme will be the introduction of a £2m multi-operator smartcard ticketing system in the region that is expected to speed up boarding, allowing passengers to use either company's buses.

World's First Software as a Service PIV Identity Solution for Enterprise

idOnDemand delivers the first PIV full life cycle employee Smartcard solution available as a Software as a Service (SaaS). idOnDemand eliminates the core complexity often associated with traditional in-house Smartcard and PKI implementations and enables organisations to easily deploy and use a secure, multi-purpose, smart identity managed solution. Users can consolidate multiple credentials such as building access cards, remote VPN tokens, multiple usernames and passwords into a single, secure digital and visual identification card that is globally trusted and recognised between organisations.

NEC's Facial Recognition Technology Wins the NIST Multiple Biometric Grand Challenge

NEC Corporation, a global leader in networking, communications and information technology, announced that its face recognition technologies ranked number one among all major vendors in the Still-Face Dataset of the Multiple Biometric Grand Challenge (MBGC) carried out by the National Institute of Standards and Technology (NIST), commissioned by the U.S. Department of Homeland Security.

The facial images evaluated by the Still-Face Dataset were taken by high resolution digital cameras under a variety of challenging conditions, including compressed images used for IC passports, and images taken under poor indoor lighting or direct sunlight. These situations were designed based on anticipated real-world scenarios, and test results have demonstrated high quality performance.

First Large-Scale Rollout of EMV PayPass Contactless Payment Cards in Italy

Gemalto, the world leader in digital security, has announced its supplying of Optelio solution to Setefi (Intesa Sanpaolo) for the first large-scale deployment of EMV PayPass contactless payment cards in Italy. Intesa Sanpaolo is the leading bank in Italy and is among the top banking groups in the Euro Zone, offering its services to more than 11 million customers.

This contactless payment project is developed in collaboration with MasterCard, which will be first of its deployed scheme in the Milan area. The new Gemalto technology provides Intesa Sanpaolo customers to simply tap their card on a reader for purchases of up to 25 euros.

Interview with Dr. Jack Pan, VP of International Business and Marketing at Watchdata

By Tom Tainton, Smartcard & Identity News

Tom Tainton

Can you tell me a little about the history of the company and the success experience of Watchdata?

Watchdata has come a long way since its inception in 1994. This year, Watchdata celebrates its 15-year anniversary, taking pride on its accomplishments in the past 15 years. With several data security and smart card deployments across different market segments around the world, Watchdata cements itself as a world leader in innovative smart card technology.

Watchdata began expanding its overseas market in 2001 and it overseas sales has increased by 102 times to date. Setting cultural differences aside, Watchdata is able to strengthen and gained better recognition from its overseas customers. The international business now accounts for 40 percent of all businesses. In addition, Watchdata has established a full set of effective supply chain networks as well as sales offices to support its growing overseas business and market presence.

Currently, Watchdata ranks among the top five global smart card suppliers and develops its business throughout the countries and regions in Asia-Pacific, India, EMEA and the Latin America. To keep in line with its steps for overseas expansion, Watchdata emphasizes on its core competencies. It also reserved a massive R&D team and established a timely supply chain network ready for deployment.

Watchdata is the only smart card vendor to comply fully with the Contactless ePurse Application Specification (CEPAS). Why is this significant?

This is very significant to Watchdata because after the release of CEPAS, the Land Transport Authority of Singapore invited many world-renowned smart card manufacturers to develop a card that would conform to the CEPAS standard. Through its hard work and dedication, Watchdata beat the competition and successfully won the bid. Taking advantage of the opportunity, Watchdata then developed the smart that conforms fully to CEPAS. Watchdata passed the strict testing criteria in 2007 to provide a CEPAS-compliant smart card. Its in-depth understanding and dedicated research in this technology provided superior speed and distance performance to meet the stringent requirements of the transport card issuers. This therefore, exemplifies Watchdata's commitment and relentless pursuit of excellence in providing innovative products and solutions to its customers.

What is the advantage of Watchdata's products and technology over its competitors?

Watchdata strongly focuses on providing "differentiated innovation" that creates value-added solutions to help customers achieve innovation and obtain new value. Its growing global presence, in-depth understanding and in-field experience gives it an added advantage to drive the adoption of emerging smart card applications across industries that include telecommunication, transportation, banking and finance, government and the enterprise.

Watchdata's knowledge and expertise, such as the CEPAS standard, for example is second to none. The Singapore CEPAS-compliant transport card fulfills the demand placed on multi-application smart cards that need to be innovative. Watchdata plans to bring such knowledge and expertise across the globe providing its customers more secure, fast, efficient, flexible, interoperable and cost effective transport products and solutions.

The R&D team of Watchdata excels in new product and technology development. Its ability to be the first and only supplier (as of this day) of CEPAS-compliant cards speaks volume of the team's capability. In addition, Watchdata continues to explore payment spaces including the EMV market. As a result, Watchdata provided DBS bank of Singapore the first 3-in-1 contactless smart card that combines Visa payment, Visa payWave and transport functionalities in a single-chip smart card. Furthermore, because of Watchdata's superiority in technology development and industry relations, it continues to have in-depth discussions with key industry stakeholders in the telecom, transport and payment industry. Watchdata remains one of the main drivers that coordinates and collaborates among the stakeholders to support the vision of a "cashless society" and making it into a reality.

What's the biggest challenge that Watchdata currently faces in the industry?

The biggest challenge that Watchdata currently faces is the penetration of the banking sector in Europe and the Americas. In order to tackle this challenge, Watchdata hopes to replicate its success in Singapore banking sector in providing multi-application solutions that combine EMV, contactless payment, transport and other applications in a single-chip smart card.

Despite the current economic circumstances do you still see a significant demand for Watchdata technology in the industry?

Yes, we still see a significant demand for Watchdata technology in spite of the current economic circumstances. Watchdata sees the economic downturn as an opportunity and not a threat to its business. Under the current economic circumstances, Watchdata remains optimistic and focuses on the opportunities the emerging markets have to offer, exemplifying its relentless pursuit of excellence through innovation. Watchdata shall continue to provide "differentiated innovation" to help its customers achieve innovation and obtain new value that will ultimately benefit the end customers.

Watchdata continues to expand its overseas market presence, what are the difficulties involved in this?

Watchdata realizes that new entrants to the market will be competing based on low cost pricing. This may work at the beginning but Watchdata ultimately sees that this type of business model is not sustainable. Therefore, Watchdata shall focus more on selling its brand, focusing on winning the respect and loyalty of customers not only with relatively reasonable cost but also with high quality products and solutions. This will be its main driving force to further excel and surpass both present and future market expectations.

What next for Watchdata?

Looking ahead into the near future, the exponential growth and proliferation of smart card technology is well underway. More and more industry sectors such as telecom, transportation, banking and finance, e-government and enterprises seek new solutions to reduce cost while providing value-added services to end customers. Watchdata believes that the convergence of these sectors, such as in the form of a mobile phone and non-card form factors (NCFF), could provide consumers more choices for ubiquitous payment means and more secure digital lifestyle. Thus, Watchdata shall continue to focus providing converged products and solutions as the market adoption continues to grow.

World News In Brief

Barclaycard taps MasterCard for New InControl Account Personalisation Service

Global payment company Barclaycard, part of the Barclays Global and Retail Banking division, has teamed up with MasterCard Worldwide to offer the option of MasterCard inControl functionality.

MasterCard inControl provides cardholders with the ability to set spending controls and receive real-time information about their accounts. The new functionality provided by MasterCard inControl enables Barclaycard to provide a service which allows them to give Barclaycard customers more control over their accounts in terms of going online and setting personalised controls and spend budgets, with SMS alerts or emails instantly sent to tell the customer when they have reached a budget or control set on their credit card.

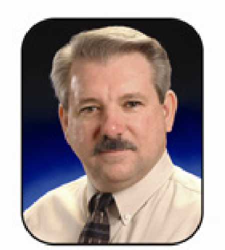
Ukash Expanding in 2010

Ukash, the world's fastest-expanding prepaid-cash issuing estate, continues its international expansion in 2010, with the announcement that the company's e-cash vouchers are now available directly nationwide to consumers in France for the first time, through a partnership with major issuing network la SAF.

On-line issuing is now available to customers in Greece and Hungary through its partnership with Citadel Commerce. This marks another step forward for the global alternative payments provider in achieving its aim of enabling everybody in the world to benefit from safe online payments.

RFID Accomplishments: From Public Transport Ticketing to Personal Wireless Devices

By Walt Bonneau Jr., President, Cubic Security Systems, Inc.



Walt Bonneau Jr.

Radio Frequency Identification Devices (RFID) have become mainstream technology in many, if not most, parts of the world. They are used for security, ticketing, credit and debit purchase, inventory control and many more applications. At the core of these applications is an integrated circuit with antenna that in most cases is electronically standardized through ISO/IEC 14443 (Proximity), ISO/IEC 15693 (Vicinity) or similar standards. For the most part, these devices operate as a passive unit where they are energized by power made available through air coupling from a reader or reader/writer device.

RFID started out in the 1990s as a new and immature technology. Achieving ISO standards by 2001 opened the door to several companies investing in RFID integrated circuits and applications, and since then RFID has developed into a multibillion unit industry. In a relatively short nine years, nearly 20 different RFID circuits have been made available, offering various capabilities and security levels. These circuits and their associated card bodies or other encapsulating formats have achieved significant functional sophistication where they are often selected for use in newly issued government IDs, banking instruments and other security applications.

Many have read that some of these RFID devices and cards have been challenged and/or compromised by moderate to very sophisticated individuals and/or organized groups. As with any technology, there is a constant need to advance the technology to stay ahead of potential threats and obsolescence. The RFID industry has not stood still; it has developed new devices with a high order of cryptology, anti-probing, anti-cloning, key diversification, device "DNA" tracking and other techniques, and has improved or enhanced standards to stay ahead of these challenges.

Benefits of RFID

It is most interesting to step back and evaluate a particular technology to see if it has truly improved our daily lives and equally, benefited in a financial manner. We now have sufficient enough years of adoption and use to evaluate RFID's overall benefits, which of course can be placed in both an objective and or subjective set of slots. For anyone who has had the opportunity to use both magnetic and RFID-based products, it is not too difficult to see the benefits or lack thereof for each product type, especially when the associated application is taken into account.

Clearly in applications like public transport ticketing, the RFID smart card has improved overall reliability, user access and exit throughput (dwell time) for both rail and bus systems. It is interesting that this specific area of application also represented some of the first adopters and remains a significant volume leader for the technology. Every year the transportation industry increases the volume of RFID products deployed in various formats.

One of the more recent product classifications is the Limited Use smart card, which has seen significant growth in the last three years with major transit agencies in Europe, Asia, North America and South America, using over 500 million units a year. It was not until the ANSI-410 standard, which couples directly to ISO/IEC 14443, did Limited Use smart card product adoption accelerate. Some of the first products available were based on NXP's Ultralight (original devices that preceded ANSI-410) followed by devices from Kovio, Infineon and others. The popularity of these Limited Use devices was attributed to companies and organizations requiring or desiring 100 percent contactless smart card systems.

When taking cost into account, many systems integrators and organizations were reluctant to replace single-trip, daily, weekly, and monthly passes that were commonly issued on magnetic cards or tickets. Until just recently, Limited Use cards were simply too expensive for wide distribution. Added competition and advanced production techniques have reduced the cost of these cards to nearly match that of magnetic, if the total cost of ownership is considered. Added security and fraud protection have also made these cards more attractive to operators.

RFID or contactless bank cards using the standard ISO 7810 (ID1 physical format) have also seen significant volume growth in the last two years as various banks reissue credit and debit cards with this embedded technology. Obviously, this is challenging for the issuers of these cards since the transition from millions of magnetic cards to smart cards required point-of-sale reader conversion, issuer and customer education, and the development and acceptance of added security features. The success of these bank cards is still being evaluated, but there is no doubt that the added security and improved durability are proving to be beneficial.

Convergence of Wireless and Consumer Electronics

The advent of "Smart Book" and "Mobile Wallet" are the most recent examples of wireless products providing personal connections to the internet in support of a gamut of web applications via multiple wireless links. WiFi (802.xx), proximity (such as ISO/IEC 14443), vicinity (ISO/IEC 15693), NFC, Bluetooth, GPRS and CDMA are prime examples. These new consumer electronic products are trying to create a virtual book, wallet, real-time knowledge-based system and personal communicator. It is all about being wired whenever and wherever we have the need for instant information and communications, supported by very light weight, low power, secure and cost-effective personal devices. These new wireless products will most likely present challenges to traditional RFID/smart card products in the not so distant future. Already some of these devices integrate various RFID technologies to effortlessly communicate with established reader devices and systems to provide transit, entertainment, security, and banking and identity capabilities.

The developed standards and abundance of available RFID solutions give greater need for these new devices. The end-users must see advantages to consolidate their card and cash wallets to make this switch. Security of an individual's information is going to be essential to have an electronic device that would hold such significant data. It is easy to image the convenience of having a single personal device that would provide multiple applications and reduce the wallet to a virtual wallet. Would it not be compelling to have such a device to let you in and out of your home or business while also providing the equivalent of a transit ticket? To have a device that manages personal funds with real-time banking capabilities?

Time Frame of Change

It is simply not wise to predict when one technology will overcome or replace another. However, it is safe to say that all technologies are overcome by better technologies. This is especially true if the new technology provides additional capabilities with minimal risk to adoption. Further, market and economy factors will greatly influence the time frame of any product adoption. As with the transit and banking industry, these changes simply do not happen overnight and there is often good reason behind these slow technology transitions. First of all, both these industries must carefully manage millions of customers who depend on transit, security and bank products to effectively function day-to-day. Secondly, these industries are addressing very high-volume use requirements where a few pennies or pence receive a very large multiplier, making for large profits or losses. Lastly, the transition period can be long, since both industries typically work on a three- to five-year phase-in and out of technologies.

All of these concerns are somewhat tempered with the need to adopt and promote new technologies when they provide a competitive differentiator or the customer base starts to demand change. This is why these industries are experiencing the type of changes we are presently witnessing. Transit has all but transitioned to smart cards from magnetic cards on a worldwide basis. Banks have mostly moved from magnetic cards to either contact (chip & pin) or contactless cards. In both cases, this has taken nearly a decade to make the change, and there are still systems that have not made the change.

What Comes Next

Devices that provide the same smart card functionality as part of a personal device set should see opportunity. A few substantial events must take place before we experience the next big evolution in methods of payment, ticketing and security. There needs to be a compelling business case, risk assessment and realistic transition period. The product that integrates existing functional requirements with minimal system infrastructure change will find the faster lane toward adoption and volume acceptance. Smart phones are on this path but still face challenges with integration cost and various security challenges as well as legal challenges. As for the integration cost, it takes time to integrate RFID components in a cost-effective manner and ensure they are acceptable system wide. As with smart cards, phone volumes are very large and a few cents of market misjudgement can be very costly.

We are going to see a shift toward a new generation of personal wireless devices. These devices will integrate existing RFID capabilities presently in smart cards, such as Near Field Communications and proximity (ISO/IEC 14443), as well as other communications methods. These devices will transition what was a transit, security or banking application or unique identifier on existing smart cards to a web-based application with limited local information.

Security on new these devices will have to be substantial to prevent loss of personal and financial information under many circumstances. It would not be surprising to see this next wave of wireless devices takes five or more years to achieve market critical mass.

Change is coming, and now it is a matter of how much and when. Most likely, traditional ID1-microprocessor and state machine-based 30 mil thick plastic smart cards will be replaced by these new devices, and remaining smart card usage will transition toward low-cost paper Limited Use smart cards for all other user/application types.

World News In Brief

Low-cost, New Embedded-Process Biometric Iris Cameras in Market

IriTech Inc., has unveiled a revolutionary advancement in its IriCAMM family of low-cost iris recognition cameras. Built around an ARM processor, the new cameras perform on-board processing that greatly reduces the workload for a host PC. This dramatically expands the number and types of acceptable host systems, enabling a wide variety of existing infrastructure to become iris-biometric enabled.

Two important functions embedded within the new IriCAMM cameras are IriTech's proven automated quality-based image acquisition and IriTech's performance-leading matching. The cameras rapidly capture iris images and offer standards-compliant formatting. Matching can be performed on-board or via the host, depending on operational requirements. The IriCAMM cameras are available in single-eye or dual-eye configurations, OEM or attractively packaged, and in either fixed or automatic focus, fitting a wide variety of applications.

HIS in Next-Generation SmartMX™ Security Chip Technology

NXP, has announced a collaborative agreement to license and deploy a hardware intrinsic security (HIS) solution in NXP's next-generation SmartMX™ security chip technology. The partnership enables NXP to utilise Intrinsic-ID's Quiddikey™ solution to secure SmartMX-powered assets against cloning, tampering, theft-of-service and reverse engineering.

Through this partnership, NXP will also be able to implement Quiddikey, the first production-proven HIS solution, to offer cost-effective key storage to secure semiconductor products against today's common security breaches. NXP SmartMX products incorporating Intrinsic-ID Quiddikey are targeted to enter the market in 2011.

Heartland Reaches $60 Million Settlement with Visa Issuers

V3.co.uk reports that the Heartland Payment Systems has reached a record $60 million settlement with Visa issuers to compensate them for losses incurred after the huge data breach in 2008. According to PCWorld.com, 80 percent of the eligible card issuers must accept the deal for the settlement agreement to go into effect. In December, Heartland Payment Systems reached a $3.6 million settlement with American Express.

Suffolk County National Bank Suffers Security Breach

Suffolk Bancorp announced that on December 24, 2009, its banking subsidiary, the Suffolk County National Bank ("SCNB") discovered through an internal security review that an unauthorised intruder accessed certain customers' Log In information via the computer server hosting SCNB's Online Banking system.

Suffolk County National Bank discovered the breach during a routine internal security review, and the officials believe that the intrusion happened during a six-day period between Nov. 18 and Nov. 23 last year. 8,378 Online Banking customers were affected, amounting to less than 10 percent of SCNB's total customers. The company is allocating $351,000 (217,128 GBP) for expenses related to this incident.

Fingerprinting Campaign Helps to Identify Bombers

A fingerprinting campaign in southern Afghanistan is helping international forces identify insurgent bomb-makers responsible for killing increasing numbers of coalition soldiers.

Like detectives at a crime scene, soldiers from Canada and 6 other coalition countries search exploded and unexploded bombs for fingerprints. They share the prints in a database along with other "biometric" information in the hope of finding a match.

Interview with Alain Rollier – Executive VP of Sales and Marketing, AXSionics

By Tom Tainton, Smartcard & Identity News

Tom Tainton

What is Axsionics and how did the company come about?

AXSionics is a spin-off which derived from the University of Applied Science in Biel and was created in 2003. We founded it with the vision of providing a security and identity management infrastructure which can be used by any online service provider, independently from each other.

What are the factors in the success of Axsionics?

The success factors are many. For instance, the AXSionics Passport System works even in the most hostile IT environments where the local PC, Laptop, SmartPhone or the internet connection is under control of an attacker. Also, the Internet Passport is biometrically linked to the physical presence of the end-user without giving away any biometric data and the end-user has one internet passport to manage multiple services. It's important to mention that the technology is extremely cost efficient for service providers who require higher security.

Axsionics has won a series of awards this year, how pleasing is it to be recognised by the industry?

We are very pleased that industry experts recognize the strength of the AXSionics Passport System which provides great benefits to all the stakeholders. In particular, the industry recognized some key elements of the solution, including the 'Trusted Display' approach and the end-user controlled biometrics. Both elements enable the service provider to benefit from a biometric authentication without having any biometric data under anyone else's jurisdiction – in simple terms, the user has absolute control. This implementation was also recognized in the EU FIDIS, a network of excellence about the Future of Identity in the Information Society.

What are the issues associated with smartphone and internet security?

Smart phones share the same issues surrounding security as a PC or Laptop, plus a couple more which come from the additional interfaces. By nature – having a lot of interfaces like voice communication, machine to machine communication, internet traffic and a operation system on the same platform is not helping to secure devices. We believe a shift in thinking is required. It will always be impossible to fully secure a Smart phone, Laptop or PC. The question we have to answer is, 'how do we make sure that identities and transactions are always secure when this is the case?' Essentially, this is what has driven our thinking at AXSionics and thus we have developed a solution that provides this security regardless of how unsecure all the elements in the chain are.

How do Axsionics solutions eradicate these problems?

Our solution works regardless how secure or unsecure the operating system of the Smart phone, Laptop or PC is. We use the Smart phone, Laptop or PC and the internet connection only to transport encrypted information from the service provider to the AXSionics Internet Passport. It's very secure, doesn't drive usage costs and is very convenient for the end-user. It works for simple authentication as well as for transaction verification and secure short message distribution.

Will companies and individuals be able to afford these solutions?

We see that the accumulated costs companies are paying to secure their online assets are constantly rising. We are providing a solution that is increasing security and reducing cost at the same time. The solution is available as a managed security service or a private controlled solution.

What are the main challenges facing the company in 2010?

One of the major challenges was to pass the stringent validation criteria and have the first Swiss Bank introduce the Internet Passport to its end-users. Obviously, this is a big step in the history of our young company and one we are proud to have achieved with the help of the BEKB. Our next challenge is to replicate this success in the many other projects we are working upon.

What next for Axsionics?

Since every Internet Passport can be used independently by more the 100 Service Providers the next step is building and developing the Ecosystem where 'The Internet Passport' can be used and the model replicated to be successful in different regions of the world.

World News In Brief

Motorola and VTech Resolve Patent Litigation

Motorola, Inc. VTech Communications Inc. and VTech Telecommunications, Ltd. have announced that they have entered into a Settlement and License Agreement that will end their pending patent litigation in the Eastern District of Texas.

Although the terms of the settlement are confidential, VTech's license and consideration is consistent with Motorola's intellectual property-licensing program, which is licensed extensively throughout the telecommunications industry. The lawsuit related to six Motorola patents asserted against VTech.

US Army Website Compromised by Hackers!

A website belonging to the United States Army was fully compromised by a Romanian grey hat hacker. The hacker has disclosed an SQL inject (SQLi) vulnerability, in the website called Army Housing OneStop that is used to provide information about military housing facilities to soldiers.

The Army Housing OneStop (AHOS) is "the official Army website for soldiers who need information about Military Family Housing (MFH), Unaccompanied Personnel Housing (UPH) and/or Community (Off-Post) Housing. It includes both comprehensive and quick-reference information for Army installations worldwide". It has been found that the hacker stumbled upon passwords stored in plain text, a major security oversight.

mophie Announces New FeliCa Card Payment Solution for Japan

mophie, a provider of intelligent case solutions for the iPhone and other Apple devices, announced a collaboration with Flight System Consulting Inc. (Tokyo Japan), and Focal Point Computer Inc. (Tokyo Japan) to develop a mobile payment solution for FeliCa technology. Available in spring 2010 in Japan marketplace, FeliCa will allow users to instantly read and write electronic money card information using only the iPhone device and marketplace FeliCa App.

Philippines Supreme Court says No to RFID

The Philippines Supreme Court has temporarily prohibited the Land Transportation Office (LTO) from collecting fees for the new car identification system that it implemented beginning on from January 1st this year.

Acting on a petition by several party-list groups, the high court has issued a status quo ante order on the radio frequency identification system (RFID). The status quo ante order effectively directs the LTO to observe the situation prevailing before the filing of the petition.

Streetcar App now Online!

Streetcar announced its new app for iPhone and iPod touch is now available from the App Store. The Streetcar App enables users across the UK to locate, book and open a car using their iPhone or iPod touch coupled with smart card technology.

Users can unlock the rentals using either their iPhone or iPod touch, or a remotely activated smart card. Once the customer is finished with the car, he or she can return it to a dedicated Streetcar parking space.

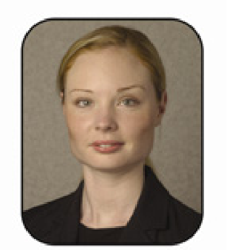
Leading Provider of PIV Cards for 4th Year in a Row

Oberthur Technologies, a global leader of smartcard and high security solutions, has maintained its position as the leading provider of FIPS 201 compliant Personal Identity Verification (PIV) cards for the fourth year in a row, after winning two new government contracts - bringing the company's total number of Federal Government agencies to 100.

The HSPD-12 directive sets the requirements for a common identification card that all Federal Employees and Federal contractors must have. FIPS 201 sets the standard PIV requirements.

Reducing Merchant Acquirer Fraud in a Changing Payments Landscape

By Michelle Weatherhead, Manager of EMEA Risk Solutions - ACI Worldwide



Michelle Weatherhead

New regulation, more competition through new market entrants, such as Payment Institutions (PIs), and changes in technology are forcing the 'traditional' financial institutions to reconsider existing business models. Merchant acquiring – an important part of many banks' business – is not immune to these changes. In fact, merchant attrition has become a growing problem as the economic slump has led to unpredictable consumer spending and affected growth in transaction volumes. However, as new technologies are deployed at the point-of-sale and the power of merchants increases, acquirers have become an increasingly important part of the card acceptance value chain.

Consolidation in the merchant acquiring sector

The changing payments landscape has significantly impacted the number of merchant acquirers in this sector, as in the rest of the payments industry, has seen a wave of consolidation. These mergers and joint-ventures have resulted in a relatively small number of major players across the globe and the trend is likely to continue. The increasing power of merchants, falling merchant service charge (MSC) levels and ever tighter margins have also contributed to this trend.

In addition, new and changing regulation, such as the SEPA Cards Framework (SCF), has put pressure on acquirers, driving standardisation of the interface between merchants and merchant acquirers. This aims to deliver "a consistent merchant experience... when there are no technical or practical barriers preventing SEPA merchants from accepting all SCF compliant cards." Within this increasingly international payments landscape, cross-border acquiring has naturally taken off in recent years. Originally developed for the airline industry in the late 1990s, increasing demand from multinational retailers has led to the emergence of new pan-European and global merchant acquirers. In addition, the increased popularity of e-commerce has all but removed country borders from a consumer perspective.

With these pressures and changes that merchant acquirers are facing, the main focus of the industry has been on improving efficiency and reducing costs. However, retailers are increasingly demanding more accurate and efficient systems at lower prices. As such, acquirers need to look at the wider services that they provide in order to add value and to differentiate themselves from the competition.

Traditionally, the main functions in merchant acquiring include vetting new customers, setting up merchant accounts and capturing, authorising and settling transactions. Most importantly, however, merchants rely on the merchant acquirer for fraud control and monitoring. In 2009, the UK Payments

Administration (formerly APACS) reported that UK merchant fraud had grown by 26 per cent to £47.4 million, the largest jump in criminal activity in payments for all card activity[1]. Consequently, it is in this area where acquirers can gain a significant competitive advantage by providing merchants with additional tools to prevent fraud.

Identifying merchant fraud and preventing it from happening

The potential exposure to charge-backs for disputed transactions, merchant fraud and factoring – when one unregistered retailer compensates another legitimate retailer to use an account to process transactions – are issues that merchant acquirers are regularly faced with. As such, there is a strong business case to support the merchants' own fraud detection processes, as fraud and unexpected charge-backs affect a merchant's cash flow and can even result in bankruptcy. This can be very costly for acquirers who are ultimately responsible for each merchant's activity and therefore will be held financially accountable if a merchant is unable to meet its obligations. Online businesses in particular can become unviable if a large number of charge-backs occur. Acquirers have fraud investigation teams in place that can help to protect merchants against charge-backs and charge-back losses.

It is therefore in the best interest of acquiring banks to thoroughly monitor their customer base, in particular high-risk retailers, such as those selling electronic gadgets or jewellery. The first step in this process is to ensure that the correct merchant category code (MCC) is assigned, according to MasterCard or VISA regulations. MCCs are used by card issuers to categorise, track or restrict certain types of purchases. It is important to realise, however, that the acquirer is actually the hidden link in this relationship, having greater visibility to prevent types of fraud such as business format change fraud where merchants who run certain types of high-risk businesses lie about business practices when applying for a merchant account. In these instances, a hold can be put on the current accounts if necessary.

While acquiring banks are in a prime position to pick up on fraud trends, with visibility over a much wider range of transactions compared to the issuing banks, an active investigations unit may also serve as a market differentiator for merchant acquirers. For example, an acquirer can flag an unusual spend pattern at a merchant or device that does not fit the expected trading pattern. These might serve to supplement the merchant's own efforts of protecting their bottom line.

Furthermore, insider fraud has moved to the top of the agenda for merchants and reports state that it has increased as a result of the recession. Merchant acquirers can help identify fraudulent usage of cards at retailers and detect a compromised card, protecting the retailer from an unexpected rise in charge-back rates. For example, if an unusually large number of refunds are being processed at a single point-of-sale, this could be the result of a single employee acting fraudulently by processing payments, then refunding them, to avoid credit card charges. This can be pinpointed by the acquirer, providing the merchant with valuable information in their fight against insider fraud.

Sharing experiences

Sharing the knowledge between the acquiring banks and the issuing team is an opportunity for both parties to improve their offering to merchants. By proactively engaging in discussions on how to prevent and detect merchant fraud and improving the communication and knowledge sharing within the different parts of the industry, merchant fraud can be prevented much more effectively.

For acquirers and issuers to work effectively together, it is important to acknowledge their differing priorities and time constraints. The issuer effectively operates in near real-time for fraud detection and prevention, and is likely to block cards and payments that are deemed high risk. The maximum spend on the credit card, which is at around £5,000[2], limits the potential losses that the issuer can suffer from one defrauded card. However, on the acquirers' side, fraud investigations tend to span a longer timescale and usually involve building relationships and providing education and support for merchants. When a merchant is fraudulent, the losses are unlimited and can escalate very quickly within a short space of time.

Acquirers are faced with many of the same fraud issues as the rest of the payments industry, as well as new legislation regulating the space. While not all acquirers have the ability to immediately spot fraud patterns, they already focus on monitoring and investigating their customers to prevent merchant fraud. However, the true opportunity for acquirers lies in offering value-added services and in the technology to help their customers prevent fraud. That way, acquirers can differentiate themselves from their competition. In an industry that is characterised by increased consolidation and high levels of competition, and where revenues and profits rely heavily on reputation, this can only be a step in the right direction.

[1] http://thefinanser.co.uk/fsclub/2009/04/index.html

[2] http://www.debtwizard.com/news/politics-and-economey/429-uk-debt-numbers-for-november-2009