Smart Card Alliance

Smart Card Talk

A quarterly newsletter for members and friends of the Smart Card Alliance

May 2015

In This Issue:

On the Web:

Will Healthcare Warm to Security?

The impact of secure chip technology has varied greatly in various markets because of the separate and unequal strength of market drivers in each segment. I expand on this theme and more in my letter in this quarter's Smart Card Talk newsletter. We also have an update on Alliance Councils, a Member Profile on Ingenico, new CSCIP and CSEIP recipients, and much more.

Sincerely,
Randy Vanderhoof
Executive Director, Smart Card Alliance

Click to Read Letter ...

Feature Article:
The True Cost of Data Breaches in the Payments Industry

Data breaches are a growing problem globally, with every industry sector affected by breaches. What is the true cost of a data breach? This month's article defines a comprehensive list of costs for payments industry stakeholders to assess the true cost of a breach.

Click to Read More …

Member Profile:
Ingenico Group

In this issue, Smart Card Talk spoke with Allen Friedman, Director of Payment Solutions at Ingenico Group, North America, where he is responsible for Ingenico Group's EMV Payment Solutions and the EMV implementation strategy in the United States.

Click to Read More …

Smart Card Alliance Events

Transportation Council Meeting
June 9-10, 2015
Washington Convention Center, Washington, DC

Smart Card Alliance Government Conference
June 9-10, 2015
Washington Convention Center, Washington, DC

Smart Card Alliance Member Meeting
October 4-6, 2015
Arizona Grand Resort, Phoenix

Smart Card Alliance NFC Solutions Summit
October 7-8, 2015
Arizona Grand Resort, Phoenix

Will Healthcare Warm to Security?

Dear Members and Friends of the Alliance,

Over the last decade, the adoption of smart card technology has seen significant but uneven growth, depending on which markets and applications you have interests in. This disparity is a result of the differences in the business and technology needs for security in markets like consumer payments, government and commercial ID cards, and health IT. The impact of secure chip technology has varied greatly in these markets because of the separate and unequal strength of market drivers in each segment and the environment for smart card investment and stakeholder adoption. Like farmers planting seeds in the fields in springtime, some plants may produce very little because the conditions were not right at the time or there was a sudden and unexpected change in the environment. If farmers are patient enough, they may see conditions change over time, and what was once a harsh environment may now be very conducive to a rich harvest.

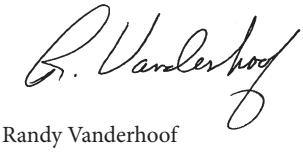
In the case of consumer payments, the market conditions were primed for investment and rapid growth back in the late 90's when American Express, MasterCard and Visa began a major issuance campaign with financial institutions, only to see those ripe conditions dry up and fade away under the weight of a major recession and lack of merchant and consumer buy in. The market sprang to life again in 2004-2005 with the introduction of ExpressPay, PayPass and payWave contactless cards, keyfobs, and mobile stickers, only to see weak consumer and merchant acceptance again stifle momentum and then get hit with the financial market meltdown and economy crash in 2008. Only after the banking industry got back on its feet in 2011 and consumers started spending again did the next big investment in chip cards for the consumer banking industry happen with the major payment networks' alignment on an EMV liability shift. Today the market is overflowing with chip cards for payments – to the tune of 50 million to 75 million cards A MONTH entering the U.S. market in 2015. That is being matched by between 4 to 6 million new POS terminals being installed in preparation for consumers to start using their chips in retail stores instead of magnetic stripes

The government and consumer ID market over than same decade went from non-existent, except for a few million DoD Common Access Cards, to over 15 million government-issued ID cards and more than 100 million electronic passports, driven by the need to enhance the security of our federal government enterprise and our borders after September 2001. Unlike commercial markets and smart card adoption, the weight of the federal government directives (HSPD-12) and legislation (The Visa Waiver Program of 2006) produced a dramatic change in requirements that resulted in a very steady and sustained growth curve for smart cards. That growth curve has flattened in 2015. The federal government has issued cards to 90+% of all eligible government employees. Plus nearly everyone who possesses a U.S. passport today has had a new ePassport issued to them by now, since they expire every 10 years. The government has also been a recent driver in the payment cards market with the President signing an Executive order mandating that all federal programs that issue credit, debit, and benefits cards to citizens must issue chip and PIN cards; and those departments who accept payments must be able to accept chip and PIN cards by the end of 2015. Although smart card usage as an access credential for validating citizen identity at the border and enabling access to secure networks has lagged behind card issuance, there is no concern that these security devices are going to go away anytime soon.

Which leaves us with the least mature smart card market today – the healthcare market. This is a market that has not benefited from any significant market drivers or extraordinary events to stimulate a rapid change in demand for secure chip cards. The HITECH Act of 2009 created a framework for government and commercial investment in electronic health information and health data exchanges that eventually stimulated demand for secure identification and authentication of individuals and sensitive health data. However, the first 5 years were spent changing the way health IT systems are designed and driving healthcare providers to adopt new electronic health records and establish exchanges to move data across newly connected health information highways. Meaningful use is the term most used to describe transforming the way electronic patient data is handled. There has been no outcry yet for how to protect this data or how to securely identify all of the patients, healthcare providers and insurers with secure chip technology. That is beginning to change. In 2014, the Workgroup for Electronic Data Interchange (WEDI) collaborated with the Smart Card Alliance on how the insurance industry could use smart cards and biometrics to secure access to health information. Last month, the Government Accountability Office (GAO) published a report on the Potential Uses of Electronically Readable Identity Cards for Beneficiaries and Providers. This report evaluated several card technologies for the Centers for Medicare and Medicaid Services (CMS) to consider so that Medicare cards could be improved to electronically authenticate beneficiaries and providers, electronically exchange beneficiary medical information, and electronically convey beneficiary identity and insurance information to providers.

It is encouraging to see the healthcare market beginning to look at security in similar ways that the government security market and the consumer payments markets have already discovered. Perhaps it will take another decade to get to the same level of adoption. Or there may be some major event like a colossal health information data breach to stimulate faster action. The Smart Card Alliance will be at the center of this effort for years to come. Plus we can look back on the consumer payments market and government ID markets and feel proud of these smart card industry accomplishments. As a reminder: the 2015 Government Conference is June 9-10th in Washington DC. There is still time to register for the early registration discount.

Sincerely,



Randy Vanderhoof
Executive Director, Smart Card Alliance
rvanderhoof@smartcardalliance.org

Understanding Stakeholders Requirements for Change

Dear Members and Friends of the Smart Card Alliance Latin America (SCALA),

Sometimes when we are far away it is hard to understand the details of a particular situation. We try to solve these problems with formulas that are supposed to be universal in hopes to make a significant impact on their resolution. Others decide to avoid influencing the outcome by not getting involved and letting each make their own decisions and not providing any guidance on improving the outcome. This is why it is important to strike a balance between guidance, impositions, and non-interference.

The American psychologist Abraham Maslow once said, "If you only have a hammer, you tend to see every problem as a nail." In my view, many parts of the world are in turmoil due to financial, military, social, geographic/environmental, and religious unrest. Some of these are situations so complex that at times they appear to be interrelated. Historically established structures are challenged to come up with solutions to more complex problems using tools that seem antiquated for today's more sophisticated population. The tools used by these established structures are no longer working to solve the basic underlying problems of society and newer more effective tools are needed.

Technology seems to provide the tools that can relieve some of these social tensions. For example, in the past month, SCALA presented to the Inter-American Development Bank and International Monetary Fund a vision on how transportation could serve as a key pillar for financial inclusion in Latin America through the use of open payments systems. The objective would be to move the fare collection systems, which are now closed loop in nature, to become open loop with the EMV standard, allowing the use of financial payment cards in the transportation system. In Latin America, the expected result would be that a portion of the unbanked population that uses transportation systems would gain access to bank accounts and financial services. Other information could also be used for the development of a financial risk assessment and history such as ridership, transactions, and microcredits on fares.

Financial inclusion has been discussed since the early 2000's, but still over 50% of the population in Latin America is unbanked. This has created significant income inequalities and lower GDP growth. Contactless smart card technology can help to not only create convergence among different vertical markets, but can also solve fundamental problems in our society.

SCALA also established a meeting with the Organization of American States (OAS), other regional international organizations, and local governments to discuss their need for regional integration for economic and social development with the focus on an individual's credential. In this sense, our organization had the opportunity to obtain their feedback and to align strategies on our industry-led initiative to create an interoperability specification for all of the national identity documents (NID) in the region using smart card technology.

I am pleased to announce that the feedback received from both local, regional, and international government led organizations has been positive, increasing the number of stakeholders who buy-in and commit to support this initiative.

SCALA plans to release a detailed framework for collaboration and development of the interoperable specification for national identity documents during our SCALA Mexico Summit, being held from July 7th to 9th, 2015 at the Marriott Hotel – Reforma. This event will gather the key decision makers from government agencies, transportation authorities, fare collection system providers, payments organizations, and technology solution providers to discuss the impact, benefits, and the future of integrated circuit cards (ICC) in mobile and wearable devices.

Our organization has spent a significant amount of time helping industries influenced by our technology to understand the benefits, opportunities, and value added with the use of integrated circuit cards. We have also embarked in several industry initiatives that we feel can help resolve some of the key problems being faced in our region and by different vertical markets. This has led us to the understanding that in order to be able provide a significant long-lasting solution, we need to first understand the reality of our stakeholders, their challenges, and the goals they are trying to accomplish with our technology. We also have to listen to their needs as we develop solutions for their problems, addressing their key issues and understanding their root causes.

This can only be done with an engaged group of members and by counting on their support to lead the charge in improving best practices, industry relations, and overall sense of collaboration among companies for specific initiatives. We invite all of you to join our industry initiatives by becoming part of the Smart Card Alliance Latin America chapter organization.

Sincerely,

Edgar Betts
Director
Smart Card Alliance Latin America (SCALA)
ebetts@smartcardalliance.org
www.sca-la.org

ingenico GROUP

Allen Friedman

In this issue, Smart Card Talk spoke with Allen Friedman, Director of Payment Solutions at Ingenico Group, North America, where he is responsible for Ingenico Group's EMV Payment Solutions and the EMV implementation strategy in the United States. Prior to joining Ingenico Group, Allen worked for Vital Processing Services (now TSYS Acquiring Solutions) in Tempe, AZ, beginning in 1999. During his 15 year tenure he held a variety of management positions in technical support, solutions implementation, and Product Management. Most recently Associate Business Development Director, Allen was responsible for the core authorization and capture platforms, payment forms and connectivity solutions, and led the EMV implementation strategy for the merchant segment of TSYS. Allen is an active contributing member of the Smart Card Alliance Payments Council, and serves on several Working Committees for the EMV Migration Forum.

1. What are your main business profile and offerings?

Ingenico Group is the global leader in seamless payment, providing smart, trusted and secure solutions to empower commerce across all channels, in-store, online and mobile. With the world's largest payment acceptance network, we deliver secure payment solutions with a local, national and international scope. We are the trusted world-class partner for financial institutions and retailers, from small merchants to several of the world's best-known global brands. Ingenico Group has led the payment terminals space for the past 30 years, with more than 27 million terminals installed worldwide. We work with more than 1000 acquirers and banks, and our solutions can process 300 different payment methods. We do business in about 170 countries. At a high level, Ingenico Group has three divisions: Smart Terminals, Payment Services and Mobile Solutions.

2. What role does smart card technology play in supporting your business?

We are in the payments business, so in that context smart cards are primarily EMV/chip cards – the new credit and debit cards that are replacing older magnetic stripe cards, which are very susceptible to counterfeiting and fraud. Right now, there is a huge shift taking place in the U.S. – we are the last developed country in the world still using magnetic stripe cards. As a result, much of the card fraud in the world has migrated here. In order to try to eliminate that, the U.S. is finally moving to the EMV standard. EMV stands for Europay, MasterCard, Visa – the three card brands that initiated the standard years ago. EMV cards rely on a chip rather than a mag stripe for authentication, and they have been proven to be highly secure as compared to mag stripe.

In October 2015, the major U.S. card brands will initiate a liability shift – merchants who are not able to process EMV card payments will assume liability for any fraudulent transactions they process. Merchants who do upgrade to EMV card processing will still be covered by the card brands in the event of fraud.

> **Ingenico Group is in a great position to help merchants pull all of these trends together, providing a seamless payment experience for customers across online, in-store and mobile environments.**

As a result, most merchants – especially the very large ones – are gearing up to accept EMV card payments. This requires a lot of work and in some cases all new software and hardware. It's a big change for U.S. merchants and for the overall payment acceptance infrastructure.

Ingenico Group has been through this transition many times in many countries, so we know the process well, and our customers are really benefiting from that experience.

3. What trends do you see developing in the market that you hope to capitalize on?

Well, EMV of course is a big one. Another is NFC, which is the technology behind a lot of mobile wallets including Apple Pay. Also called "contactless," it's the technology that enables customers to tap a chip card on a special reader in order to pay. We've seen in every other country that NFC quickly follows EMV. That's because dipping chip cards into payment terminals tends to slow things down a bit. It's not quite as fast as a swipe. And those few seconds per transaction can really add up for a high-volume merchant. Hence, most merchants want to accelerate things with NFC/contactless technology, which also relies on EMV cards.

Ingenico Group has been shipping EMV- and NFC-enabled terminals in the U.S. for almost three years – we knew based on our experience in other countries that merchants would eventually want both. Not all our customers immediately turned those capabilities on, but they all have the ability to. And now that banks are starting to ship chip cards to customers – one of my colleagues received four chip card replacements in just one week recently – merchants are starting to activate their EMV and NFC capabilities.

Another trend we're seeing a lot of is interest in is enhanced security, due to all the high-profile card breaches merchants experienced over the past year. Ingenico Group recommends an approach called Point-to-Point Encryption, known colloquially as P2PE, which ensures card data is never stored at the point of sale, so even if hackers were to access the POS, they could not get any card data. Another is tokenization, which involves replacing a customer's account number with a surrogate value called a token, which is meaningless to anyone except the issuer. Hence, if hackers accessed the system, they would only find meaningless tokens instead of card data. We are doing a lot of work with merchants right now implementing P2PE and tokenization along with EMV, as they are complementary technologies.

Semi-integrated payment solutions are another trend we are following. This approach separates the payment application and device from the merchant's POS application and device, allowing for communication of non-sensitive data from one to the other to facilitate transaction processing. The result is that sensitive cardholder data does not enter the merchant's POS system, enhancing security.

A fifth trend is mobile POS, or mPOS – mobile payment acceptance solutions for use in store (think line-busting) or out of store (like pay-at-the-curb, pop-up stores and community events). BI Intelligence recently published some new research that found that by 2019, nearly 80 percent of merchants will have at least one mPOS terminal in place. That's 4 out of 5 merchants. Those terminals will need to be secure and EMV and NFC enabled. Ingenico Group was first out of the gate with both EMV- and NFC-enabled mPOS solutions in the U.S., thanks to our international experience in this area.

Ingenico Group is in a great position to help merchants pull all of these trends together, providing a seamless payment experience for customers across online, in-store and mobile environments.

4. What obstacles to growth do you see that must be overcome to capitalize on these opportunities?

Testing and certification queues are a huge issue right now. There are a lot of changes taking place in the U.S. payments infrastructure, and application changes are subject to testing and certification at many levels, both in-house and by third parties who are up and down the payments chain. Those third-party certifications can

> **We've been involved in crafting white papers on technology and policy, and have both shared and gathered knowledge that's critical to moving our industry forward. We're giving and getting a lot of insight into market needs.**

cause bottlenecks, especially as that October liability shift deadline gets closer. Companies who wait too long to get into testing queues will find themselves out of luck in terms of meeting that deadline.

We also see a real dearth of information in the mid-tier of merchants. The very large merchants tend to have their own robust IT departments or ongoing relationships with application developers, and they started prepping for EMV early on. Very small merchants tend to rely on acquirers, who just provide them with a new terminal and help them turn it on. But the mid-tier doesn't have the benefit of that large IT group, or the handholding acquirer. They aren't always properly educated about the need for EMV or the complexities of rolling it out. The partners in this space sometimes aren't as conversant about the technology. We think out of all the merchant tiers, the mid-market is least likely to be prepared for the liability shift.

The impact of that may be, I think, a migration of fraud from the top tier to the mid tier, unless and until they are prepared to support EMV.

Another big obstacle here in the U.S. has been implementation of the U.S. Common Debit AID. The U.S. has some unique regulations regarding debit transactions. The new requirements, updated for EMV, did not become available until late in 2014. At that point, merchant application development for EMV credit was already underway, so EMV will be implemented in phases: credit cards first, and debit cards later.

5. What do you see are the key factors driving smart card technology in government and commercial markets in the U.S.?

Well, President Obama issued an executive order requiring federal agencies that accept or issue credit or debit card payments to adopt EMV technology and specifically chip and PIN. That's obviously driving demand for EMV-capable systems within the U.S. government. In the commercial space, that EMV liability shift is a huge driver. Merchants don't want to take on liability for card fraud.

6. How do you see your involvement in the Alliance and the industry councils helping your company?

Our participation in the Smart Card Alliance Payments Council and EMV Migration Forum (a chapter organization of the Smart Card Alliance) in particular, gives us a voice. We've been able to learn about and provide input on where Alliance member resources are used and which Alliance projects are implemented. We've been involved in crafting white papers on technology and policy, and have both shared and gathered knowledge that's critical to moving our industry forward. We're giving and getting a lot of insight into market needs. Hopefully Ingenico Group's international perspective and experience has been helpful to our peers in the Alliance.

7. What are some of the challenges you see confronting the smart card technology industry?

From an EMV perspective, the biggest challenge right now is reaching that tipping point of payment acceptance. Once the majority of transactions are being processed using EMV technology, we'll start to see a major impact on counterfeiting and fraud. There's a bit of a chicken and egg problem right now, as most consumers are still equipped with their magnetic stripe cards. But that's starting to change – about half of my cards are now chip cards, and the number is growing each month.

Member point of contact:

Allen Friedman, CSCIP/P
Director of Payment Solutions, North America /Ingenico Group
allen.friedman@ingenico.com
(T) 678-456-1726
(M) 770-605-6450
http://ingenico.us/emvportal

The True Cost of Data Breaches in the Payments Industry

ISO/IEC Standard 27040 defines a data breach as a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data that is transmitted, stored, or otherwise processed." In other words, a data breach results in the intentional or unintentional loss of secure or personal information. Data breaches can involve any kind of data: financial information, individual identity information—even data that is considered to be intellectual property.

Data breaches typically result when an individual or group of individuals accesses a logical or physical infrastructure, including hard drives or database information that may be stored unencrypted. Bank card data breaches are usually achieved through one or more of the following:

- A skimming device
- Malware that infiltrates the computer system that manages or processes banking or personal information
- A phishing website
- Key logging to steal PIN data
- A listening device that taps into telephone lines to intercept unencrypted information
- Employee negligence
- System failure

Most bank card data breaches are a result of skimming or a database compromise which can occur due to one of the methods listed above. Traditionally, skimming requires the installation of a physical device, most commonly at an unattended location, such as an ATM. A total of 87 percent of reported skimming attacks occurred at unattended ATMs. [1] Data can also be skimmed logically, using wireless Bluetooth devices or by replicating the database records that temporarily hold payment card data. Other recent major data breaches resulted from malware installed in backend computer systems or databases that access and copy valuable data to other systems. Regardless of the source, the data is sold to interested parties and used illegally.

Recent statistics on data breaches are startling:

- In the first 9 months of 2014, 904 million records were compromised in 1,922 confirmed incidents. Many of the incidents reported in 2014 involved record-setting amounts of data, including 20 incidents that compromised more than 1 million records each. [2]
- The number of U.S. data breaches tracked in 2014 hit a record high of 783 in 2014, according to a recent report by the Identity Theft Resource Center (ITRC) and sponsored by IDT911™. This represents a substantial hike of 27.5 percent over the number of breaches reported in 2013 and a significant increase of 18.3 percent over the previous high of 662 breaches tracked in 2010. The number of U.S. data breach incidents tracked since 2005 also hit a milestone of 5,029 reported data breach incidents, involving more than 675 million estimated records. This equated to 15 breaches each week in 2014. This press release even foretold 2015 with the statement, "Without a doubt, 2015 will see more massive takedowns, hacks and exposure of sensitive personal

Table 1: Costs Applicable to Data Breaches

Audits	Insurance fees
Brand	Issuer fees
Call center	IT costs
Card reissuance	Law enforcement
Chargebacks	Legal fees
Communications	Liability for cost of fraudulent transactions
Criminal pursuit and prosecution	Loss of spend
Credibility	Loss of "top of wallet" status
Credit monitoring	Lost revenue
Credit rating	Market valuation
Customer pain	Merchant staff time
Customer service	New staff
Declined transactions	Opportunity cost
Educational outreach	Penalties
Equipment and system updates	Penetration test
Executive time	PR and marketing efforts
Expedited shipping	Recurring payment changes
Fees/fines	Relationships with regulators and business partners
Forensic audit	Scrubbing customer files
Fraud analysis	Settlement fees
Fraud response planning	System outages
Fraud scoring	Training
Card reissuance file generation	Security upgrades
Goodwill	Vulnerability assessment
Human resources	

information like we have witnessed in years past." [3]

- 2015 data through May 6, 2015 indicate 282 breaches and over 101 million records compromised. [4]

Costs Associated with Data Breaches

The costs of data breaches have also increased. The 2014 Ponemon Study cited that "the average cost for each lost or stolen record containing sensitive and confidential information increased from $188 to $201. The total average cost to involved organizations increased from $5.4 million to $5.9 million." [5] Their study, in its eleventh year, shows data from breaches occurring mostly in 2013. Cost per compromised record related to data breaches put financial services data breaches in the top five; health care, with a cost per compromised card of $316, is number one.

Rising costs, coupled with steadily increasing incident reports, make awareness of the types of attacks and tools used to defend against such attacks imperative. Various statistics have been published on the cost of breaches.

- One statistic indicates that in Ohio, credit unions spent over $1.3 million in the wake of the Home Depot data breach. The costs were mostly related to reissuance of cards and responding to fraudulent charges. [6] The same study reported that Alabama credit unions also posted over $1 million in costs because of the Home Depot breach.
- The per-card-issued cost was $8.02, which includes the costs of new cards, fraud, additional staffing, member notification, account monitoring, and more. [7]
- All told, the Home Depot and Target data breaches combined have cost credit unions and members nearly $100 million dollars in the last year. [8]

The cost to merchants is also high. According to *USA Today*, "The company [Target] is still recovering financially. The breach has cost the company $148 million, minus a $38 million insurance payment. Profits for the first six months of their fiscal year were down 41% from the same period a year ago."[9]

The variance in the above examples illustrates the need for a standardized approach to calculating the true cost of data breaches.

This topic – exactly what costs should a company consider when calculating the total cost of a breach – is what brought this white paper to light. Costs will apply to some stakeholders and not to others. Also, some costs may be extremely difficult to quantify, like the cost of brand damage. Some of the costs associated with data breaches are well defined; others are somewhat challenging to capture fully.

Examples of costs that will be difficult to fully capture include:

- Recoupment of disputed transactions
- Intangible cost associated with card replacement
- Loss of existing customers or a decline in new customer acquisitions
- Increased labor due to customer inquiries
- Legal fees
- Credit counseling for affected customers
- Promotional campaigns aimed at recovering customers and rebuilding trust/loyalty
- Contractual obligations to customers, partners, and others that include performance penalties that also result in audits

Costs can be increased if the breach involves any of the following:

- Engaging consultants to support the incident response team
- Replacing lost or stolen physical assets (devices)
- Notifying customers
- Handling third-party errors

Certain factors can decrease the costs associated with a data breach:

- A strong security posture (i.e., a proactive approach to preventing breaches)
- An in-place, reviewed incident response plan
- Chief information security officer (CISO) leadership

Table 1 lists the potential costs that may be incurred by payments industry stakeholders as a result of a data breach.

Summary

It is important to establish a clear definition of what constitutes a data breach and to identify the cost categories that are impacted when a breach occurs. Issuers, acquirers, merchants, cardholders and payment brands have all been impacted to a degree by breaches. The impact and costs associated with each breach are unique.

Through an analysis of potential costs, payments industry stakeholders can understand the true impact a data breach might have on their organization. In addition, this can help organizations create the business case for developing a proactive data breach prevention strategy and for creating breach reaction tools.

References and Notes

[1] *2014 Data Breach Investigations Report*, Verizon
[2] "Nearly a billion records were compromised in 2014," *Network World*, Nov. 17, 2014
[3] "Identity Theft Resource Center Breach Report Hits Record High in 2014," Identity Theft Resource Center, January 12, 2015
[4] "2015 Data Breach Category Summary," Identity Theft Resource Center, May 6, 2015
[5] *2014 Cost of Data Breach Study: United States*, Ponemon Institute LLC, May 2014
[6] "Ohio credit unions spend $1.3 million on Home Depot data breach," *The Columbus Dispatch*, Nov. 3, 2014
[7] "What did Home Depot data breach cost Alabama credit unions? Nearly $1M, survey says," *AL.com*, Nov. 3, 2014
[8] "Home Depot breach costs double the Target costs," LCSU (League of Southeastern Credit Unions) & Affiliates, Oct. 30, 2014
[9] "Target leaves breach behind this holiday season," *USA Today*, Oct. 21, 2014

About this Article

This article is an extract from the white paper, "The True Cost of Data Breaches in the Payments Industry," published by the Smart Card Alliance Payments Council in March 2015. The white paper provides an educational resource on the potential costs that could be incurred during a data breach. The white paper consolidates industry information on and provides definitions for categories of costs as a reference document and identifies stakeholders impacted by each cost.

Members involved in the development of this white paper included: ABnote, American Express, Capgemini, CH2M, CPI Card Group, First Data, Fiserv, Giesecke & Devrient, Heartland Payment Systems, Infineon Technologies, Ingenico, INSIDE Secure, Intelcav, NXP Semiconductors, OATH, Oberthur Technologies, OTI America, Tyfone, Verifone, Visa Inc.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council published the "Guide Specification for Architects & Engineers for Smart Card-Based PACS Cards and Readers for Non-Government PACS." The white paper provides a tool for architects, engineers, consultants, integrators, manufacturers and end users to incorporate smart card-based PACS cards and readers into the A&E specification. Steve Rogers, IQ Devices, led this project. Members contributing to the development of the guidance document included: Advanced Card Systems, Ltd.; Allegion; AMAG Technology, Inc.; Booz Allen Hamilton; CH2M HILL; HID Global; HP Enterprise Services; Identification Technology Partners, Inc.; Identiv; IDmachines; IQ Devices; NXP Semiconductors N.V.; Oberthur Technologies; Quantum Secure (part of HID Global); Roehr Consulting; Secure Mission Solutions; Stanley Security Solutions; Tyco Software House; U.S. Department of State; XTec, Inc.
- The Council hosted a full-day preconference workshop, "Enterprise Physical Access Control Systems (EPACS) Using Smart Card Technology for Government and Commercial Organization," at ISC West on April 14. Members presenting in the workshop included: Peter Cattaneo, Identiv; Sal D'Agostino, IDmachines; Tony Damalas, Stanley Security Solutions; Frazier Evans, Booz Allen Hamilton; Dave Helbock, XTec, Inc.; Stafford Mahfouz, Tyco Software House; Roger Roehr, Roehr Consulting; Steve Rogers, IQ Devices; Adam Shane, AMAG Technology; Mark Steffler, Quantum Secure; Lars Suneborn, Smart Card Alliance. Chi Hickey and Vince Eckert from GSA also presented.
- The Council will be hosting a full-day preconference workshop, "Best Practices and Technology Trends for Strong Multifactor Authentication and Managing Identities of People and Internet Devices," at the Government Conference on June 8.
- The Council will be holding an in-person meeting at the Government Conference on June 10.

Health and Human Services Council

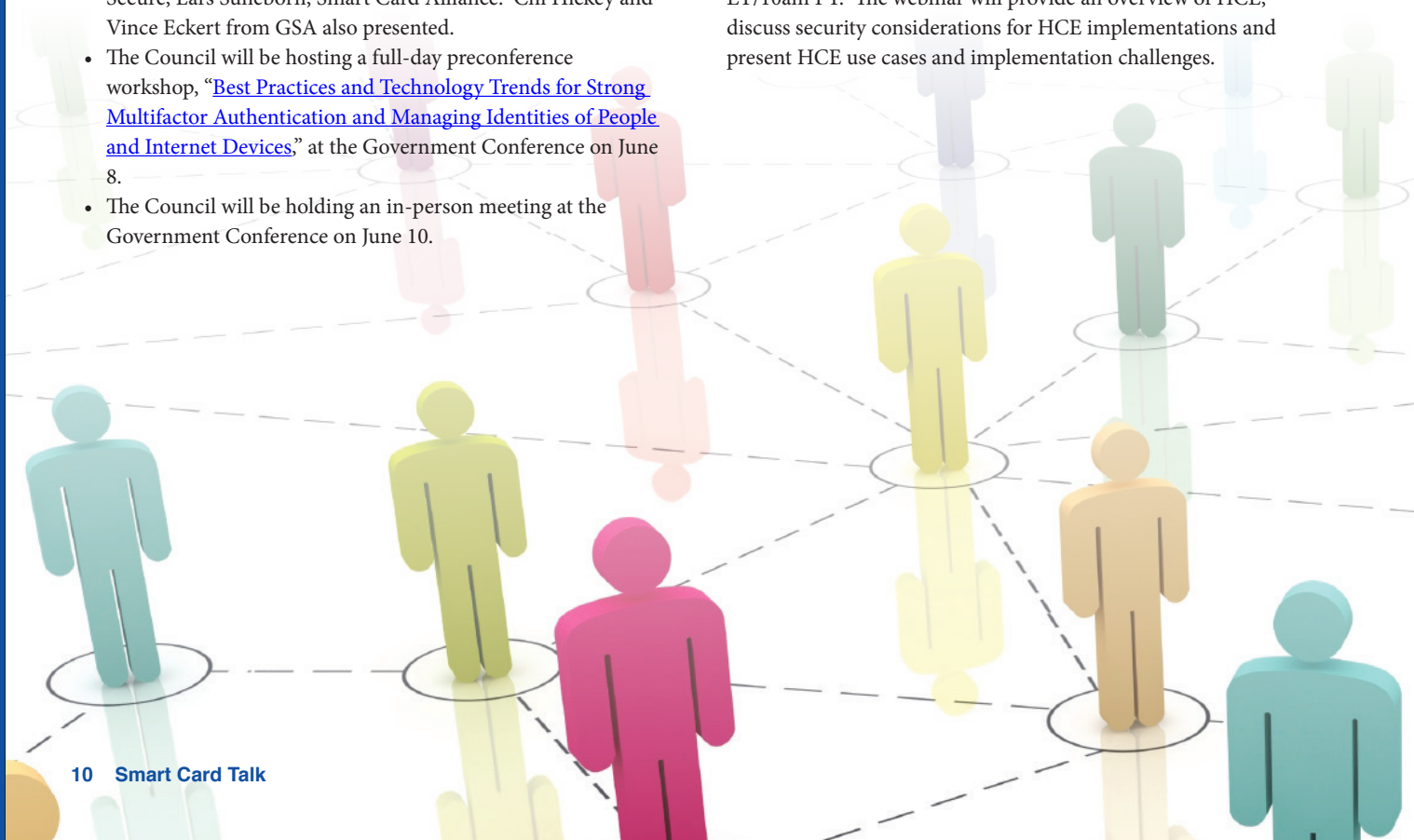
- The Health and Human Services Council was represented at the NAHAM conference by David Batchelor, LifeMed ID.
- The Council is working on additional speaking proposals for industry events and on statements of work for two white papers – one on patient identity and one on EMV and healthcare.
- The Council will be holding an in-person meeting, in collaboration with the Identity Council, at the Government Conference on June 9.

Identity Council

- The Identity Council is working on a new white paper on the FIDO protocol and smart card technology. The white paper will describe the role that smart card technology plays in FIDO implementations. Peter Cattaneo, Identiv, is leading this project.
- The Council will be holding an in-person meeting, in collaboration with the Health and Human Services Council, at the Government Conference on June 9.

Mobile and NFC Council

- The Mobile and NFC Council has completed its 2015 project planning and has launched three projects: a Host Card Emulation (HCE) webinar; a white paper on EMV and NFC (in collaboration with the Payments Council); and a white paper on NFC uses cases for non-payments user credentials.
- The Council is hosting an HCE webinar on June 18, at 1pm ET/10am PT. The webinar will provide an overview of HCE, discuss security considerations for HCE implementations and present HCE use cases and implementation challenges.



Payments Council

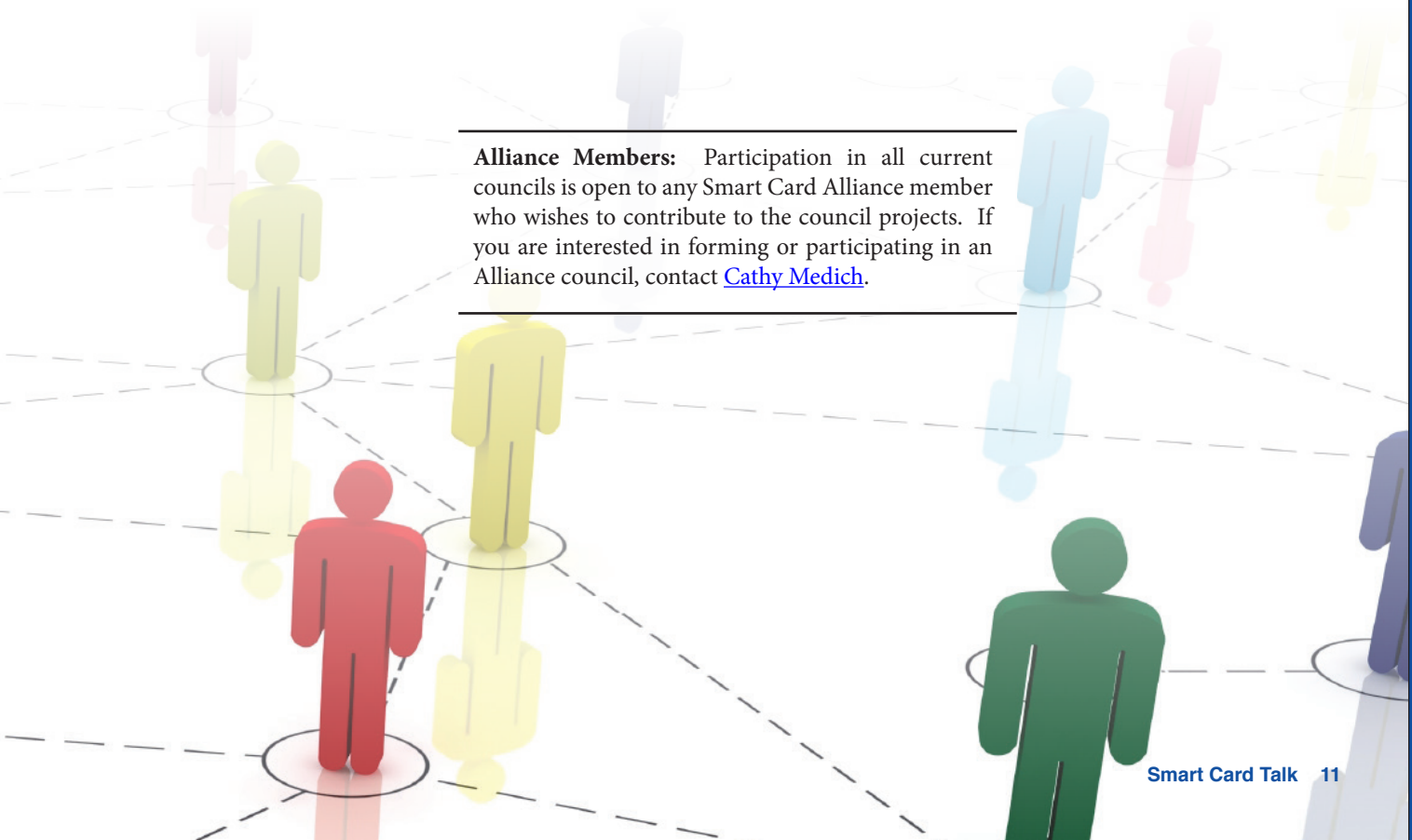
- The Payments Council published the new white paper, "The True Cost of Data Breaches in the Payments Industry." The white paper provides a resource for organizations to better understand the substantial tangible and intangible costs associated with data breaches, and discusses why investing in strong preventive technologies is important. Docia Myer, CPI Card Group, led the project. Members contributing to the development of the guidance document included: ABnote, American Express, Capgemini, CH2M HILL, CPI Card Group, First Data, Fiserv, Giesecke & Devrient, Heartland Payment Systems, Infineon Technologies, Ingenico, INSIDE Secure, Intelcav, NXP Semiconductors, OATH, Oberthur Technologies, OTI America, Tyfone, Verifone, Visa Inc.
- The Council has completed its 2015 project planning and has launched two projects: a white paper on EMV and NFC (in collaboration with the Mobile and NFC Council); a white paper on tokenization.

Transportation Council

- The Transportation Council was represented at the APTA 2015 Revenue Management and Fare Collection Summit, with a panel moderated by David Leininger, DART.
- The Council is holding a two-day, in-person member meeting on June 9-10, 2015, concurrent with the Smart Card Alliance Government Conference. The program committee has planned content-rich sessions on: multi-modal payments convergence, open bank card payments for public transportation, validator interoperability, use of PIV in account-based systems, and mobile payments. Also included will be updates from a variety of transit agencies on the status of their initiatives. The meeting will be highlighted by a WMATA presentation on their new fare collection system project and a tour featuring the WMATA pilot.
- The Council has several active projects: EMV impact on parking white paper; EMV and transit white paper; reference enterprise architecture on transit open payment system.

Other Council Information

- Members-only council web pages are available at http://www.smartcardalliance.org/councils. These are password-protected pages that contain council working and background documents and contact lists. Each Council area has a separate password since Councils may have different membership policies. If you are a Smart Card Alliance member and would like access to a council site, please contact Cathy Medich.



Alliance Members: Participation in all current councils is open to any Smart Card Alliance member who wishes to contribute to the council projects. If you are interested in forming or participating in an Alliance council, contact Cathy Medich.

Welcome New Members

- Creative Information Technology, Inc., General
- Dell Inc., General
- Octopus Cards Ltd, General
- Systems Engineering, Inc., General
- Banco Central de Costa Rica, Latin America

New Certification Recipients

CSCIP/Payments

- Sanjay Varghese, Capgemini Financial Services
- Tia Waters, Gilbarco Veeder-Root

CSEIP Recipients

- Douglas Kim, Business Integra*
- Matthew Martino, Business Integra*
- David Miller, Business Integra*
- Anthony Shields, Business Integra*
- Carlos Gaskin, Chenega*
- Jesse Tatum, Chenega*
- Jeff Deweese, Tyco Integrated Security*
- Clyde Fox, Tyco Integrated Security*
- Martin Hoffman, Tyco Integrated Security*
- Joe Mikula, Tyco Integrated Security*
- Mike Plaugher, Tyco Integrated Security*
- Jeff Ryder, Tyco Integrated Security*
- Jason Wills, Tyco Integrated Security*
- JC Viricochea, Tyco Integrated Security*
- Shawn Hood, Xator Corp*

- Charles Campbell, Security & Energy Technology Corporation
- Ray Dickler, eMentum
- Mark Entrikin, SCI Inc.
- Mike Ford, Apex Integrated Security Solutions, Inc.
- Derek Greenland, AMAG Technology, Inc.
- Eric Grist, S2 Security
- Mala Grover, Digitronics, Inc.
- Kayee Hanaoka, NIST
- James Hansen, Chenega Corporation
- Nathan Hott, Genesis Security Systems, LLC
- Quinn Knight, DHS – U.S. Customs and Border Protection
- Karen Marshall, NIST
- Brian Mooney, Genesis Security Systems, LLC
- Cheston Obert, DHS – U.S. Customs and Border Protection
- Brian Thompson, Global Networks, Inc.
- Joseph Verdi, Security & Energy Technology Corporation
- Joshua Wernick, Kratos Public Safety and Security
- William Windsor, Department of the Treasury

**Denotes corporate training class recipients*

For more information, visit our website at www.smartcardalliance.org. Members can also access white papers, educational resources and other content.

Smart Card Alliance

191 Clarksville Road
Princeton Junction, New Jersey 08550
1.800.556.6828
Fax: 1.609.799.7032
info@smartcardalliance.org
www.smartcardalliance.org

About Smart Card Talk

Smart Card Talk is the monthly e-newsletter published by the Smart Card Alliance to report on industry news, information and events and to provide highlights of Alliance activities and membership.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.