PCI Security Standards Council

PCI Perspectives

JULY 2013

IN THIS ISSUE

UPCOMING EVENTS

MasterCard Global Risk Management Conference – Asia Pacific
20–23 August 2013
Phuket, Thailand

International Association of Financial Crimes Investigators – 2013 Training Conference and Exhibitor Show
26–30 August 2013
Denver, Colorado

PCI SSC North American Community Meeting
24–26 September 2013
Las Vegas, Nevada

Visa Global Security Summit
1–2 October 2013
Washington, DC

MasterCard Global Risk Management Conference – Europe
14–17 October 2013
St. Julians, Malta

PCI SSC European Community Meeting
29–31 October 2013
Nice, France

PCI SSC Asia-Pacific Community Meeting
20 November 2013
Kuala Lumpur, Malaysia

Welcome!

I'm pleased to introduce the first issue of your PCI community newsletter – written by you and for you.

One of the biggest values of being part of a community like this one is the opportunity to learn from each other, to share your expertise and make connections. And that's what this newsletter is all about.

Thank you for contributing your stories, insights and recommendations.

In the next few pages, you'll get a window into the types of businesses and industries that make up this group, with spotlights on our newest Participating Organizations as well as insights from some of the folks who have been with us from the very start. You'll hear from some of our newly elected Board of Advisors, PCI Special Interest Group participants, and how your colleagues are managing their payment security challenges through practical case study applications. Also, there are tips on recommended events and books to check out, as well as regional perspectives on payment card security developments.

Our community offers a wealth of experience and opportunities for you and your business – we hope this new forum will help you take advantage of it. If you have any ideas or feedback on what else you'd like to see in this newsletter or how we can make it better, please email us at: pcinewsletter@pcisecuritystandards.org.

Enjoy!

Regards,
BOB RUSSO
General Manager, PCI SSC

$1.4 million over 10 years!

Read more about Team Russo's fundraising efforts on page 10

PCI Reflections – Five Years Later

Today the Council has nearly 700 Participating Organizations. Many of these companies have been involved since the early stages of PCI SSC, more than seven years ago. In this section, your colleagues reflect on their involvement in PCI and the growth in payment card security.

Bluefin Payment Systems (Participating Organization since 2007)

Ruston Miles, Senior Vice President & Chief of Product Innovation E-Commerce Division

Bluefin Payment Systems immediately recognized the value of not only keeping up with the PCI Security Standards as they evolve with and adapt to the payment industry, but also having a voice in the creation and grooming of the standards. As an active and long-standing Participating Organization, Bluefin can ensure that our unique perspective and position in the market is represented and taken into account in the drafting of the security standards. The Community Meetings are particularly valuable to our organization. These meetings include all of the key players in the PCI SSC, including PCI SSC employees, QSAs, ASVs, POs, PCIPs, as well as related vendors. In my opinion, these Community Meetings are the meat of our membership and are NOT to be missed. Only so much can be done over the phone and through email. Meeting together with PCI SSC stakeholders from around the world and deep-diving into the standards and programs has given our organization a living understanding of the standards, which helps us craft new payments initiatives in line with the intent of the standards. This helps Bluefin better plan for security, better communicate with our assessors, and improves the overall culture of security within our organization.

DST Output (Participating Organization since 2007)

Christy Schauffel, Enterprise Security Manager, Privacy, Security & Continuity

DST Output became involved in PCI SSC in 2006 with the company receiving a Report of Compliance in 2008 for our electronic payment processing. At the time DST Output's participation was unique in that few companies from the transaction printing industry were participating members. The company believed that focusing solely on electronic payment processing did not make sense since the standards had relevance in other aspects of our business. In April 2010, DST Output developed a PCI print environment that includes PCI for our offerings in CSR Web Presentment, Quality Validation and CD/DVD. Most recently in the summer of 2011, the company achieved compliance for credit card security in both our payment and print PCI (Payment Card Industry) environments in our El Dorado Hills, Kansas City and Hartford locations. We have maintained this compliance with the most recent recertification occurring in April.

THANKS FOR YOUR SUPPORT!

The following companies have been involved in the PCI Council as Participating Organizations for five years or more.

- Airlines Reporting Corporation
- AirTight Networks
- AJB Software Design
- Akamai Technologies
- AlgoSec
- Alliance Data
- Allstate Insurance
- American Family Insurance
- AT&T Management Services LP
- Atos Worldline
- Australian Payments Clearing Association (APCA)
- Bank of America Merchant Services
- Bank of Montreal Financial Group
- Barclaycard
- Barnes and Noble College Booksellers Inc
- Big Lots Stores Inc
- Blackboard Inc
- Blue Pay Processing LLC
- Bluefin Payment Systems
- BP Products North America
- British Airways PLC
- Canadian Tire Financial Services
- Capita PLC
- Card Complete Service Bank AG
- Carlson Companies Inc
- Cartes Bancaires
- Chase Paymentech Solutions
- Chevron Products Co
- Choice Hotels International
- Cielo SA
- Cirque Corporation
- Citgo Petroleum Corporation
- Citrix Systems Inc
- CKE Restaurants Inc
- Comcast Cable Communications
- Commerce Bank
- Compass Group USA
- Co-op Financial Services
- Cost Plus World Market
- Cryptera
- CSC Computer Sciences Corporation
- CSR
- DataPipe Inc
- Dell Inc
- Demoulas SuperMarkets Inc
- Domino's Pizza Inc
- DST Output
- EchoSat Communications Group Inc
- Elavon Merchant Services
- Element Payment Services
- Epicor Software Corporation
- Equens SE
- Equinox Payments
- European Payment Council AISBL
- Exxon Mobil Corporation
- First Data Merchant Services
- Fiserv Solutions Inc
- GE Money
- Givex Corporation
- Global Payments Direct Inc
- Hamilton Manufacturing Corporation
- HCA Healthcare
- Heartland Payment Systems
- Higher One
- HSBC
- Hudson Group
- Hughes Network Systems Inc
- Imperva Inc
- Independent Community Bankers of America (ICBA)
- Ingenico
- Intel Corporation
- Interac Association
- InterCard AG
- InterContinental Hotels Group
- Intermountain Healthcare Inc

European Payments Council AISBL (EPC) (Participating Organization since 2008)
Ugo Bechis, Chair of the EPC Cards Working Group

The European Payments Council (EPC) represents the European banking community. EPC plays an important role in card related security standardization for Europe and therefore a good relationship with PCI SSC is essential. EPC has been a Board of Advisors member almost since the beginning, five years ago. We are very happy with the contribution of Jeremy King, the European Director of PCI SSC, in the several working groups and task forces active in this domain in Europe. Jeremy makes use of the knowledge of an excellent PCI SSC network. Due to this relationship we were also able to give more focus to the European needs related to the PCI SSC domain. We look forward to continuing the good work in the coming years.

Kilrush Consultancy Ltd. (Participating Organization since 2007)
Connie G. Penn, Managing Director

Having grappled with the challenges of addressing the individual card brands' security requirements in our clients' environments during 2005, Kilrush Consultancy were relieved with the launch of PCI DSS in 2006. As an active PO since 2007, we have encouraged many others to participate and also facilitated a valuable exchange of information to the benefit of both the Council and other POs. Although a very small card consultancy, the investment has been very worthwhile, helping grow our knowledge of the standard as it has evolved and matured and helping us develop strong rewarding relationships with individuals from the Council and card brands as well as with other POs. We believe being an active PO has been a key contributor to our success in helping our clients achieve compliance. As a PO we have attended every community meeting in both North America and Europe, witnessing the attendance grow from less than 400 in Toronto in 2007 to over 1,100 in Orlando last year, reinforcing how important protecting card data has become. Being given the opportunity to contribute to the Special Interest Groups (SIGs) has also been very worthwhile and believe the output from these SIGs will be valuable to all concerned with the security of card data.

SSH Corporation (Participating Organization since 2007)
Jonathan Lewis, Director of Product Marketing

All involved with the PCI Council learn that in the world of security standards the only constant is change. Not only are we striving to improve our existing guidelines to make them more effective and useable, we do so in an environment that is rapidly changing. PCI contributors bring diverse perspectives which enable us to evolve to meet these challenges – from the need to address new technologies such as virtualization, cloud and mobile, emergence of new threats, to the real world practicalities of implementing security standards. As technologists and security specialists, SSH Communications Security is proud to have brought some new perspectives that we think have made a significant contribution in expanding the definition of "identity" in the PCI world. This is helping Participating Organizations make real improvements in protecting critical payment information – to the benefit of our industry and consumers alike. At the same time we have learned a great amount from our colleagues at PCI SSC who do a wonderful job of bringing diverse perspectives together. It is a collaborative and rewarding effort and we feel privileged to be a part of it.

THANKS FOR YOUR SUPPORT!

- International Air Transport Association
- IP Commerce Inc
- Ipswitch
- ITS Inc
- JCPenney Company Inc
- John Lewis PLC
- Kilrush Consultancy Ltd
- Kingfisher IT Services
- L.L. Bean Inc
- Layered Tech Inc
- Linoma Software Inc
- Lloyds TSB Cardnet
- Marathon Petroleum Co
- McDonalds Corporation
- Merchant Link LLC
- Merchant Warehouse LLC
- Mercury Payment Systems
- Micros
- Microsoft
- Minacs Worldwide Inc
- Moneris Solutions Corp
- MoneyGram International
- Motorola
- National Association for Information Destruction
- National Association Of College and University Business Officers (NACUBO)
- Nelnet Business Solutions
- Net One Systems Co Ltd
- Nets Oy
- NetSpend Corporation
- Network Frontiers LLC
- NIC Inc
- Nordea Bank AB (PUBL)
- North Carolina Office of the State Controller
- Ogone
- Optimal Payments
- PAN-Nordic Card Association
- Parkway Corporation
- Paymetric Inc
- PayPal Inc
- PetSmart Inc
- Phoenix Payment Systems Inc dba Electronic Payment Exchange (EPX)
- Point International
- Posera
- Premier Bankcard LLC
- ProPay Inc
- QuikTrip Corporation
- Radiant Systems
- RBS
- Reitmans (Canada) Limited
- Reliant Info Security Inc
- Rewards Network
- Rite Aid Corporation
- Royal Dutch Shell Ltd
- RSA
- Safeway Inc
- Sage Pay Europe Limited
- Saks Fifth Avenue
- SBI VeriTrans Co Ltd
- SEB AB
- Secure Technology Integration Group Ltd
- See's Candies Inc
- SERVIRED
- Shift4®
- SIX Payment Services Ltd
- South African Retailers and Payment Issues Forum (SARPIF)
- Spacenet Inc
- SSH Corporation
- Staples Inc
- Star Networks Inc
- State Farm Mutual Automobile Insurance Company
- Storm Interface
- Suncor Energy Inc
- Sunoco Inc (R and M)
- TD Bank NA
- Tesco Stores Ltd
- The Hertz Corporation
- The Powertech Group Inc
- The Walt Disney Company
- Tokheim
- TouchNet Information Systems Inc
- Townsend Security Inc
- Transaction Network Services
- TSYS
- US Bancorp
- UK Payments Administration
- University of Notre Dame
- Venda Ltd
- Vendorcom
- VeriFone Inc
- Vonage Holdings Corp
- Wal-Mart Stores Inc
- Wawa Inc
- Wayne, a GE Energy Business
- Wells Fargo
- Wyndham Worldwide
- Yum! Brands Inc

Interested in submitting for the January 2014 newsletter?
Email us at pcinewsletter@pcisecuritystandards.org to learn more!

PCI Training – In Your Own Words

Meet Randy Braatz, PCIP

The PCI SSC sat down with Excentus Corporation's Randy Braatz to learn a little more about why he became a PCI Professional and how it's helping him and his company in their payment security efforts.

PCI SSC: What do you do for your company?

Randy: I've been with the company for 12 years and have held a variety of roles over the years. This year, I am developing our Information Security Office. I report directly to the SVP of Tech Operations.

PCI SSC: What is your professional experience?

Randy: I have worked on software development for the petroleum industry for 25 years. Starting off my career, I wrote accounting software for petroleum jobbers. Later I joined the Excentus team to develop POS fuel systems for both commercial and high-volume grocery retailers. The POS system had to adhere to PA-DSS standards.

PCI SSC: Was there a personal/corporate issue that prompted you to seek PCI training?

Randy: As part of Excentus' continued commitment to security and privacy of our member data, I was given the opportunity to develop our Information Security Office and formalize our security policies, procedures, and processes while guiding us through the requirements for PCI DSS compliance.

PCI SSC: Why did you choose to get training through the Council?

Randy: I was already familiar with the PA-DSS requirements and I felt the PCIP certification offered by the council would provide evidence of my knowledge and help add credibility to my recommendations both internally and externally. The online class helped to reassure me of my PA-DSS knowledge and bridge the gap to PCI DSS knowledge.

PCI SSC: How do you plan to use the knowledge gained from this training?

Randy: The knowledge gained was immediately useful in helping to provide guidance regarding new policies, procedures, and even systems we were in the process of implementing.

PCI SSC: What two pieces of knowledge are you most likely to use in your job?

Randy: Promoting the idea of not storing card data to minimize scope and costs; and proper network segmentation. Specifically, the training around network configuration and monitoring requirements provided an immediate benefit in helping us to implement new systems appropriately.

PCI SSC: If you had to pick one best thing about your training what would it be?

Randy: The Crazy Chicken Case Study was great! It really helped me to transition my thinking from POS perspective to an enterprise perspective.

PCI SSC: How long would you estimate before the average employee is faced with a situation on the job where this training applies?

Randy: This type of training would be an eye opener and provide an immediate benefit to any employee who has some responsibility for Payment Card Data or related compliance requirements. I think this training provides the most benefit to employees who are directly involved in compliance requirements or have a responsibility for leading the organization through compliance.

Name: Randy Braatz

Title: Information Security Manager

Company: Excentus Corporation

Training takeaway: The training around network configuration and monitoring requirements provided an immediate benefit in helping us to implement new systems appropriately.

Company background:
Excentus Corporation is the leading provider of loyalty marketing programs and services that utilize cents per gallon fuel savings as the ultimate consumer reward - and holds nine patents on the associated technology for the Fuel Rewards Network. Excentus has spent more than 15 years developing and perfecting the Fuel Rewards Network's™ technology and program features to make it easy for businesses to build loyalty and create value for their customers. The growing Fuel Rewards Network™ program provides Members with the opportunity to earn free fuel simply by purchasing the things they normally would from more than 1,000 retail locations, nearly 700 online merchants, and 10,000+ restaurants, and redeeming their rewards at participating fuel stations across the country.

Global Security Insights

Payment Security in Europe – an update on the regulatory landscape

Jeremy King
European Director,
PCI SSC

The Single European Payments Area, (SEPA) covers most of Europe, including countries that have not migrated to the Euro, such as the UK, Denmark and Sweden. Within the SEPA region there are three key European bodies developing standards that will impact all card schemes, banks, merchants, service providers, and everyone involved in the transaction process.

Currently there are three standards at various levels of development:

- European Data Protection Directive – developed by the European Commission
- Recommendations for Securing Internet Payments – developed by the European Central Bank
- The SEPA Cards Standardisation Volume – developed by the European Payments Council

Of these three, only the ECB's Recommendations for Securing Internet Payments has been released. The organisational structure of the ECB is such that it can only produce recommendations, but these recommendations are turned into law by the regulatory authorities of each individual member state. The Bank of France and the Central Bank of Germany are likely to implement the recommendations in full by the agreed date of February 2015. In the UK, the Financial Services Authority (FSA) is forming a new organisation responsible for this implementation, the Financial Conduct Authority (FCA), and will likely wait for this process to be complete before moving forward. To plan for the implementation and the impact for their organisation, businesses in the region should become familiar with these recommendations now.

The European Data Protection Directive is another standard that as it evolves is one to keep an eye on. The first draft of the document highlighted large penalties to organisations who suffer a breach, formal requirements for breach notification and requirements about having nominated data security officers (more likely a CISO). One of the current issues for debate involves the "Right to be forgotten" (Article 17 – gives consumer power to essentially erase their digital data history) which in a digital world is no mean feat, and this amongst others has resulted in a vast amount of suggested changes to the document. Working through the sheer number of proposed updates is going to take time, so although the target date for release was the end of 2013 with an implementation date of 2015, it is unlikely to be achieved.

Finally, the Card Standardisation Volume is being prepared for its latest draft release, with the aim to provide a single European Approval process for cards and terminals. It includes both security and functional requirements. The document has been in development for a number of years – this draft will be version 7.0, and still it is only a draft document. Throughout the course of this development, there has been a significant shift toward the inclusion of PCI Standards, as our standards have grown in maturity and acceptance. As such, the latest draft includes PCI PTS 4.0, PCI DSS, PCI HSM, and PCI PIN Security Requirements. As we roll out standards for P2PE, card production and tokenization, these may also be incorporated into future editions. What remains unclear about the Card Standardisation Volume is exactly who will use it and when.

Aside from these specific regulatory developments, as in the USA the UK Government has also recently reached out to request information about available standards for Data Security that could be used throughout the UK. We're pleased with this development and have provided the PCI DSS standard to the UK Government for consideration. We will be meeting with them regularly on this front moving forward.

Overall, we are encouraged by the continued awareness of the PCI Standards across the European region and the increased involvement from stakeholders. Looking ahead, we will continue to monitor developments from all European and national governments that will impact PCI to ensure our involvement in issues and discussions directly impacting cardholder data security.

Regional Perspectives – PCI SSC in Singapore

Jeremy King, European Director, PCI SSC

I had the opportunity to visit Singapore in March of this year to raise awareness of PCI Standards in the Asia-Pacific region, and to generate interest for organizations to join the PCI community and attend our first ever Asia-Pacific Community Meeting in Kuala Lumpur.

It was a busy week that included speaking engagements at both the 6th Asia Mobile Commerce Summit and the CARDS Security Working Group hosted by MasterCard, as well as the opportunity to meet with the Monetary Advisory of Singapore (MAS) and the Cloud Security Alliance's Asia-Pacific head, and a number of interviews with local IT, security and financial trade media.

The 6th Asia Mobile Commerce Summit was attended by more than a dozen different countries in the APAC region, from Sri Lanka to Vanuatu to the Philippines. As the 6th such meeting, it is clear that in Asia as in the rest of the world, everyone is still trying to figure out how to do mobile commerce. This was reflected in the fact that every speaker had a different idea of how their product would be the one to make it.

MasterCard's Philip Yen, head of Emerging Payments for APAC and EMEA, talked about the ability to use your NFC phone to pay for taxis in Singapore. All taxis in Singapore accept cards, and most accept NFC, which is an interesting move forward. Christean Cadeo, head of mobile for Google, talked about the new 4G and indicated that this would bring a return to the use of the web browser on the phone rather than relying on apps, as the browser speed would be fast enough to provide the quality of service required. This could as a by-product improve security. He also stated that globally 1.2 M Android phones and 0.8M iPhones are being activated each and every day, underscoring the reality that smartphones and m-commerce won't be going away anytime soon.

continued on page 7

PCI PEOPLE ON THE MOVE

Nichol Stark has joined Woolworths as our IT Compliance and Assurance Manager. Prior to that she had an 18 year career at Suncorp, most recently as the PCI Program Manager.

Neira Jones, former Director of Payment Security and Fraud at Barclaycard and former member of the PCI SSC BoA, has become a partner at the payments consultancy Accourt where she manages the Risk & Digital practice. Accourt offers specialist advice on areas such as payments, strategic advice, mobile and digital strategies, payments regulation and compliance, risk management, fraud, product development and implementation. She is also chairman of the Cybercrime Advisory Board for the Centre for Strategic Cyberspace and Security Science, and can be contacted via Twitter @neirajones or on LinkedIn.

Parminder Lall has moved on from his post as PCI Programme Manager at Everything Everywhere (EE) to join Sysnet Global Solutions as Lead Principal Consultant in their London office.

2013 COMMUNITY MEETINGS

Asia-Pacific Community Meeting

20 NOVEMBER 2013
SHANGRI-LA HOTEL • KUALA LUMPUR, MALAYSIA

FEATURED SPEAKER

PATRICK LUM
Senior Consultant
Verizon RISK Team

Patrick Lum is currently the senior consultant within the Verizon RISK Team. He has assisted numerous clients in investigating data breaches within the Asia Pacific region. His investigations include the identification of documents lost, allegations of fraud and misappropriation of assets, collation of evidence, computer forensic investigation, leakage of confidential information, leakage of credit card data.

With more than six years of experience in digital investigation, Patrick has developed a high level of competency with various tools and methodologies and holds various internationally recognized certifications in technology forensics.

Topic: **Forensics Overview**

In this session, Patrick Lum, lead consultant for Verizon Singapore, will outline the different situations that may require a PCI Forensic Investigation (PFI) and what to expect during a PFI investigation. He will also be sharing case studies from actual investigations, emphasizing where organizations have failed, and giving advice on how not to become the next victim.

continued from page 6

Other speakers focused on mobile commerce and the opportunity to provide banking services to the unbanked, especially in countries like Nepal, Sri Lanka and India amongst others. Overall, people understand the challenges, especially relating to malware, and are interested in developments from the Council and other sectors working on the problem.

I also met with the Monetary Authority of Singapore (MAS), the local bank regulator. The purpose of the meeting was to make introductions and to share information on PCI Standards. They are aware of the security challenges surrounding the use of mobile phones and are keen to keep abreast of all requirements including those from PCI SSC. Similar to how I have found regulators in Europe, they cannot be seen to be linked to one entity, but do recognize the importance of the PCI Council and support our aims and goals.

Another interesting point was that MAS does not have any specific ATM requirements or guidelines; however, they have deactivated magnetic stripes for transactions abroad, and these have to be turned on by request of the cardholder when they travel overseas. According to MAS, this helps prevent the cloning of cards in Singapore for use abroad. In terms of EMV, they are intending to migrate all ATMs to EMV with no magnetic stripe fall back by June 2013.

The Cloud Security Alliance has recently appointed an Asia-Pacific Director, Aloysius Cheang, based in Singapore. This was a great opportunity to discuss and raise awareness around the Cloud Special Interest Group's information supplement on PCI DSS and cloud computing. Cloud was a hot topic for the media there too, and I enjoyed exchanging information with a number of local reporters who were interested in payment security, particularly with the evolution of mobile payments.

In conclusion, my time in Singapore was a great opportunity to get on the ground and gain insights into payment security in the area as well as raise awareness of PCI. As you know, this is essential because PCI SSC works best as a community and having active participants from Asia will help ensure the standards reflect the needs of this region.

We look forward to meeting with everyone again at our Community Meeting in Kuala Lumpur at the end of November.

PAYMENT SECURITY BOOKSHELF

Phil Jones, Payment Security Strategy Manager, Barclaycard, recommends reading *Dark Market* by Misha Glenny for a great insight in to the minds of organised crime profiting from compromised card data and the law enforcement agencies countering these threats. Currently reading *McMafia* by the same author and am really looking forward to meeting Misha at the European PCI SSC Community Meeting in Nice.

Andrew Updegrove, Gesmer Updegrove LLP: When *The Alexandria Project, a Tale of Treachery and Technology* came out, the blurb stated, "The only thing that's fictional about it is that it hasn't happened yet." But then the events portrayed in this riveting cybersecurity thriller started occurring with unsettling frequency. In-Q-Tel CSIO Dan Geer calls it, "Fiction that cuts close to the Bone." Available at Amazon, Barnes & Noble, and all other popular Web stores.

Ralph Poore, PCI SSC Director, Emerging Standards, recommends the *Information Security Management Handbook*. CRC Press/ Taylor & Francis publish a new edition each year. It is a compendium of articles by subject matter experts. As an ongoing reference work, it deserves a place on every information security professional's bookshelf (or virtual bookshelf as electronic or CD-based versions are available).

As a career security practitioner, **Mark Mrotek**, PCI SSC Standards Manager, enjoys hacker-type books to better understand the enemy and know as much of what they know as possible. An oldie but goodie that he thinks should be on every IT security pro's shelf is *Secrets and Lies: Digital Security in a Networked World* by Bruce Schneier, a guidance book for achieving network security.

Interested in submitting for the January 2014 newsletter?
Email us at pcinewsletter@pcisecuritystandards.org to learn more!

PCI in Practice: A Small Business Case Study

Introduction

Working for a small business (StoreFinancial has approximately eighty employees), and as the sole individual responsible for maintaining PCI compliance, it did not take long for me to realize after I took the job that an army of internal compliance auditors, risk managers, and compliance staff was not going to walk through the door and help me. Unfortunately, resources for small businesses, especially those that have to complete a Report on Compliance (ROC), are few and far between.

Much of the Council's guidance documentation and the talks at the Community Meetings are geared towards companies with a large staff of people dedicated to ensuring PCI compliance for their respective organizations. While these can be helpful, there is a gap that needs to be filled for small businesses and companies with only a handful of people, or, in my case, one person, in charge of compliance efforts. I know that there are a lot of small businesses, both merchants and acquirers, who could benefit from some guidance as to how to make PCI work in a small environment, and I have spoken directly to people who have no idea where to start with the PCI DSS, and are looking for any help or guidance to get them started down the path to compliance.

Challenge

I was hired over two years ago into a situation where PCI compliance work was being performed on an ad-hoc basis by individuals in different departments, with little cohesion or organization. I had absolutely no guidance or understanding as to how to organize PCI compliance efforts in a small business.

The biggest challenge I faced when I started at StoreFinancial was getting my co-workers and my management to understand what the PCI Standards were and why they were important. It turns out that this is a fairly collective problem – security is everyone's responsibility, as we have been told again and again, but it generally comes in a close third behind making hardware, software and technology work, and keeping them working through change and catastrophe.

Another issue I had to deal with is that I had no idea where the company stood from a PCI compliance perspective. The company was obviously compliant in previous years, as evidenced by clean ROCs; however, I was unaware if anything had changed between then and now, and if the governance documentation was truly being followed in practice.

Approach

I first approached the PCI awareness problem by developing a communications strategy with my company's executive team. Your company's executives not only drive the business, which in turn drives your technology department, but they also control your budget and set the tone and culture for the company. Getting these individuals to not only understand why you are employed, but that security, and by proxy compliance, are important, is essential to the success of your information security efforts.

There are a myriad of ways to accomplish this, but one of the most effective is to create an executive information security summary report, and fill it with content pertinent to your security program. You can outline the status of your major projects; detail your achievements, individually, such as certifications, and collectively; discuss some basic metrics around alerts, events, and incidents; and write up a summary of security- and compliance-related events in the news, and how it applies to your company. Keep it fairly short and simple, and try not to get bogged down in technical details that they will ignore. Distribute it to all of your

continued on page 9

Name: Andrew Barrett

Title: Director of Information Security

Company: StoreFinancial

Email: abarrett@storefinancial.com

Twitter: @Br8den

Challenge: Organizing PCI compliance efforts in a small business

Background:
I am the Director of Information Security at StoreFinancial, which is a pre-paid and payment processing company based in Overland Park, Kansas. Prior to StoreFinancial, I worked in a variety of security roles with a national telecommunications company, spending time on both the Incident Response and Risk Management Teams, and as part of a contract with the United States Department of Agriculture.

I received a B.S. in Management Information Systems and an MBA from Park University. I also hold a variety of security-related certifications, including PCIP, and I am a PCI ISA. I am a founding member of SecKC, and I regularly speak on topics such as compliance and risk management at events around the Kansas City area.

continued from page 8

company's executives on a quarterly or semi-annual basis, and make sure to follow up with them in the hallway or break room to see if they have any questions.

Another way to communicate with your company's executives is to use risk assessments to your advantage. The PCI DSS requires that we create a risk assessment on an annual basis for our in-scope systems and applications. Your risk assessment should highlight the security-related gaps in your environment, and it should be distributed to your executive team along with a security plan detailing how you're going to resolve the issues. Use the data from the risk assessments to drive purchases and projects - "We have this problem. I can fix it if we purchase X, and write policies Y and Z."

In this same vein, your company's security awareness is equally important. While security awareness has gotten a bad rap recently for being a waste of time and money, I have found it to be an essential way that I can communicate with my co-workers, some of whom I do not interact with on a regular basis, and get them to take me and my position seriously.

Security awareness is much more than an annual lesson in "don't click on that link in the e-mail message." Use it as your platform to get simple messages across, using humor and real-world examples; weave in PCI ("Just because it's a screenshot of a card number doesn't mean you can e-mail it") and any other compliance requirements that your company may have to work through; and teach classes that cover things like password security, which is applicable to your co-workers professional and personal lives. In other words, get your name out there, and make sure that your company equates your word as the end-all, be-all for security and PCI compliance.

To solve the problem I had of not knowing where StoreFinancial stood from a current, PCI compliance perspective, I decided to use the PCI DSS as a benchmark to determine the on-going level of the company's compliance efforts, as well as an overall check of the company's security posture. While compliance does not necessarily equal security, this exercise gave me an understanding of immediate gaps that I would need to fill in preparation for the annual assessment.

I took this gap analysis, and after I completed my risk assessment, I used the results from both to determine my program's goals for the next year. Establishing a combination of security and compliance goals allows you to focus on your immediate needs, tie the tasks and projects required to complete these goals back to tangible gaps and weaknesses, and create an instant justification to your executives for budget, resources, and support.

Lessons Learned

During my time at StoreFinancial, I have learned a lot in regards to ensuring continued PCI compliance and making PCI work for me to further other compliance and security initiatives, all while employed at a small business where PCI compliance is not always at the forefront of everyone's mind.

While I presented some strategies which helped me get on my feet and integrate PCI compliance and security into my company's existing processes, there is no right or perfect way to get things done. Security is not a one-size-fits-all kind of business, so be bold and try different strategies to see what works. Do your best to integrate yourself with the business side of your organization, and then leverage those leaders as allies and use them to achieve your goals. Security leaders traditionally fail when they always say "no," so learn to be agile and creative ("it depends" is always a good first answer when presented with a non-PCI compliant idea) in working out solutions that everyone can be happy with, and you can defend in front of your assessor.

"While I presented some strategies which helped me get on my feet and integrate PCI compliance and security into my company's existing processes, there is no right or perfect way to get things done. Security is not a one-size-fits-all kind of business, so be bold and try different strategies to see what works."

PCI SSC – Did You Know?

It's not all standards, standards, standards at the Council.

When not collaborating with industry partners to develop security standards, here's a look into other areas of life the team is working to impact.

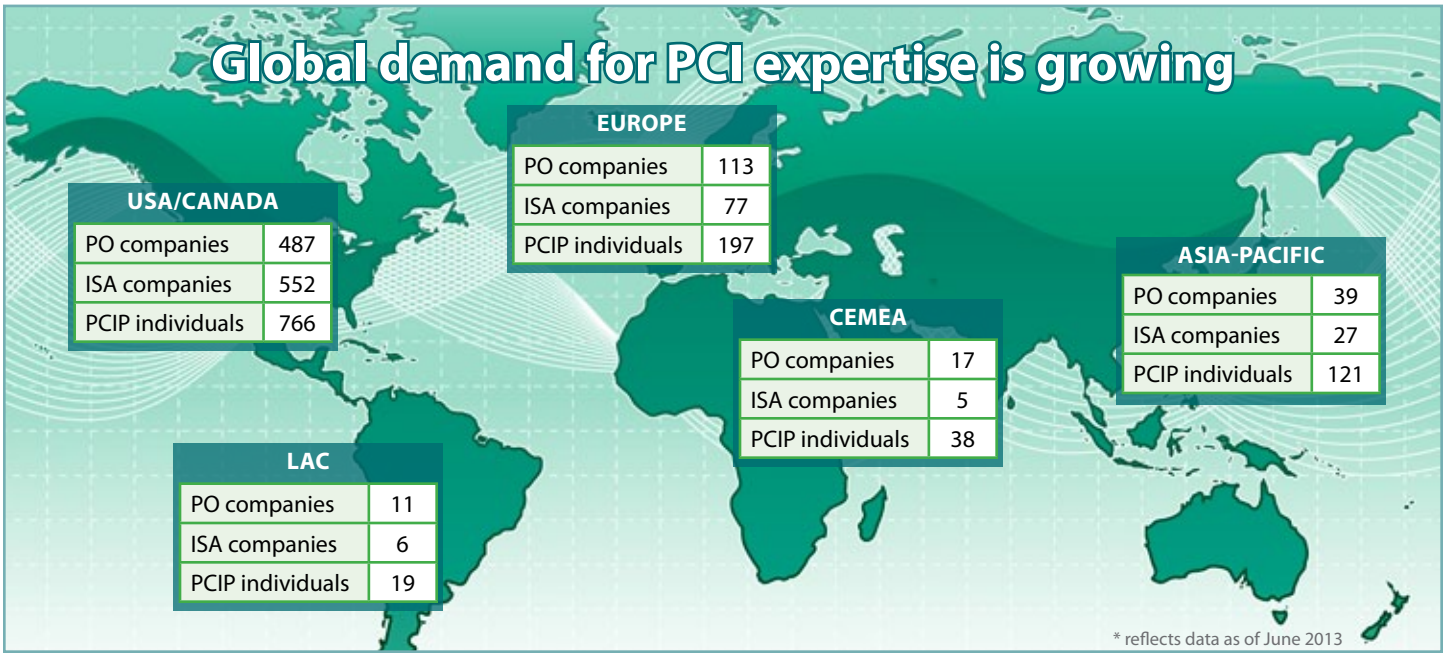
Some of you may not know but the Council's General Manager is a cancer research fundraising supremo!

When not busy raising awareness about payment card security, Bob Russo and his supporters, many of who are reading this now, have been working on another cause – cancer research. Team Russo, as the group is called, has raised 1.4 million dollars for the Jimmy Fund and Dana-Farber Cancer Institute over the past 10 years with annual participation in Boston's Fenway Park Fantasy Day as the cornerstone of their efforts.

Team Russo recently celebrated the dedication of a cancer research lab at Boston's Dana Farber Cancer center. The lab is dedicated to Bob's eldest son Rob, who is living with Sarcoma, and working hard to advocate for research in this area to help others also fighting the disease. Congratulations on this momentous milestone.

The Jimmy Fund
DANA-FARBER CANCER INSTITUTE

If you're interested in supporting The Jimmy Fund, you can find information here. Congratulations Team Russo.



Who's Who – Meet Your Board of Advisors

Berna Sirel
Vice President, IT Risk, Compliance and Information Security, Bankalararasi Kart Merkezi (BKM)

I am very excited to be seated on the 2013-2015 Board of Advisors, taking the opportunity to represent Bankalararasi Kart Merkezi (BKM) and Turkish payment industry in such a global and strategic platform.

Since it was founded in 1990, BKM has been the single Payment Service Provider for operating Message Switching System as well as Clearing & Settlement for all issuers & acquirers in Turkey.

Contribution of BKM from PCI SSC's CEMEA region will not only increase geographical diversity, but will also ensure that all voices from all acquirers and issuers in Turkey are heard.

I strongly believe, Turkey being one of the largest credit and debit card markets of Europe, with a good track record in fraud coupled with matured positive experience in chip and pin as an early adaptor, that BKM will have valuable contribution in the Board.

Phil Jones
Payment Security Manager, Barclaycard

I am thrilled that Barclaycard has been re-elected on to the PCI SSC Board of Advisors and would like to take this opportunity to thank all of the POs who voted for me. As someone who's attended numerous Board meetings in the past as an alternative representative, I'm delighted to be representing Barclaycard on the BoA in my own capacity, and will be keen to influence the Council towards making the PCI DSS easier for smaller merchants and in the adoption of a risk based approach for larger merchants.

Philip Morton
Information Security and Compliance Manager, British Airways

I am delighted to be representing British Airways and other Participating Organisations on the Payment Card Industry (PCI) Board of Advisors to the Security Standards Council for the period 2013-2015. British Airways has been involved with the Council and a supporter of the PCI Standards from the very start, and I am looking forward to assisting the Council in the development of their key work to protect cardholder data. My hopes for the Board include a desire for it to reflect the challenges that information security present to merchants and, in particular, I see my role as one of providing the Council's Executive Committee with appropriate feedback and guidance concerning such matters as:

- the development of the Council's priorities and strategic roadmap
- the future development of the PCI Data Security Standards.

BOARD OF ADVISORS

Ed Ritter
Senior Vice President, Information Security Policy and Governance Executive, Bank of America N.A.

Berna Sirel
IT Compliance, Risk and Information Security Vice President, Bankalararasi Kart Merkezi

Phil Jones
Payment Security Manager, Barclaycard

Philip Morton
Information Security and Compliance Manager, British Airways PLC

Kathy Orner
Vice President, Enterprise Governance and Chief Information Security Officer, Carlson

Pierre Chassigneux
Chief Risk & Audit Officer, Cartes Bancaires

Henrique Kazuhiro Takaki
Risk Control Manager, Cielo S.A.

Christian Janoff
Enterprise Architect, Cisco

Ash Khan
Head of Global Consumer Information Security, Citigroup Inc

Ugo Bechis
European Payment Council AISBL, Chairman - EPC Cards Working Group

Denise Wood
Corporate Vice President, Chief Information Security Officer and Chief IT Risk Officer, FedEx

Lara Nwokedi
Head, Information Security, First Bank of Nigeria

Pierre Chassigneux
Chief Risk & Audit Officer, Cartes Bancaires "CB"

On behalf of the CB Card Scheme, I would like to thank all the Participating Organizations that supported our recent re-election to the Board of Advisors. During my tenure, CB will once again be committed to play an active role in supporting PCI and sharing with the BOA our knowledge and expertise within the French and European markets.

Izdehar Safarini
Deputy CEO – Technical and Operation, Middle East Payment Services, Inc.

I am honored and proud to represent MEPS as the first PCI Board of Advisors member from the Middle East. I am looking forward to provide an active contribution to the development, awareness and adoption of payment card industry security standards in the Middle East. Thanks to all the PO's who supported me in the election process and for granting me this great opportunity.

Kevin Glass
Senior Manager, Information Security, PayPal

I am very excited to represent PayPal on the PCI Council Board of Advisors. It is a privilege to be a voice for merchants, service providers and payment innovators in the process of advancing information security standards and guidance.

Dave Faoro
Vice President, Payment Security Officer, VeriFone

Serving on the PCI SSC Board is a pleasure and an honor. As Chief Payment Security Officer of VeriFone, I look forward to working with other industry leaders to not only promote existing payment security requirements, but to also assist in the creation of new, emerging security guidelines that address industry trends, such as mobile commerce, and mobile payments in particular.

Peter Cooper
Group Information Risk Manager, Business Technology Services, Woolworths Limited

Woolworths is proud to again be representing the APAC region on the BoA. It's a great opportunity to share insights into the practical challenges that PCI presents for large and complex organisations as well as raising awareness among the PCI community in the region of the council and its good work.

BOARD OF ADVISORS

John W. Graham
Vice President Global Information Assurance & Risk, First Data Merchant Services

Rodney Farmer
President, Global Payments Europe, Global Payments Inc

Eric Brier
Chief Security Officer, Ingenico

James Walsh
Chief Information Security Officer, Micros

Izdehar Safarini
Deputy CEO – Technical and Operation, Middle East Payment Services (MEPS)

Kevin Glass
Senior Manager, Information Security, PayPal Inc

Joseph Finizo
President / CEO, Retail Solutions Providers Association (RSPA)

Rob Sadowski
Director, Payment Solutions, RSA

David Estlick
Vice President, Global Infrastructure and Enterprise Security, Starbucks Coffee Company

Dave Faoro
Vice President, Payment Security Officer, VeriFone Inc

Mike Cook
Senior Vice President Finance & Assistant Treasurer, Wal-Mart Stores Inc

Peter Cooper
Group Information Risk Manager, Woolworths Limited

PCI SIG Highlights

Submit your ideas for Special Interest Group (SIG) projects

Now through 25 July you're invited to submit your ideas for Special Interest Group (SIG) projects.

SIGs are PCI community-led initiatives that address specific areas or security challenges in relation to the PCI Standards. Whether you've participated in the past or never been involved, we encourage you to take advantage of this great opportunity to shape PCI focus areas in the coming year.

"Because the Risk Assessment SIG was such a rewarding experience, I joined the Maintaining PCI Compliance SIG! While working to draft a guidance document, you have the opportunity to discuss how the standards affect your organization and learn how others have addressed similar issues. Because SIG membership is so diverse, it is a great opportunity to understand a lot of different perspectives."

– **Renee I. Hodder**, Information Security Analyst IV, Progressive Insurance, is an active participant in the 2013 Best Practices for Maintaining PCI DSS Compliance SIG

"As security professionals, we are typically focused on our own domains and issues that directly affect us or those of our customers. Working as a team on the SIG changes that paradigm. In the meetings, we are exposed to a variety of unfamiliar scenarios as we discuss complex payment environments from across the globe. The nature of this collaboration helps us to individually expand our personal levels of expertise while at the same time allowing us to give back to the community and influence the direction of PCI compliance with our input. SIGs are the forum where the requirements of PCI are blended with industry best practices as determined by its expert members so that practical guidelines can be produced to help everyone who struggles with PCI on a regular basis. It is an honor and a privilege to be able to contribute to that process. "

– **Brad Cyprus**, Chief of Security and Compliance, VendorSafe is an active participant in the 2013 Third Party Security Assurance SIG

SURVEY SAYS...

In the recent annual PCI PO survey, Participating Organizations cited the opportunity to participate in SIGs and benefit from SIG documents as a key membership value and a reason for continuing membership with the Council.

"To stay involved with new requirements and SIGs to further the cause of data security"

"Learn about the latest PCI updates and have access to information as it is being developed in the SIGs"

"I enjoy participating in the community meetings and SIG process, which allows for more insight into the evolution of the PCI DSS controls."

"Receiving breaking news, guidance documentation and SIG outcomes is a bonus that allows us to stay ahead of the curve, also like to participate in some of the SIGs."

SIG FACTS & FIGURES

7	SIG proposals presented at the 2012 Community Meetings
35	Percentage of POs that voted in the 2013 election
150+	Organizations that participated in Special Interest Groups in 2012
7	Information Supplements published since 2006; with two more currently in development
48 hours	Average annual time commitment to contribute a SIG

Review the SIG Information Supplements on our website:

- PCI DSS E-commerce Guidelines
- PCI DSS Cloud Computing Guidelines
- PCI DSS Risk Assessment Guidelines
- PCI DSS Wireless Guideline
- PCI DSS Virtualization Guidelines
- PCI DSS Tokenization Guidelines
- PCI DSS Applicability in an EMV Environment v1.0

Interested in submitting for the January 2014 newsletter?
Email us at pcinewsletter@pcisecuritystandards.org to learn more!

Technology Update

Point-to-Point Encryption

The building blocks of a strong security program are people, processes and technology. The PCI Standards help businesses address these core components to protect their payment card data. Point-to-Point Encryption (P2PE) technology can help merchants simplify their PCI compliance programs by eliminating clear-text cardholder data from a merchant's environment and reducing the scope of PCI DSS requirements.

The Council's P2PE program provides a method for vendors to validate their P2PE solutions and applications, and for merchants to reduce the scope of their PCI DSS assessments by using a validated and PCI-listed P2PE solution for accepting and processing payment card data. The PCI P2PE validated applications listing is now available. Congratulations to Handpoint and The Logic Group as our first companies on the listing – below, they share a few words on the value of this program in helping improve payment card security.

"P2PE represents a significant breakthrough for mobile payments in the enterprise retail market. It has allowed us to overcome the barriers that have prevented enterprise retailers in Europe from embracing mobile payments; namely concerns over security, compliance and integration. Processing card payments on smartphones and tablets themselves is simply not secure enough for the enterprise market. The P2PE certification from PCI enables us to provide a secure robust mobile payment application on a PCI PTS-approved secure card reader that, when used as part of a PCI-validated P2PE solution, can be easily integrated into any payment system or retail environment. Most significantly, PCI-validated P2PE solutions will save retailers time and money on PCI compliance procedures."

– **David Gudjonsson,** CEO and co-founder, Handpoint

"As a supporter of the PCI DSS standard it was a natural step for the Logic Group to look at the Point to Point Encryption standard (P2PE) and to assess the benefits that a solution would offer to our clients.

Our P2PE application, Solve Datashield will form a key part of The Logic Group's P2PE solution and we were extremely pleased to achieve a world first in gaining accreditation for the application. The benefits to our merchant base are clear. Not only does use of a PCI-listed P2PE solution enhance the security of their card present payments but it also allows a merchant to concentrate on what they do best, namely selling their goods knowing that whatever the nature of their store environment this card payment data is transmitted securely through to the bank.

We are already moving towards accreditation for our full P2PE service and look forward to providing input to the PCI SSC through the various Special Interest Groups (SIGs) as the new standards are developed."

– Robin Adams, Director of Technical Strategy & Architecture, The Logic Group

Applications play an important part in the development of solutions, but don't forget – listed P2PE applications must be part of a validated P2PE solution to enable any merchant PCI DSS scope reduction. If you're a P2PE solution developer, please take advantage of this listing in developing your P2PE solution. For more information on submitting an application or solution for PCI validation, please visit the P2PE program page on the PCI SSC website, or contact p2pe@pcisecuritystandards.org.

Questions? Use the PCI Knowledge Base FAQ tool and search by the P2PE category.

ISA numbers are rising worldwide

Since the launch of the Internal Security Assessor Program in 2010, there has been a steady increase in payments professionals participating in the program.

2010	164
2011	591
2012	1006
2013	1093

New Member Spotlight

Austria Card-Plastikkarten und Ausweissysteme Ges.m.b.H.

Austria Card is a market leading and internationally operating company in the field of secure communications for payment, government and industrial applications. The development of a native operating system for smart cards (ACOS) in Austria Card's in-house Research and Development Department is one of the key components for today's success: ACOS complies with the global EMV standards and allows for flexible solutions to individual customer requests. Being experts in personalisation as well as data processing, Austria Card has leveraged its experience and knowledge to offer products and services for and beyond smart cards. For further information please visit www.austriacard.at.

Careington International Corp.

Since 1979, Careington has provided affordable dental and other health-related products to nine million members nationwide. As a licensed Discount Medical Plan Organization (DMPO) our portfolio of more than 100 industry-best discount plans delivers savings and value to our customers. Careington incorporates innovation into every aspect of our security-minded, service-oriented operation. Careington joined PCI SCC to ensure we are apprised of the latest developments in PCI so we can continue to identify and implement security measures that provide the strongest possible safeguards for the information stored in our systems including but not limited to credit card data.

Delta Air Lines, Inc

Headquartered in Atlanta, Delta Air Lines serves more than 160 million customers each year. Delta and the Delta Connection carriers offer service to 59 countries on six continents. A founding member of the SkyTeam global alliance, Delta participates in the industry's leading trans-Atlantic joint venture with Air France-KLM and Alitalia. Committed to safety and security, ensuring the confidentiality of customer's credit card information is paramount. Delta has been PCI compliant since 2007. Being a Participating Organization allows us to be more proactive regarding changes to the PCI requirements and PCI-related activities of the other Participating Organizations.

Emerging Markets Payments (EMP)

Emerging Markets Payments (EMP) is a leading electronic payments processing company in the Middle East and Africa (MEA). The company covers all elements of the payments value chain, from issuing, acquiring and switching through to card procurement and personalization. EMP is currently partner to over 130 banks and 30,000 retailers across 45 countries in MEA. The company also offers a full range of eGovernment solutions. EMP offices are located in Cairo, Egypt; Amman, Jordan; Lagos, Nigeria; Cape Town and Johannesburg, South Africa. For more information, please visit: www.emp-group.com.

Giesecke & Devrient GmbH (G&D)

Giesecke & Devrient (G&D) is a leading international technology provider headquartered in Munich, Germany. G&D develops, produces, and distributes products and solutions in the payment, secure communication, and identity management sectors. The Group's customer base mainly comprises central and commercial banks, mobile network operators, business enterprises, governments, and public authorities. G&D joined the PCI Security Standards Council to support safeguarding reliable transactions and authenticity within the industry and to contribute to the development of existing and future security guidelines for the payment sector. For more information, please visit: www.gi-de.com.

NEW PARTICIPATING ORGANIZATIONS

Congratulations to our new Participating Organizations!

Participating Organizations are the foundation of the PCI Council. We're pleased to welcome a number of new organizations representing a variety of industries and geographies.

The following companies have joined the PCI Council in the last six months.

- AAA National American Automobile Association
- ABECS
- Abu Dhabi Commercial Bank (ADCB)
- Accor
- Aon Service Corp
- Arxan Technologies
- Aurora Financial Systems Inc
- Austria Card-Plastikkarten und Ausweissysteme GmbH
- BBPOS Limited
- Canadian Imperial Bank of Commerce (CIBC)
- Careington International Corp
- CDG Commerce
- Celerity IT LLC
- Charter Communications
- City of Sacramento
- Cognia
- College Entrance Examination Board
- Continental Finance Company LLC
- CR2 Limited
- Credit Union Australia
- CyberSource Corporation
- Davis and Henderson
- Deloitte & Touche LLP (USA)
- Delta Air Lines Inc
- Demandware Inc
- Dubai Aviation Corp (flydubai)
- Ecentric Switch (Pty) Ltd
- Emerging Markets Payments
- Epsilon Data Management
- EVO Payments International
- Fair Isaac Corporation (FICO)
- Feitian Technologies Co Ltd
- First Bank of Nigeria
- Flint Mobile
- Giesecke and Devrient GmbH
- Groupon
- Habib Bank Limited

Promocion y Operacion SA de CV (PROSA)

Founded 45 years ago, PROSA has strengthened its participation in Mexico's payment card industry to protect payment card data. Since the creation of the PCI DSS, we have achieved compliance with the same, and constantly increase our level of maturity and culture of security of payment cards for the Mexican financial industry. Currently, it is very important for us to be a Participating Organization and to be involved in the Special Interest Groups, since it allows us to exchange opinions of specialists in the industry and learn about new trends and security risks in the payment card industry.

Scheidt & Bachmann USA, Inc.

As a world-class transportation solutions provider, Scheidt & Bachmann recognizes the importance of complying with PCI Security Standards as part of the company's mission to provide parking and public transportation industries with reliable and effective solutions. With the changing ease of payment methods in transportation, the company places priority on protecting the process of exchanging secure data information. This emphasis on responsibility, attention to detail and high standard of performance will secure Scheidt & Bachmann's longevity and reputation in the industry.

Semafone Limited

Semafone protects customers who are making a payment over the telephone using a credit or debit card. Our customers span Europe, North America, Africa and Australia, in industries ranging from financial services and retail to government and airlines. We believe that PCI regulations exemplify best practice in the industry and that as a technology company it is our responsibility to make PCI compliance as simple and easy as possible. We are delighted to be a Participating Organization of the PCI Security Standards Council!

Shenzhen Sunson Tech Co., Ltd

Shenzhen Sunson Tech Co., Ltd is one of the leading manufacturers of rugged metal PinPad devices in China. Established in 2003, Sunson focuses on the encrypted pinpad (EPP) for financial self-service terminals (ATMs, CRS and kiosks, etc.). With an experienced R&D team, Sunson EPPs gained the certificate from China Union Pay (CUP) in 2005. Sunson earned PCI PTS 2.0 and PCI PTS 3.0 approval from PCI SSC in 2010 and 2012. To keep pace with payment security technology, provide secure EPPs to our clients, and share the encryption technology, Sunson has joined PCI SSC as a Participating Organization.

TNS Smart Network, Inc. (TNS)

TNS Smart Network Inc. (TNS) is a premier payment processing acquirer organization operating the largest network of White Label ABMs in Canada. TNS is also a Direct Connect member of the IMN (Inter Member Network) of the SCD (Shared Cash Dispensing) processing network of Interac Association. Joining the PCI Security Standards Council will allow TNS to review drafts of all revisions to the DSS and PA-DSS specifications, and any new specifications prior to release, recommend new initiatives for consideration and provide the Council with understanding and guidance on technology/recommend changes and improvements to the PCI Standards.

NEW PARTICIPATING ORGANIZATIONS

- Health Alliance Plan
- Hitachi-Omron Terminal Solutions Corp
- HVHC Inc
- Hyatt Hotels Corporation
- IntegraPay Pty Ltd
- International Franchise Association
- Jack In the Box Inc
- James Avery Craftsman
- Johnson & Wales University
- Lego Systems Inc
- Magnetic North Software Limited
- MegaPath Inc
- Merseyrail Electrics 2002 Ltd
- Middle East Payment Services (MEPS)
- Move Sales Inc
- Navy Federal Credit Union
- NewNet Communication Technologies
- Parlex Pacific Limited (a Johnson Electric Company)
- PAX Computer Technology (Shenzhen) Co Ltd
- PayU SA
- Post Office
- Priceline.com
- Promocion y Operacion SA de CV (PROSA)
- Ralph Lauren Corporation
- Rational Group Limited
- Research In Motion Ltd
- Sabre Inc
- Samport Payment Services AB
- Scheidt & Bachmann USA Inc
- Secure Hosting Ltd
- Securenet Payment Systems
- SemaFone Limited
- Shenzhen Kaifa Technology CO Ltd
- Shenzhen Sunson Tech Co Ltd
- Shred Works Inc
- Sirius XM
- Spire Payments Holdings SARL
- Strategic Payments Services Pty Ltd
- The Liquor Control Board of Ontario
- TNS Smart Network Inc
- Towne Park Ltd
- United HealthCare Services Inc
- University of Miami
- University of New Mexico - IT Security
- Vantiv LLC
- Viseca Card Services SA
- Web.com
- Yorkshire Building Society