Safer Business Newsletter

Autumn 2014

Welcome!

To our new look newsletter, we hope you like the new branding....

Hello and welcome to this, the third edition of our safer Business Newsletter of 2014, and the first using our new branding, and formatting. I am sure that you will agree that our new brand is more modern, and portrays WorldPay as being the Leader in Modern Money. We have also modernised our own approach to the newsletters, by introducing our new 'Step up to the Mic' and 'Tech Talk' sections.

I hope that you have all had a relaxing time away from the work place over the summer holidays and that you are all ready to gear up ready for the pre Christmas rush. Yes, I have said the dreaded word, but it is September, and Santa will soon have to fill his large sack with lots of expensive goodies, which means that you will all be very busy ensuring that your payments are stored, processed and transmitted securely.

We have some fantastic articles in this edition for you to enjoy, so read on to find out more. Jeremy King, International Director at the PCI Security standards Council is 'stepping up to the mic' in this edition and has written 2 interesting articles. The first on the impending PCI SSC Community Meetings, and the second on how European Card Fraud has hit an all time record. These both make very interesting reading.

We have Connie Penn from Kilrush Consultancy writing for us again; this time on PCI in the level 2 arena, and how validating compliance can be achieved and the MasterCard requirements for doing so.

The concerns around v3.0 of the PCI DSS still continue to rumble on, so we have included some further clarification/guidance for you, which we hope you will find beneficial. In addition to this, Visa Europe has also recently launched TIP2,

We have also included some recent security alerts for your information, the first via Visa on Remote access, and the second on Magneto Extension that has been communicated to us via Foregenix. These alerts along with a reminder on Windows XP end of support will be of particular interest to your IT colleagues.

So, enjoy reading and as always, I hope you find this content useful

Tracey Long
Tracey.Long@worldpay.com
Worldpay: www.worldpay.com

In this issue

worldpay

Industry Events – Autumn 2014

(All events are in London unless otherwise stated and are mostly (v) Vendorcom or (a) AKJ Associates)

September 2014

16th: Thought Leadership Conference (v)

17th: PCI Contact Centre (a)

9-11th: PCI SSC Community meeting, North America Orlando)

30th Sept – 1st Oct: MasterCard ARM conference, Europe (Dublin)

October 2014

7-9th: PCI SSC Community meeting, Europe (Berlin)

22nd: Payment Security & Risk Management SIG (v)

23rd: eCrime & Information Security Conference (a)

November 2014

12th: Payments in Retail (v)

18-19th: PCI SSC Community meeting, Asia Pacific (Sydney)

26th: Mobile Payments (v)

27th: PCI Europe Amsterdam (a)

Quarterly Reporting Date

Your next progress update should be submitted to us no later than
Friday 19th September 2014

Please remember:

- Milestone report via prioritised approach tool(if working towards compliance)
- Latest RoC or SAQ with AoC (if compliant)
- Network vulnerability scan executive report.
- Confirmation you are using a PA DSS compliant payment application.
- Confirmation you are not storing Sensitive Authentication Data (SAD) in any of your systems.

Any queries please contact your dedicated PCI manager at Worldpay who will be more than happy to help. https://support.worldpay.com/support/saferbusiness/

In Focus - The PCI SSC Community Meetings.

Ensuring the security of payment card data is everybody's business, and the PCI Security Standards Council works together with the entire payments community to accomplish this goal. In fact, that's the overarching theme of this year's 2014 European Community Meeting being held in Berlin in October: securing the future of payments together.

Our global community encompasses all areas of the payment card processing industry. Participants are able to review, discuss and comment on new versions of the PCI Security Standards, learn about Council initiatives, and share their experiences and best practices. In addition they nominate and vote on Special Interest Group projects, and take a more active role by nominating themselves for our Board of Advisors.

The Community Meetings mark the one time each year that this community gathers together in one place. This year, we expect more than 600 global payment security leaders from the European region to attend –across all industries from airlines to education, retail to hospitality – and everything in between - including business owners, store operators and hotel managers, who are trying to understand how to make PCI a part of their daily business practices.

This year's program offers a variety of ways for you to participate in the community, collaborate and network with your peers, and share feedback with the Council, members of the payment card brands and other stakeholders. And new this year following feedback received from our community – an extra day has been added to the agenda to accommodate technical and business tracks, so you can customize your experience.

Starting on day one, you can choose to attend the technology symposium – or if you're new to the Community Meeting, you may prefer to attend our PCI 101 session. On day two, we are very excited to welcome Admiral James Stavridis, who'll reveal some untraditional cybersecurity tools and how they affect the global marketplace. On day three, we have a keynote from Bob Arno who has infiltrated criminal gangs of credit card thieves around the world. This is sure to be an eye-opener – and a session you won't want to miss!
There will also be sessions on the ROI of PCI, PCI Forensics, tokenization and more. Plus, you can get tips directly from the PCI Standards team on implementing version 3.0 of the PCI-DSS and PA-DSS along with the Council's current work in technology areas such as tokenization, PTS technology and more. Not forgetting the PCI and Brand Booths where your specific questions can be answered.
One of the ways the Council is facilitating collaboration, is by offering PCI in Practice sessions – back by popular demand!
Implementing long-term PCI compliance programs that build security into every day practices is critical to protecting payment card data - in this unique forum, merchants and acquirers will share their real-world successes and challenges in doing so through case study presentations.
The Council also facilitates networking opportunities to make it easier to connect with others in your industry. The "birds of a feather" program designates specific zones for the following industries: education, healthcare, hospitality, insurance/financial, restaurants and food service, travel and transportation – including airlines, and utilities. Look for designated industry signs on the tables during scheduled networking times - including receptions to help you find each other.
A great tool for collaboration and networking at this year's meeting is the mobile app. It offers easy and on-the-go access to the latest information about the meeting. Some of the key features of the mobile app include:

- Access the event schedule anytime and customise your agenda
- See all the speakers and read their bios
- Check out the exhibitors and locate their booths
- See who's attending and share contact information so you can set up meetings in advance of arriving on site - This is a great way to invite other attendees to meet you at the industry designated tables.

There is time allotted for you to engage directly with representatives from the payment card brands as well.
The Community Meeting also features a vendor showcase where the world's leading technology and service providers exhibit their products. You can find the most up-to-date list of those companies exhibiting in the vendor showcase on the PCI Community Meetings microsite.
The 2014 European Community Meeting takes place 7-9 October at the Maritim Hotel Berlin, centrally located between Kurfürstendamm and the Brandenburg Gate.

A Closer Look – Level 2 Merchants & MasterCard.

Connie Penn of Kilrush Consulting wrote a piece for our newsletter in Q1 2013 regarding the challenges and issues facing small and medium sized merchants in identifying their PCI compliance position. She has continued to work with Worldpay and other UK acquirers to identify other ways to reduce the cost and burden of becoming compliant and evidencing that compliance and written a follow up article for us this quarter.
UK merchants process their face to face card data in a mature Chip and Pin environment, and often also process card data in other channels – Mail Order, Telephone Order/Customer Services and eCommerce. A large number of UK merchants outsource this card processing to third parties, with the result that often merchants do not have a cardholder data footprint in their environment.
Many level 2 merchants also outsource most of their IT and only

have a small retained team therefore they don't have a dedicated IT and security person suitable to be trained as an Internal Security Assessor (ISA) and complete the relevant SAQ's. As a consequence, merchants have to retain QSA's to evaluate their environments. Where merchants feel they don't have a cardholder data footprint, it is difficult to cost justify QSA support to evaluate and evidence compliance.

In addition to meeting the requirements of PCI DSS, Kilrush Consulting encourages merchants to secure their business against growing internet based threats, by improving IT Security generally across the business not just around card data. With these challenges in mind we went to market to look for a registered QSA organisation willing to look at a new approach. This would mean they would act as a security partner for clients and would complete the appropriate SAQ's, per channel if required, acting as an ISA. As well as this they could provide security advice, guidance and additional support services across the business not just around card data.

We partnered with Cipher, a multinational, specialist Information Security and Risk Management company focused on Protection of Information systems, Prevention of financial losses caused by fraud and Compliance with evolving regulations. Cipher agreed to look at the proposal and a formal "Technical and Commercial Proposal" for PCI DSS Services and Security Support for one client was completed.

The client accepted the proposal on condition their acquirer, Worldpay, and the Card Schemes also accepted the approach, particularly in relation to the QSA acting as an ISA and able to complete SAQ's per channel instead of a ROC. Happily Worldpay approved the approach and saw it as a continuation of it's strong working relationship with both it's Merchants and the Card Schemes to be flexible in the reporting of compliance per channel. Worldpay had already obtained approval from Visa Europe for this approach prior to the engagement with Cipher; they then negotiated with MasterCard who also agreed to the approach on a merchant by merchant basis.

Conditions:

- ALL payment channels are outsourced
- Merchant completes transaction journeys for all of it's channels
- Merchant employs a Security Company which has security experts who are qualified QSA's to manage elements of the security of the merchant environment;
- *Evaluate the architecture and network and advise how best to maintain them securely*
- *Complete vulnerability scanning, penetration testing AND work with the merchant to evaluate and remediate the results. This is undertaken subject to correct segregation of duties and formal SLA's*
- *Help the merchant manage it's perimeter better and watch for intrusion attempts so immediate action can be taken should any compromise attempts be detected.*

Deliverable

SAQ for each environment completed by the merchant and security company with a qualified QSA, signed by an officer of the merchant company and the Security company and supported with;

- Clear and detailed transaction journeys for each channel outlining the architecture and listing the 3rd parties handling the outsourced card data
- Supply of vulnerability test results and penetration test results

Step Up to the Mic – Jeremy King

According to the latest report released by FICO, a leading analytics software company, card fraud across Europe has reached an all-time high, beating the previous high set back in 2008. Card fraud losses across Europe hit €1.55 billion, an increase of 6.2% over the previous year. Interestingly, the UK and France together accounted for 65% of the total fraud losses across the 19 countries included in the report. This is supported by the annual fraud report from the UK Cards Association. Face to face fraud

declined significantly in the years after 2008, whereas card-not-present (CNP) fraud has remained stubbornly high. Whilst mandating CVV/CVC 2 use, and the rollout of 3-D Secure made some initial impression, the fraud figures for CNP have in 2013 grown to over £300M and the expected trend will see this figure continue to rise.

Impact on PCI

What these results clearly show is that on its own EMV is not the answer to card fraud. Whilst it is very successful at reducing face to face fraud, the criminals simply migrate to the next weakest part of the payments chain, which is CNP.

From a PCI SSC perspective, these resuts fully support the fact that in order to tackle fraud you need PCI and EMV together. What it also clearly shows is that everyone invovled in the transaction lifecycle must adopt and implement the PCI DSS controls in order to remove the source of cardholder data for the criminals.

Unfortunately, it is still far too easy for criminals to gain access to company systems where they can install malware to capture cardholder data. To counter this means tackling the three key topics; people, process and technology.

People, Process and Technology

People: As a UK prime minister once said, it is all about Education, Education, Education, and not just of your sales asistants or front office staff. This means starting at the top and training your board to understand why data security is essential for your organisation. Then rolling this out across your entire organisation. It means having clear solid password requirements that ensure easy to guess passwords such as "Password1" or " Summer14" are not permitted.

Process: Is all about reinforcing the training with clear processess to help your staff stay focussed and understand why data security is necessary, and how they can help protect your customers and your organisation. PCI have a range of helpful guidance documents covering many topics which can be found on our website. Including a newly updated Anti Skimming Best Practises document.

Technology: Techology is constantly changing, with new options for payments it seems being introduced almost monthly. Unfortunately, this new technology can bring new opportunities for the criminals and introduce new weaknessses to your organisation.

In terms of CNP fraud, we are seeing many organisations use the services of a third party payment provider to remove cardholder data from their environment.

Whilst this is a very understandable and positive step, there are some key risks that you should be aware of and some critical steps that organisations should follow to help ensure that by using a third party provider you are not introducing weaknesses into your system.

The issue around third party providers was considered of such high priority by the PCI community that in 2013 it was voted for and selected as a Special Interest Group (SIG) project. PCI SSC runs two Special Interest Group projects each year on topics submitted and voted on by members of the PCI community, representing organizations across industries and around the world.

The SIG developed the Third-Party Security Assurance Information Supplement to provide specific recommendations for meeting PCI Data Security Standard (PCI DSS) requirement 12.8 to ensure payment data and systems entrusted to third parties are maintained in a secure and compliant manner.

This guidance is available on PCI's website. The guidance, along with SIG projects currently underway and proposed projects for 2015, will be discussed at the 2014 Community Meetings in Orlando on September 9th – 11th and in Berlin on October 7th – 9th.

What is clear is that if you are going to use a third party, firstly check to ensure that they are PCI DSS compliant and that this compliance has been assessed by an independent Qualified Security Assessor(QSA).

If your third party provider supplies and manages the payments page of

your website, then please pay careful attention as to how and when the customer is re-directed.
Unfortunately there are many solutions which can allow the criminal to gain acces to the cardholder data. As a result of this, the PCI SSC introduced new requirements in the latest version of the PCI DSS, especially the Self-Assessment Questionaires (SAQ), introducing a new SAQ A-EP. Further information on this topic can be found on our website ,but also from the card schemes and your acquirer. This is an area where the brands are seeing a lot of fraud, so do pay close attention and do follow the guidance.

Conclusion

What is clear is that there remains a significant effort here in Europe to ensure the protection of cardholder data throughout the transaction process, and PCI SSC remains best positioned to provide support in this task.
Card-not-present fraud is real and is happening here in Europe - unfortunately the figures do not lie. It is up to you and your organisation to adopt and implement the PCI DSS as well as utilising all of the support and guidance available to make sure it does not happen to you.

Remember: People, Process and Technology.

Version 3 Developments

Hopefully you are all aware that the PCI SSC have released their prioritised approach tool for PCI DSS version 3.....
https://www.pcisecuritystandards.org/documents/Prioritized_Approach_v3.xlsx
As you know this is a fantastic resource to allow you to track your progress towards compliance to the Data Security Standard and, as your acquirer, we request updated versions from you all on a quarterly basis in order to accurately report your compliance position to the Card Schemes.
We hope that you are busy reviewing the changes to the document and preparing your next update to us for mid-September.
The only negative we could find with the new document was the lack of flexibility it provided in reporting either a channel by channel compliance position or progress towards a self assessment questionnaire (Level 2 & 3 merchants). In these circumstances there are controls that are simply not applicable and that option did not exist.....However we are pleased to inform you that we raised this with the Council and a new PAT will be available very shortly with this capability – Hurrah! Keep an eye out for the document release on the Council website or contact your dedicated PCI manager here at Worldpay for further information.

A or A-EP, that seems to be the ongoing question.....(!)

The changes version 3 have introduced for the eCommerce payment channel have got everyone talking throughout this year and for good reason. The changes have meant that there is a distinct possibility of more DSS controls being applicable to your environments. In order to help clarify the changes and their intent Visa Europe released a 'Processing eCommerce Payments Guide' in early August. We believe it is a fantastic guide to help you determine your compliance requirements and risk exposure and thoroughly recommend you reading it
http://www.visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx.
We are confident this will resolve the outstanding questions you might have and allow you to confidently review the scope of your security obligations for your eCommerce payment channel.

Visa Europe have been very busy in the last quarter and it's fantastic news for both you as merchants and us as your acquirer, without their assistance and guidance we would not be able to answer all those niggly DSS queries.....

Visa Europe's Technology Innovation Programme 2 or TIP2

Hot on the heels of the eCommerce guide Visa Europe also released their updated technology innovation programme – handily referred to as TIP2. Here's a quick overview and we'll hope to bring you more in our next newsletter direct from the team themselves.....

- Revised to align with v3 of PCIDSS & reflect the current threats to CHD in an EMV environment
- Participation is optional, however compliance maybe simplified if adopted
- Classifies DSS requirements in milestones 1&2 as mandatory & recommended, therefore allowing Acquirers to adopt a risk based approach with individual merchants
- Provides a way of recognising investment in non-validated P2PE solutions by giving a mechanism for all parties to gain assurance of the level of protection offered by the non-validated solution.

To qualify for entry to TIP, a merchant must:

- Have separated their face-to-face channels from their e-commerce and MOTO channels
- Have at least 95% of the total face-to-face POS transaction count originate from approved chip-enabled devices
- Not have been involved in an account data compromise within the last 12 months.

Watch this space for more news on the programme before the end of the year however in the meantime, if you have any questions at all, please contact your dedicated PCI manager for more information.

Tech Talk

We think it's beneficial for our customers to be 'in the know' so this is our new 'Tech Talk' section hopefully covering things of interest within and around Card Payment security....

Windows XP

It's five months since the demise of Windows XP – you were aware weren't you?! Just in case it missed you, XP is no longer supported by Microsoft. From April 8th 2014 no patches or security updates have been or will be released by Microsoft for XP meaning that any payment system and computers still running it will be vulnerable to future attacks. Hopefully you've all resolved this issue by upgrading to a later version. Organisations using unsupported systems cannot comply with requirements 6.1 & 6.2 which requires the latest vendor patches to be installed, here's a couple of links to help you

https://www.pcisecuritystandards.org/documents/PCI-WindowsXPV4_(1).pdf
https://www.pcisecuritystandards.org/faq/ (search for FAQ 1130)

However, no sooner have we dealt with the 'death of XP' there is further news from Microsoft about other key products which have support deadlines approaching including windows 7. Here's a brief run down;

- Windows 7 (Enterprise, Home Basic, Home Premium, Ultimate & Starter): Mainstream, free support is ending on January 13, 2015. Extended support for Windows 7 lasts until January 14, 2020.

We've heard some industry watchers have speculated that Microsoft will end up pushing out Windows 7's support dates the way the company did for XP, given Windows 7's popularity and pervasiveness, but so far, there's been no word from Microsoft officials that this is the plan.

- Windows Server 2008 and 2008 R2 and all editions of Windows Storage: Mainstream support also ends on January 13, 2015.

- Windows Server 2003: Complete end of support is approaching next year, as well. On July 14, 2015, Microsoft's extended support period for that product cuts off, which

means the company won't be issuing patches, updates or fixes of any kind for that operating system (unless users have pricey Custom Support Agreements in place).

As we are reliably informed upgrades and migrations can take a while, the average being 200 days so we're told, So now is the time to act and start planning for your migration and keep your compliance up to date.

Remote Access: Alert from Visa

We've received notification from Visa that they have recently observed an increase in malicious remote access activity associated with unauthorized access to merchant Point-of-Sale (POS) environments and ultimately, payment card data. The details are as follows;

Insecure Remote Access:

A number of remote access solutions are commonly used to provide remote management and support for retailers (e.g., LogMeIn, PCAnywhere, VNC, and Microsoft Remote Desktop).

Used correctly, remote management applications are an effective method of providing technical support among large numbers of merchants. Used maliciously, they potentially expose payment card data and other sensitive information to cybercriminals.

Insecurely deployed remote access applications create a conduit for cybercriminals to log in, establish additional "back doors" by installing malware, and steal payment card data. The risk of data compromise is increased when remote access applications are configured in a manner that does not comply with the Payment Card Industry Data Security Standard (PCI DSS).

The following are examples of common remote access vulnerabilities that can enable intruders to gain access to merchant POS environments. Please note that most of these are also violations of the PCI DSS.

- **Remote access ports and services always available on the Internet.**
- **Outdated or un-patched applications and systems.**
- **Use of default passwords or no password.**
- **Use of common usernames and passwords.**
- **Single-factor authentication.**
- **Improperly configured firewalls.**

Compromised Remote Access Credentials

An investigation of a series of leads from recent attacks against merchants throughout the United States, pointed to a common threat involving remote access software operating in the merchant POS environment. Attacks were suspected to have occurred as a result of compromised username/login credentials combined with remote management software exposed to the Internet.

The circumstances around multiple merchant compromises in the last several months suggest an actor or group of actors are targeting merchants who share common POS integrators or remote support vendors.

The attacks take place by successfully logging in to remote access applications, presumably using common username/password combinations that are shared among large groups of merchants. Once inside the merchant's network, an intruder will typically take steps to disable anti-virus applications and establish additional "back door" connectivity through the installation of malicious software (malware). On systems where payment card data is processed, card-capturing malware is often installed and used to collect full track data from the POS system. Finally, card data is exfiltrated to remote IP addresses.

Mitigation

Visa strongly urges merchants and payment system stakeholders to share this alert with their POS vendors, resellers and integrators. To address this threat, examine remote management software for insecure configurations, use of outdated or unpatched applications, common or easily-guessed usernames and passwords, and ensure that overall payment processing environment is securely configured and maintained in accordance with the PCI DSS.

Additionally, the following security practices will help mitigate security risks:

• Ensure proper firewall rules are in place, allowing remote access only from known IP addresses.
• If remote connectivity is required, enable it only when needed.
• Contact your support provider or POS vendor and verify that a unique username and password exists for each of your remote management applications.
• Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment.
• Plan to migrate away from outdated or unsupported operating systems like Windows XP.
• Enable logging in remote management applications.
• Do not use default or easily-guessed passwords.
• Restrict access to only the service provider and only for established time periods.
• Only use remote access applications that offer strong security controls.
• Always use two-factor authentication for remote access. Two factor authentication can be something you *have* (a device) as well as something you *know* (a password).

Magento : Alert from Foregenix

Through it's forensic investigations Information Security specialist & PCI QSA company Foregenix have idenitified a new compromise trend specific to Magento users. The system compromises relate to either attackers introducing extensions to provide back door access or users unknowingly installing compromised or fake extensions to the Magento framework. The extensions permit remote unauthorised users to access the impacted site and make system modifications to harvest payment card details. For further information please follow this link http://www.foregenix.com/resources/whitepapers/FGX-2014-005_advisory_Magento%20Extension%20Alert.pdf

Thanks for reading!

Thank you for taking the time to read our newsletter. Should you have any questions about the contents, please contact either your dedicated PCI Manager or email paymentsecurity@worldpay.com.
If you would like to read any of the previous editions of the newsletter, you can find the full back catalogue on our website at: https://support.worldpay.com/support/saferbusiness/