

PCI Update Newsletter | September 2009

How time flies!

Welcome to the third edition of the RBS WorldPay PCI Update Newsletter. Once again we have new information and new articles that we hope will be useful to your business.



There's quite a lot to cover this month, but we hope that you find some, if not all of it, of interest. This edition includes;

- Payment Application Data Security Standard (PA-DSS)
- Visa Europe's October 2009 mandate: [Reminder](#)
- Compensating Controls
- RBS WorldPay PCI Level 4 Programme roll-out
- Industry Expert: **Veritape**

Plus all of the regular features!



Payment Application Data Security Standard (PA-DSS)

Payment applications (software) play a critical role in the processing, transferring and storage of card payment data, and in the small to medium sector payment applications are typically generic 'off-the-shelf' POS software products supplied either by the acquirer or payment application vendors.

The PA-DSS was developed by PCI Security Standards Council (SSC) to provide a global level of certified security for merchants (and their acquirers) when determining which payment app to use for card acceptance. PA-DSS applies to any commercially available applications which store, process or transmit card payment data. It is designed for payment applications that are sold, distributed or licensed to third parties and are installed 'off-the-shelf' with little or no customisation. The availability of PA-DSS certified applications will significantly reduce the risk of data compromises at small and medium sized merchants, as well as the cost for these entities to achieve and maintain PCI DSS compliance. Whilst use of PA-DSS certified applications will not guarantee compliance with PCI DSS, it will go a long way in securing card payment data, and will remove many of the risks which entities may face (sometimes inadvertently) as a result of the functions of their payment application.

For more information, and to see a list of products that have been independently validated against PA-DSS, please visit the PCI SCC website at: <https://www.pcisecuritystandards.org/>

Visa Europe has introduced mandates for the implementation of the PA-DSS. Effective 1 July 2010: Acquirers must ensure that all merchants using payment applications that either store (or cause to be stored) sensitive authentication data post-authorisation, or applications that are listed as 'vulnerable' by either Visa Europe or Visa Inc must move to applications that do not store sensitive authentication data.

If you require further information please visit the SSC website or make contact with one our PCI team.

Visa Europe's October compliance mandate

All eCommerce merchants processing fewer than one million Visa txns per annum (Levels 3 & 4) must use a PCI DSS certified service provider, or provide certification of their own PCI DSS compliance to their acquirer.

All impacted Level 3 merchants have been notified and we are working with each to ensure we get timely updates for Visa. You will find more information relating to this within our FAQ's which can be found at www.rbsworldpay.com/pcidss

As a Level 3 merchant you will have received reminders asking for an update to be supplied to your dedicated PCI manager. Please remember that we are here to help you and the more information you can provide with regards to your progress (especially the Prioritised Approach milestones) the more protection you will receive against Card Scheme Assessment Fees!

Your business must achieve at least one of the following requirements to meet Visa Europe's October deadline:

1. Achieve full PCI compliance and validate this with the appropriate documentation.
2. Outsource your eCommerce payment processing requirements to a PCI compliant Service Provider. Please specify the Provider to your PCI manager for verification as soon as possible and complete the Prioritised Approach tool if the other areas of your business are non compliant.

If neither of the above options are viable before the deadline, please ensure that you meet the requirement of option 3 below:

3. You **must** complete the Prioritised Approach model. As previously advised, this new risk based approach was launched to help merchants reach compliance. From **Q3 2009** RBS WorldPay must report merchant updates against progress of the 6 milestones to Visa and MasterCard. Visa has confirmed that once a merchant achieves milestones 1-4 of the Prioritised Approach they will avoid financial penalty for the purposes of this mandate only. The advantage of this model is that it not only enables you to quantify your progress towards compliance, but also gives us a high level information source so we can build a case on your behalf in an attempt to avoid any potential financial penalty for your business.

For more info, and access to the Merchant Reporting Tool, please go to www.rbsworldpay.com/pcidss. If in doubt please contact our PCI Compliance Team on 0207 672 6400 or email pcidss@rbs.co.uk.

Time is running out so if you have not yet provided us with your updates – please do not wait until it is too late!



PCI Update Newsletter | September 2009

Compensating Controls

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:

- 1) meet the intent and rigor of the original PCI DSS requirement
- 2) repel a compromise attempt with similar force
- 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements) and
- 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

Merchants wishing to use compensating controls should seek guidance and official verification from a Qualified Security Assessor (QSA). Merchants take full responsibility for any compensating control lodged within the Self Assessment Questionnaire (SAQ) and where there is a system breach related to the control in place, the merchant would be fully liable for any subsequent Card Scheme Assessment Fees.

RBS WorldPay reserves the right to challenge and dismiss any compensating control that is in conflict with the requirements of the PCI DSS. One industry standard, and an area that no QSA would ever accept a compensating control for, is based around requirement 3.2 which deals with sensitive data storage.

RBS WorldPay PCI Level 4 Programme roll-out

The focus of PCI DSS up to now has been firmly on the Level 1-3 merchants however Visa Europe's October mandate (reiterated above) brings the eCommerce element of Level 4 merchants in to scope.

Over the coming weeks and months RBS WorldPay will launch its PCI Level 4 Programme working in conjunction with our chosen security partner **Arsenal Security Group**. Arsenal are a Qualified Security Assessor (QSA) and a leader in developing security strategies that support the key metrics of your business while addressing various compliance and regulatory mandates.

Arsenal will be providing a web-based portal that will allow merchants to register and complete their PCI compliance requirements in an easy and efficient manner.

Our eCommerce Level 4 merchants will get picked up in the first phase of our programme and will be asked to register their details in to a compliance portal which is an **important** step towards meeting the requirements of PCI.

The web-based portal will allow merchants to;

- Register for the programme
- Identify and fill-out the correct SAQ
- Schedule their quarterly vulnerability scans

Over the last twelve months the majority of data compromises have taken place at smaller eCommerce merchants and these numbers are continuing to increase with alarming regularity. It is therefore imperative that you read what we send you and act accordingly. We plan to have much more information available soon so please keep a look out.

Key dates for your diary!

Card Scheme deadlines are often given well in advance. RBS WorldPay will always try and remind merchants that could be impacted. Reminders will also be added to these newsletters so always keep an eye out.



Effective Immediately

As highlighted in previous editions of this newsletter, Visa and MasterCard have now requested us to provide progress updates against the Prioritised Approach for all level 1-3 merchants within our quarterly Card Scheme reports.

To make reporting easier we have created the **RBS WorldPay Merchant Reporting Tool** which, once completed, will include the details we need minus official documentation such as quarterly external vulnerability scan results.

You can access this tool, full completion instructions and details where to send it by visiting www.rbsworldpay.com/pcidss.

If your business can complete milestones 1-4 of the Prioritised Approach, there is a very strong chance that penalties for non-compliance will no longer be a threat.

If you have any questions about this please visit the website as mentioned above or contact your dedicated PCI Manager or call the main team number on +44 (0) 207 672 6400.

Effective October 2009:

All eCommerce merchants processing one million or fewer Visa txns per annum (Levels 3 & 4) must use PCI DSS certified service provider, or provide certification of own PCI DSS compliance to their acquirer.

Within this there is also a requirement for Payment Service Providers (PSP) to achieve compliance. No deadline currently in place from MasterCard.

Effective 01 July 2010:

Acquirers must ensure that all merchants using payment applications that either store (or cause to be stored) Sensitive Authentication Data post authorisation, must move to applications that do not store.

Effective 31 December 2010:

All Level 1 and 2 merchants must complete an annual onsite assessment conducted by a PCI SSC certified Qualified Security Assessor (QSA). This is a key change to the existing requirement for level 2 merchants. MasterCard strongly encourages that all impacted merchants engage a QSA as soon as possible.



PCI Update Newsletter | September 2009

Useful information refresher

Each month we will try and update this feature as much as possible, adding new information whilst still retaining key details resulting in a list of the most important and useful sites, documents and info currently available on PCI DSS.



Please take a look at the following and bookmark where required. If you have other sites or documents that could be of use to other merchants, please email them in and we can add in future issues:

What is Cardholder Data?

Cardholder Data is the information printed on the physical card as well as the data on the magnetic stripe or chip. Cardholder Data includes;

- Primary Account Number (PAN)
- Cardholder name
- Service Code
- Expiration date

Plus it can also include Sensitive Authentication Data which **MUST NOT** be stored after authorisation even if it has been encrypted!!

- Magnetic Stripe or Track Data
- Magnetic Stripe image on a chip card
- CAV2/CVC2/CVV2/CID
- PIN / PIN Block

Where is Cardholder Data stored?

Cardholder data is stored in both known and unknown locations on most networks and can leak out of known storage locations.

Post-mortem compromise analysis has shown common security weaknesses that are addressed by PCI DSS, but were not in place in the organisations when the compromises occurred. A 2008 report from Verizon Business concluded that some 66% of cases involved data the victim did not know was being stored!!

For PCI storage do's and don'ts' please follow this link;
https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

PCI PED – PIN Entry Device Security Requirements

Here you will find requirements and guidelines, as published by the SSC, about PIN Entry Devices.

https://www.pcisecuritystandards.org/security_standards/ped/index.shtml

Important PCI related updates

We often receive programme amendments or updates from the PCI Security Standards Council (PCI SSC) or Card Schemes (Visa Europe and MasterCard International) and where we think they are of use to our merchants we will try and pass the messages out.

PCI 360 Education Program from MasterCard

The PCI 360 Program is a complimentary initiative offered by MasterCard to raise awareness and promote the adoption of PCI. The program provides a holistic and informative platform for participants to increase their understanding of PCI DSS through the following sessions led by payment industry and data security experts.



There are many very useful webinars and slides available for you to view from the 2009 curriculum, including:

- Cost of an Account Data Compromise (ADC)
- PCI Perspectives - Payment Application Vendor Data Storage
- Wireless Encryption and threat identification

To start your tour please visit -
<http://www.ian.ibeam.com/events/mast001/24008/>

eCommerce Best Practices: A TrustWave webinar

As we edge closer to the busy period of increased Web site traffic and, hopefully, sales – have you checked the security of your site? Are all your certificates, seals and patches up-to-date?

To help you prepare Trustwave is hosting a webinar where three security and compliance experts will walk you through a best practices checklist, offering detailed information and advice to assist you in the pursuit of a secure and trustworthy Web site.



Date: Wednesday, September 16, 2009
Time: 11:00am (BST)
Meeting No: 353 471 266
Password: S4fe&sound
Registration: <https://trustwave.webex.com/trustwave/onstage/g.php?d=353471266&t=a>

PCI Update Newsletter | September 2009

Industry expert slot: **Veritape**



Record calls AND still be PCI DSS compliant

The requirements surrounding PCI DSS, call recording and the impact on your business can appear confusing. In short, if your business takes card payments over the telephone and records calls - **section 3.2** of PCI DSS applies. Sensitive Authentication Data, meaning the security number on the reverse of the card (CVC2/CVV2) and the magnetic stripe data, cannot be recorded in any form, including voice. It is unlikely that your call recording system presently meets these requirements and putting compensating controls in place as a bridge is **not** the solution.

PCI DSS was introduced to protect both customers and businesses from credit card fraud, and this extends to call recording because data within audio recordings is mineable. Audio mining technology exists and people could be used to pull data from call recordings. Many customers and businesses have seen data loss happen and PCI DSS serves to stem this flow.

So, what options exist for businesses? You may be familiar with some suggested solutions to this new challenge:

- **Call encryption:** Sounds secure but it's not compliant because the Sensitive Authentication Data is still stored. Many people still need to listen to the calls (e.g. for training).
- **Obscuring the 16-digit personal account number (PAN):** Voice analytics are used to audio search for the PAN and wipe it from the recording however the CVC still remains, making this approach non-compliant.

A QSA should find neither encryption nor obscuring the PAN acceptable. On a brighter note, compliant solutions are available, some more practical than others:

- Don't record any calls - This works but you would lose the wider benefits of call recording.
- Transfer customer to an automated system - This works but not customer-friendly and could increase abandon rates. Requires significant integration with back-end IT and telephony systems and could still leave you 'in scope' for PCI DSS.
- Record all parts of the call, except the Sensitive Authentication Data which can be automatically 'bleeped out'. This is how **Veritape** works - it either:
 - "Bleeps out" calls by using commands from other applications or websites – or;
 - Watches applications or websites to determine appropriate automatic 'bleep' points

So why don't other call recording systems already do this? Unlike **Veritape**, most systems are hardware based and don't record calls at the agent's desktop. Generally, call recording systems have no associated applications running at the agent desktop meaning they can't easily map information across from payment processing systems. Therefore it is not possible to implement a solution which "bleeps out" Sensitive Authentication Data. Hardware based call recording systems are fundamentally inflexible and not easily adapted. To date, none offer solid PCI DSS compliant solutions.

In summary, call encryption or obscuring the PAN are **not** PCI DSS compliant options. To be fully compliant and still record calls, CVC data has to be excluded. With current technology, we conclude that the only way to achieve this is to use a call recording system based at the Agent desktop level.



Veritape is the leading provider and developer of call recording software. Our low-risk rental model offers a cost-effective, flexible alternative to traditionally expensive fixed hardware solutions. Founded in 2001 by business partners James Heath and Cameron Ross, **Veritape** is a privately owned UK company with offices in Manchester and St Albans. Our customer base covers health, retail, government, motor and financial sectors.

For more information please visit us – www.veritape.com

What to expect in the next edition

- An update from the PCI SSC meeting in Prague
- Industry expert slots will come from **TrustWave** and also the **Dedicated Cheque and Plastic Crime Unit (DCPCU)**

Many thanks for reading this newsletter which I hope you found useful. If you have any comments about its content, or would like to suggest something for the next edition, please send suggestions to the email address provided below.

Thanks and regards,



Phil Atherton

Head of Compliance & Scheme Management
RBS WorldPay
Global Transaction Services

+44 (0)207 672 6400

pcidss@rbs.co.uk

Level 7 | 2½ Devonshire Square | London EC2M 4BA | UK

www.rbsworldpay.com/pcidss

www.pcisecuritystandards.org/

RBS WorldPay and Streamline are trading names of
National Westminster Bank Plc
National Westminster Bank Plc is a member of
The Royal Bank of Scotland Group.
The Royal Bank of Scotland Plc
Registered in Scotland No 90312.
Registered Office: 36 St Andrew Square Edinburgh EH2