Payment Card Industry Data Security Standard (PCI DSS) – What it is and its impact on retail merchants

The Payment Card Industry Data Security Standard aims to reduce fraud by promoting the secure handling of payment card data. **Martin Bradley** and **Alexander Dent** explain the principles behind it, and assess its impact on retailers.

Royal Holloway University of London

SearchSecurity.co.UK

1. WHAT IS IT?

THE Payment Card Industry Data Security Standard (PCI DSS) [PCI06] was introduced to improve the security applied to the protection of payment card data. It applies to all retail merchants, banks, point of sale vendors, or any other organisation that transmits, processes or stores such data. Organisations who fail to comply risk being issued with financial penalties. When a customer makes a purchase in a shop, at a petrol station, in a restaurant, or online with a credit or debit card, they should expect their data to be looked after in a manner which protects them from potential fraudsters. A PCI DSS compliant organisation should be able to demonstrate that they are looking after the customer's credit or debit card data safely.

The PCI DSS is formed of a set of 6 principles with 12 technical and operational requirements for security management, policies and procedures, network architecture, software design and physical security. Figure 1, right, shows these principles and associated requirements.

An organisation is certified as being compliant after undertaking a security assessment against these requirements. The assessment may be carried out by an independent assessor, known as a Qualified Security Assessor

FIGURE 1

PCI DSS PRINCIPLES AND ASSOCIATED REQUIREMENTS

Build & Maintain a Secure Network	• Install & maintain a firewall configuration • Do not use vendor supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• Protect stored cardholder data • Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	• Use & regularly update anti virus software • Develop & maintain secure systems and applications
Implement Strong Access Control Measures	• Restrict access to cardholder data by business need to know • Assign a unique ID to each person with computer access • Restrict physical access to card holder data
Monitor & Test Networks	• Track & monitor access to all network resources • Regularly test security systems and processes
Maintain an Information Security Policy	• Maintain a policy that addresses information security

(QSA)[1], or, in the case of some merchants, compliance may be certified by an internal audit function or Self Assessment Questionnaire (SAQ). PCI DSS categorises merchants into one of four levels; these levels are determined by the volume of card transactions that are processed by a merchant. Each card scheme[2] also keeps its own definition, which is broadly in line with the PCI DSS. A level 1 merchant is a merchant that processes over 6 million card transactions annually. This is the level into which most large retailers will be categorised.

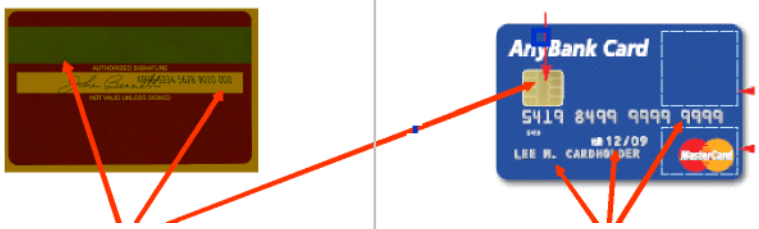
PCI DSS applies wherever the primary account number or PAN is stored, processed or transmitted. Other card holder data, such as the card holder name must also be protected if it is stored in conjunction with the PAN. Certain data, known as "sensitive authentication data," must also be protected. However, special rules apply that do not permit a merchant to store this data post authorisation[3]. The diagram at Figure 2, left, shows this data on a representation of a payment card.

It was back in December 2004 when Visa and MasterCard jointly produced version 1.0 of the PCI DSS. At the time it could have been considered a little forward of these two card schemes to call this a "Payment Card Industry" standard, as only two members of the industry were at that time heavily involved. It was not until September 2006 when American Express, JCB and Discover officially announced their support. The formation of a not-for-profit entity in the form of the PCI Security Standards Council (PCI SSC) at the same time also helped to promote the standard. The Council is responsible for the development, maintenance, storage

FIGURE 2

CARD DATA REQUIRING PROTECTION

Sensitive Authentication Data
Must not be stored under any circumstances



- **Card track data**
- **Card validation data**
- **PIN validation value**
- **Issuer discretionary data**

Sensitive Cardholder Data
May be held subject to business justification

When stored...

- **Must be rendered unreadable**
  Card primary account (PAN), personally identifiable information held in conjunction with the PAN
- **May be held in clear**
  Card transaction amount, transaction date, transaction authorisation code, card issue

and publication of the PCI DSS. The PCI SSC is an example of an entity created through the enactment of the US National Technology Transfer and Advancement Act (P.L. 104-113) whereby the development of voluntary standards from the private sector were actively encouraged. The PCI DSS is enforced through a merchant's contractual relationship with an acquiring bank[4]. Any penalties for non-compliance are issued by the card schemes to the acquiring banks. The bank will then pass any penalty on to the defaulting merchant.

2. WHY DO WE NEED IT?

For many years, organisations have struggled to adequately protect their most sensitive information assets, leading in many cases to breaches of security and the loss or disclosure of sensitive data. There are many widely publicised incidents of high-profile data losses that have occurred across the globe in recent years, and they are still occurring [PRC09]. The 2009 Data Breach Investigations Report [VzB09] found that of the 90 confirmed breaches that they investigated in 2008, 285 million records were compromised and that 80% of these records involved payment card data. The report also stated that fraudulent use of this payment card data occurred in 83% of these cases.

A statement from Andrew R Cochran, founder and co-editor of the "Counter Terrorism" blog, for the "Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing U.S. House Committee on Homeland Security" on March 31st 2009, claimed that the "terrorists who executed the devastating 2004 Madrid train bombings, which killed almost 200 people, and who carried out the deadly July 7, 2005, attacks on the transportation system in London were self-financed, in part through credit card fraud" [AC09].

There is currently no Government-backed legislation that forces organisations that transmit, process or store cardholder data to safeguard it in an appropriate manner. Despite innovations such as Chip and PIN, that has been introduced across Europe in an attempt to combat card fraud, the criminals are still able to compromise computer systems where the data is stored and use it to commit fraud in areas where such controls do not exist.

It was around the years 2000 to 2001 when notable losses were being reported. These include the JK publications case of 2000 [FTC00] whereby access to a bank's credit card trans-

action records were obtained and used to commit fraud totalling several million dollars. These incidents led to the card schemes introducing their own security standards and adding statements into merchant terms and conditions relating to security of cardholder data. These standards are still in force and each card scheme uses these to assist merchants in attaining PCI DSS compliance. Figure 3, below, shows the respective schemes that underpin the PCI DSS for the major global card schemes.

Of course, there are still numerous breaches that have occurred since these standards and PCI DSS were introduced, including perhaps one of the most widely publicised cases – the TJX breach of 2007.

3. IS PCI DSS EFFECTIVE?

Since its introduction, the PCI DSS has certainly raised the profile of payment card data breaches and the fraud that occurs as a result. It has also been effective as a means to encourage organisations such as retail merchants, who traditionally have not always been so heavily regulated, to put in place formal plans to address the security of cardholder data. Whether the PCI DSS has had a positive effect on reducing instances of data breaches and card fraud is a more difficult question to answer at this stage. There is no doubting the obvious benefits of a good information security management system. However, managing risk is at the heart of any security strategy and risk

FIGURE 3

MAJOR CARD SCHEMES SECURITY PROGRAMS

PCI DSS					
Visa International	**Visa Europe**	**MasterCard**	**American Express**	**JCB**	**Discover**
Card Information Security Program (CISP)	Account Information Security (AIS)	Site Data Protection (SDP)	Data Security Operating Policy (DSOP)	Data Security Program	Discover Information & Compliance Program (DICP)

assessment is noticeable by its apparent absence as a process within the PCI DSS. This does not mean that there are not obvious risks to cardholder data; however, PCI DSS does not require that individual organisations carry out risk assessments. A risk assessment, if carried out correctly, will identify where cardholder data may be at risk. The assessment should consider existing vulnerabilities that could lead to a data breach and should identify the effectiveness of existing controls. This may lead to recommendations of further appropriate controls to mitigate that risk to a level that can be accepted by the organisation. These controls may or may not necessarily be the same controls specified in the PCI DSS, but should have the equivalent properties to reduce risk.

Even though the PCI DSS has been in force for 5 years, it has been difficult to find material indicating that PCI DSS has reduced incidents of data breaches or credit card fraud. Indeed, the Verizon 2009 Data Breach Investigation Report [VZB09] states that the number of financial records breached in 2008 exceeded the combined total from 2004 to 2007.High profile merchant breaches reported since the introduction of PCI DSS, such as the Hannaford breach [DK08] and the Network Solutions breach [LM09], suggest that there is a lack of strong evidence that PCI DSS has had a material impact on reducing data breaches (although it has been stated that the Hannaford organisation was not PCI compliant at the time of the breach).

A number of working groups that focus on security have been established to allow like-minded organisations to get together and discuss PCI DSS related issues.

Despite this lack of effective evidence, there are strong indications that merchants have taken the requirements of the PCI DSS seriously. A number of working groups that focus on security have been established to allow like-minded organisations to get together and discuss PCI DSS related issues. Established bodies such as the British Retail Consortium (BRC), the Information Security Forum (ISF) and the Corporate IT Forum (tif) include workshops to discuss PCI DSS issues for members. Other working groups such as the PCI DSS UK Merchants Working Groups have been formed by retail merchants

to allow organisations to get together and discuss the standard, its implications and to share strategies. Furthermore, there are countless educational seminars, workshops and vendor presentations targeted at affected organisations.

The payment card industry, led by Visa and MasterCard, should be praised for actively doing something about the security of cardholder data by introducing PCI DSS.

In this respect, the PCI DSS would seem to have been very effective, and, as stated by Yvette D Clarke, chairwoman of the subcommittee on emerging threats, cyber security, and science and technology committee on Homeland Security in the US, "in the absence of other requirements they do serve some purpose" [YC09]. Kristen Lovejoy, Director of IBM Corporate Security, stated at the VISA security summit 2009, "PCI DSS has had the single greatest impact on the industry" [KL09].

However, the continued breaches suggest that PCI DSS compliance alone is not enough to combat data breaches and fraud. Ellen Richey, Chief Enterprise Risk Officer at Visa, recognised the limitations of PCI DSS, stating that "the standards provide a strong foundation and the best security strategies build on that foundation into a multi layered approach that evolves the defence over time" [ER09].

4. IMPACT ON UK MERCHANTS

The payment card industry, led by Visa and MasterCard, should be praised for actively doing something about the security of cardholder data by introducing PCI DSS. However, many merchants would come to realise high costs, lengthy IT programs and discover difficulties in interpreting the standard (see section 5). Supporting the view that there were early issues is a Gartner paper titled, "How to improve the ailing PCI program" [ALPJ06]. The main points raised in this document are:

- The process is manual and fraught with poor communications
- The card schemes have not established suitable compensating controls[5]
- The Self-Assessment Questionnaire (SAQ)

does not allow for compensating controls
- The effects of outsourcing are unclear
- The standard is too broad in scope, too detailed in some areas and not enough in others

Of the merchants surveyed (including many of the top 10 UK retailers by sales as listed in the Mintel Oxygen list of top 250 European retailers), 100% have a PCI compliance programme in place, and 92% felt that the standard was providing benefit.

During 2009 we conducted our own survey of a number of UK merchants in order to gain anonymous feedback on PCI DSS. Of the merchants surveyed (including many of the top 10 UK retailers by sales as listed in the Mintel Oxygen list of top 250 European retailers), 100% have a PCI compliance programme in place, and 92% felt that the standard was providing benefit.

Section 5 describes a sample of the results obtained.

5. MERCHANT SURVEY

In order to gain some insight into how PCI DSS had affected some of the largest UK retailers, we asked a selection of retailers to complete a written questionnaire on their PCI DSS compliance programme. The questionnaire sought to identify how the introduction of the PCI DSS had affected each organisation, and obtain views and feedback on their interpretation and understanding of the standard, its value, and to establish projected costs and timescales. At the time of survey, all merchants surveyed were level 1 merchants and all had a compliance programme in place. None had been through a compliance assessment at that time. Of the merchants surveyed, 12 responded, which as mentioned earlier includes many of the top 10 UK retailers by sales. A summary of the responses is presented in this section.

5.1 DRIVERS

The major drivers for merchants to comply with PCI DSS were identified as “brand protection” and to “secure customer data”. Of the

HOME
WHAT IS PCI DSS?
WHY WE NEED IT?
IS IT EFFECTIVE?
ITS IMPACT ON MERCHANTS
SURVEY OF UK MERCHANTS
FOOTNOTES & BIBLIOGRAPHY

choices given, these reasons were scored high by a significant majority of merchants. These two factors are intrinsically linked, in that a breach of security for customer data would lead to a loss of brand reputation that could ultimately drive customers away from a particular merchant. It is also an indicator that merchants do seem to take the security of customer data seriously. The other driver that scored highly for some was "penalty avoidance", suggesting that this is also a way to motivate organisations to comply.

5.2 UNDERSTANDING OF THE STANDARD AND GENERAL VIEWS

A number of questions were asked looking for each merchant's understanding or interpretation of the PCI DSS.

- 83% of merchants surveyed felt that the standard was not issued in an appropriate

FIGURE 4

TABLE SHOWING UK MERCHANTS PREDICTED PCI DSS PROGRAMME LENGTH AND COSTS

Merchant	PCI DSS Programme Start date	Predicted Length of Programme (years)	Predicted Cost (millions of £)
1	Quarter 2 2005	5.25	1 - 2
2	Quarter 1 2006	4.25	5 - 10
3	Quarter 1 2006	4.25	5 - 10
4	Quarter 1 2006	4.75	5 - 10
5	Quarter 2 2006	5.5	5 - 10
6	Quarter 2 2006	6	10+
7	Quarter 3 2006	5.5	10+
8	Quarter 1 2007	3.5	5 - 10
9	Quarter 1 2007	4	5 - 10
10	Quarter 2 2007	2.5	2 - 5
11	Quarter 3 2007	3	2 - 5
12	Quarter 4 2007	3.5	5 - 10

manner and without a good explanation of the requirements. This may be a reflection on the period in and around 2005 when the standard was becoming widely distributed to merchants, but with little warning or explanation of its importance and where to find help.

- 67% of merchants surveyed agreed that the standard seemed more appropriate to online merchants than to traditional bricks and mortar retailers. On reading the standard, it appears in places to be more relevant to, and achievable by, online-only merchants[6]. The complex issues on how an established national retailer should be expected to comply with the requirements throughout numerous (hundreds of) locations does not seem to be appropriately considered. For example, requirement 5 in the standard requires the use of regularly updated anti-virus software. This applies to all point of sale devices (tills). There are huge complexities for retailers in managing and supporting thousands of these devices to which even the smallest of changes can have a dramatic effect on the operation of such a device. For an online-only retailer, there is no concept of a physical till. However, as merchants have become more aware of how to interpret the standard, issues such as this have been addressed on an individual basis.
- 83% of merchants surveyed agreed that the later versions of the standard (Version 1.1 and 1.2) improved the quality and relevance to traditional bricks and mortar retailers. This appears to support the view that the earlier version was more focussed towards online-only merchants and that change was required.
- Only 33% of merchants surveyed claimed to be clear on what was needed to achieve compliance. Having such a small number of respondents declare that they are clear on what they were required to achieve indicates the PCI DSS is complex and that it is not easy to translate the requirements into solutions. It is perhaps the diversity of retail IT solutions that contributes to this complexity. This will likely make it more difficult for a QSA to assess a merchant's compliance and for a merchant to understand a QSA's requirement.
- 100% of the merchants surveyed reported that it was not easy to obtain good quality and consistent information from the card schemes, acquiring banks or their QSA. Inconsistent or incorrect information can only serve to frustrate an organisation and is likely to lead to inappropriate and delayed solutions being deployed. It is important that organisations

can have confidence in information that is provided to them if they are to embrace the standard and work efficiently. The PCI SSC have introduced more rigour into the process for certifying a QSA and have welcomed feedback from merchants on these matters.

92% of merchants surveyed believed that there should be no charge for membership as a participating organisation of the PCI SSC.

- 92% of merchants surveyed believed that there should be no charge for membership as a participating organisation of the PCI SSC. The annual fee of $2500 is seen as a deterrent to merchants. This indicates that merchants do not see a material business benefit in becoming a participating organisation. Greater inclusion of merchants could lead to wider acceptance and better understanding, and is perhaps an area that should be addressed by the PCI SSC ensuring that merchants are aware of the benefits.
- 92% of merchants surveyed agreed that the standard was overall a good idea. Almost all merchants agree that the PCI DSS exists to improve the security of cardholder data. This is another strong indication that merchants do realise the importance of keeping this data secure and welcome the guidance.

5.3 VIEWS ON SECURITY

Each merchant was asked questions seeking their views on security and how it may have been affected by the introduction of the PCI DSS.

- 92% of merchants agreed that the security of cardholder data within their organisation had improved since the introduction of the PCI DSS. This declaration indicates that despite none of the merchants having been certified as compliant, they are actively looking to implement improved controls.
- 75% of merchants felt that the PCI DSS would not be necessary if more organisations applied security more effectively in the past. Although all merchants were aware of good standards such as ISO/IEC 27001, the contractual obligations and financial penalties are effective differentiators for PCI DSS. It does not necessarily mean however that PCI DSS is a better standard.
- 83% of merchants surveyed have used the

HOME
WHAT IS PCI DSS?
WHY WE NEED IT?
IS IT EFFECTIVE?
ITS IMPACT ON MERCHANTS
SURVEY OF UK MERCHANTS
FOOTNOTES & BIBLIOGRAPHY

PCI DSS to drive greater security within the organisation and to improve the security applied to other sensitive data. The high percentage of merchants who have achieved this demonstrates how the PCI DSS has had a positive impact on security stretching further than just cardholder data.

5.4 COSTS AND TIMESCALES

Each merchant surveyed was asked to give projections for when they believed they would have completed their PCI programme and be in a position to undergo assessment for compliance. Each merchant was also asked to give an indication of predicted cost for the programme. The table at figure 4 below shows the data gathered from the UK merchants surveyed starting with the earliest starting date.

There is an interesting trend that appears which shows that the merchants who began their programmes earlier are generally predicting a longer timescale. The average length of time predicted for organisations that began their programme prior to 2007 is over 5 years. The average time scale predicted by merchants who began their programme from 2007 is just over 3 years. UK Merchants who began their programme earlier have perhaps discovered that the task is greater than predicted when they began and have revised their plans accordingly. Alternatively, the improved resources and expertise now available is assisting merchants in achieving compliance more expediently

There is general recognition that costs to achieve PCI DSS compliance will exceed £5 million. This compares to a Gartner report undertaken in the US in March 2008 [AL08] that reported an average spend of $2.7 million for the level 1 merchants (which had increased from an average of $0.5 million in 2006).

6. REDUCING THE SCOPE OF PCI DSS

The high costs that will be incurred by many of the larger merchants to achieve compliance are partly related to the size and complexity of their existing environments. Stores networks have been identified as one area where significant cost is incurred to achieve PCI DSS compliance. Since the original thesis was written, some UK merchants are considering solutions that could reduce the scope of their compliance programme. One such initiative is based on the strong encryption of cardholder data

supported by good key management. The intention being to reduce the scope of the cardholder data environment. Further work is ongoing to develop this concept for proposal to the PCI SSC. Visa, have already released guidelines to assist merchants who wish to use encryption as part of their solution [VISA09].

7. FINAL THOUGHTS

The value of cardholder data is the reason that it is sought after information for fraudsters. The numerous breaches that are still being discovered are an indication that payment card data still holds a high value for criminals. Initiatives such as PCI DSS are vital in order to try and reduce the number of successful attacks. Other solutions that aim to reduce the value of the data that is held outside highly secure environments should continue to be investigated. Stronger authentication of the rightful user of a payment card is also required to enable a customer to use their card safely in all situations, including, in person, online and over the telephone. There are already several initiatives that have been introduced or are being investigated, including Chip and PIN [UKP09], 3D Secure [NC09] and even dynamic PAN solutions [IMJLNL07]. These initiatives and others are a topic for discussion outside the scope of this document. ■

ABOUT THE AUTHORS

Martin Bradley has worked in information security for 18 years and is currently security assurance and compliance manager at Marks and Spencer, where he is responsible for the technical solutions required to deliver the compliance PCI DSS compliance initiatives.

Alexander W. Dent is a lecturer in Information Security at RHUL. His research interests are primarily on the theory of provable security in public-key encryption schemes.

FOOTNOTES

[1] A QSA is an individual who has been certified to provide consultancy and guidance on PCI DSS in an official and authoritative capacity. The individual may also conduct PCI assessments on an organization to determine their compliance. The individual must work for a company that has also been authorized by the PCI SSC to provide these services

[2] A card scheme is an organisation that controls the operation of credit card transactions, e.g. Visa, MasterCard, American Express. Card schemes set the business rules that govern the issue of the payment cards that carry their logo

[3] Authorisation is the process performed by a bank which verifies that the customer's credit or debit card account is valid and that sufficient funds are available to cover the transaction's cost transaction.

[4] An acquiring bank is a bank having a business relationship with merchants, retailers and other service providers to process their plastic card transactions.

[5] A Compensating Control may be used where an organisation seeking compliance with PCI DSS cannot meet a specific control requirement. An alternative control may be selected if approved by a QSA.

[6] An online-only merchant is viewed as a merchant that runs an e-commerce Web site for selling goods only, and does not trade from bricks and mortar retail stores. Most major retailers now run an online store as well as the traditional high street or retail park shops.

[7] The stores network is the term used to describe the IT networks in retail shops. These networks consist of wired and wireless networks and the devices such as tills, PCs and servers that are connected to them. The stores network usually has connectivity back to retailers head office network.

BIBLIOGRAPHY

[AC09] Prepared statement Andrew R Cochran
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Committee on Homeland Security. March 31, 2009 hearing: "Do the payment card industry data standards reduce cybercrime?"

[ALJP06] Avivah Litan and John Pescatore of Gartner Research How to Improve the Ailing PCI Program. 17th February 2006.

[AL08] Avivah Litan of Gartner Research PCI. Compliance remains challenging and expensive, page 7 16th May 2008

[DK08] Dan Kaplan,. Article published in *Secure Computing* magazine reporting on the credit card data breach at the PCI compliant Hannafords, a US supermarket chain. March 18th 2008
http://www.scmagazineus.com/Experts-try-to-make-sense-of-Hannaford-data-breach/article/108134/

[ER09] Ellen Richey Chief Enterprise Risk Officer at Visa, March 2009. Presentation at the Visa Global Security Summit 2009
http://www.visasecuritysummit.com/popupVideo.html

[FTC00] Court Case of the Federal Trade Commission case against JK Publications in August 2000.
http://www.ftc.gov/os/2000/09/jkpublicationfindingsoffact.pdf]

[IMJLNL07] Ian Molloy, Jiangto Li, Ninghui Li, Dynamic Virtual Credit Card Numbers – February 2007
http://www.cs.purdue.edu/homes/imolloy/slides/FC07.pdf

[KL09] Kristen Lovejoy, director, IBM Corporate Security. Presentation at the Visa Global Security Summit 2009
http://www.visasecuritysummit.com/popupVideo.html

[LM09] Linda McGlasson Network Solutions Breach Revives PCI Debate August 10th 2009.
http://www.bankinfosecurity.com/articles.php?art_id=1691

[NC09] Nochex reference for 3D Secure
http://www.nochex.com/merchant-account/security-fraud/3d-secure.html

[PCI06] PCI Standards Security Council
https://www.pcisecuritystandards.org/

[PRC09] 2009 Privacy Rights Clearing House – Chronology of Data Breaches
http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

[UKP09] UK Payments Chip and PIN description of service
http://www.ukpayments.org.uk/payment_options/plastic_cards/card_industry_initiatives/chip_and_pin/-/page/248/

[VISA09] Visa best practices July 2009. Data Field Encryption Version 1.0
http://corporate.visa.com/_media/best-practices.pdf

[VISA09a] PCI DSS qualifying merchant levels published and maintained by Visa
http://usa.visa.com/merchants/risk_management/cisp_merchants.html

[VzB09] 2009 Data Breach Investigations Report. A study conducted by the Verizon Business Risk Team.
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

[YC09] Prepared statement chairwoman Yvette D. Clarke (D-NY)
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Committee on Homeland Security. March 31, 2009 hearing: "Do the payment card industry data standards reduce cybercrime?"