PCI DSS Compliance
More Important Than Ever

The drivers for compliance

Matt Ball
January 2018
Introduction

At some point in the PCI DSS process someone will ask the question or a variation of the question:

- Why bother becoming compliant?
- Why does the organisation need to become compliant?
- What happens if we don’t become compliant?

From the perspective of the person asking the question they don’t see the potential card compromise, the potential fines, what they see is the here and now, the risks that may never materialise, the compromises that may ever happen.

While prevention and contingency planning is essential for any business, the uncertainty of a breach ever occurring and impact it will have, may not be sufficient to not justify the investment, time and system upheaval that implementing and maintaining PCI DSS compliance can bring. The person asking the question needs the “it will” or “it won’t” or as close as black & white that PCI DSS can achieve.

This document has been written from the merchant’s perspective to address the questions and provide the core business reasons for the organisation to achieve and maintain PCI DSS compliance.
What is PCI DSS?

PCI DSS: Payment Card Industry Data Security Standard is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data.

Card companies have been continually trying to reduce the millions of pounds lost globally through fraud, which the card companies, merchants and ultimately the consumer pay for. The majority of card fraud can be traced back to the data thief exploiting flaws within merchant's security or weak business practices. If the merchant could identify those potential security flaws, change their business practices before they are exploited, then in theory losses could be reduced significantly.

PCI DSS – the Payment Card Industry Data Security Standard was born out of five different programs: Visa Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program. Each program's intention was to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data – effectively plugging those aforementioned exploitable holes.

The Payment Card Industry Security Standards Council (PCI SSC) was formed, and in December 2006 when the councils founding payment brands, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. aligned their individual policies and released version 1.0 of the Payment Card Industry Data Security Standard (PCI DSS). Version 2.0, the current version, was released in October 2010.

PCI DSS is now a mandatory standard that the card companies expect merchants to achieve and then maintain, regardless of their size and complexity.

The Risk

Every transaction made has a risk attached to it. For the consumer the risk is his/her card holder data being compromised combined with the problems, heartache and potential upset that this would bring. For the merchant, the processing of card holder data makes them an attractive target for the data thief – the more transactions the merchant processes, the more worthwhile the target becomes.

The Primary Account Number (PAN) and the authentication data stored on the card or chip is the prize for the fraudster. Once stolen, those details would be sold on and it could be maybe days, weeks or months before they are used for card-not-present frauds or other activities. UK fraud during 2016 was £432.3 million in card-not-present frauds, up 9% on 2015, and has almost doubled from the £220.9 million that was quoted in the first version of this document published in 2013.

However, risk goes beyond the stolen cards. Unlike the consumer where he or she would be compensated for any losses by the card schemes, the merchant can and has incurred heavy financial losses through fines, forensic investigation costs, costs associated with implementation of remediation actions and quite often reputational damage from public disclosure of the losses.

It is the risk of card holder data loss from the merchant's card processing activities that PCI DSS intends to address.
Who requires compliance?

Ultimately it is the five card brands; Visa, MasterCard, JCB, Discover, American Express, who require merchant to become PCI DSS Compliance.

However it is the acquiring bank providing the card services to the merchant who will monitor and push for the merchant to become and then maintain compliance.

Acquiring banks will report to the five card brands the number of merchants who are and aren’t PCI DSS compliant, that they provide services for.

What happens if we aren’t compliant?

Stepping into the real world, when a merchant is faced with a shrinking market share, decreasing sales, increasing overheads and reducing profits (in worst case loss) the reasons for achieving and maintaining PCI DSS compliance need to be tangibly justified.

So what happens if a merchant isn’t PCI DSS compliant?

- **Contractual Obligation**

  PCI DSS is a contractual obligation and is not a legal requirement. PCI DSS compliance will appear as a contractual requirement as part of using the acquiring bank’s card services.

  When a merchant fails to comply with PCI DSS, it could be considered a breach of contract on behalf of the merchant, by the acquiring bank resulting in fines and penalties levied against the merchant for the duration of non-compliance.

  There may be a period of grace where the acquiring bank may allow the merchant to work towards compliance without incurring any fines, especially if the merchant is a new or high profile client, however at some point action will be taken. But at some point the merchant must demonstrate compliance.

  The following highlighted contractual clauses extracted from a Global Pay contract with a UK University illustrate the contractual obligation and the potential penalties that can be incurred for non-compliance.
Whereas the PCI DSS standard has been developed by the five brands, it should not be forgotten that the card brands are still competing organisations with their own distinct corporate objectives.

Each card brand will have its own program for ensuring the merchants achieve compliance with their own internal fine structure. For the merchant there is currently no published set guidelines for the scale of fines or penalties that maybe issued by the card brands for non-compliance.

The card brands have what is referred to as a “discretionary” fine that can be levied on an acquirer for having non-compliant merchants. The agreement between the acquirer and the merchant typically states that the acquirer will pass on any incurred fines or fees to the merchant.
For non-compliance the resulting fine the merchant incurs from the acquirer may be determined by the size of the business and the volumes of the card processed. The value of the merchant as a good client and or the risk the merchant’s non-compliance poses to the acquirer would also be influential.

**Example of types penalties and fines**

*Source Barclaycard website (2014 publication, expect fines to have increased significantly)*

<table>
<thead>
<tr>
<th>Cost Type</th>
<th>MasterCard</th>
<th>Visa</th>
</tr>
</thead>
</table>
| **PCI DSS Non Compliance** |  • Level 1 category per merchant: up to $25k  
  • Level 2 category per merchant: up to $10k  
  • Level 3 category per merchant: up to $5k  
  Limited at Acquirer level to $500k in aggregate in a 12 month period |  Visa have a tiered fine structure based on notification to the member:  
  • Confirmation of compliance status not received within 30 days of notification €5,250  
  • Confirmation of compliance status not received within 90 days of notification €10,500  
  • Confirmation of compliance status not received within 120 days of notification €26,250 + €26,250 for every additional 30 days (If the total amount exceeds €250k in a 12 month period this could be referred to Visa Europe Board)  
  • Finally Visa could choose to revoke the Merchants license. |
| **Compromise Fines**  | Issuer reimbursements  
  • $25 for each account reissued  
  • $5 for each account monitored but not reissued  
  Severity of fine will depend upon Acquirer / Merchant progress, co-operation, number of accounts at risk, what sensitive data has been stored i.e. CSC, Track 2  
  Failure by Acquirer to comply with ‘Acquirer Responsibilities’ defined in the Rules can incur a further $25k per day until compliant.  
  The assessments for Wrongful Disclosure and Failure to Secure Data are up to USD 100,000 per violation.  
  The assessments for Retention of Prohibited Data (mag stripe, CVC 2) are up to USD 100,000 per violation. |  • Tiered structure depending on merchant level (see below). |
PCI DSS Compliance – More Important Than Ever

For both Schemes, Acquirers can be liable for all fraudulent spend following a data compromise; this is dependent upon the Issuers making a compliance case to the scheme.

<table>
<thead>
<tr>
<th>Compromised Entity</th>
<th>Initial Penalty (€)</th>
<th>Insufficient remediation after 90 days (note 1)</th>
<th>Monthly PCI DSS Violation (after 4 months)</th>
<th>Monthly PCI DSS Violation (after 5 months)</th>
<th>Monthly PCI DSS Violation (subsequent months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>€50,000</td>
<td>€30,000</td>
<td>€50,000</td>
<td>€75,000</td>
<td>€75,000</td>
</tr>
<tr>
<td>Level 2</td>
<td>€25,000</td>
<td>€15,000</td>
<td>€25,000</td>
<td>€50,000</td>
<td>€50,000</td>
</tr>
<tr>
<td>Level 3</td>
<td>€10,000</td>
<td>€5,000</td>
<td>€10,000</td>
<td>€15,000</td>
<td>€15,000</td>
</tr>
<tr>
<td>Level 4</td>
<td>€10,000</td>
<td>€5,000</td>
<td>€10,000</td>
<td>€15,000</td>
<td>€15,000</td>
</tr>
<tr>
<td>VisaNet processors/ Member Processors</td>
<td>€50,000</td>
<td>€30,000</td>
<td>€50,000</td>
<td>€75,000</td>
<td>€75,000</td>
</tr>
<tr>
<td>Merchant Processor</td>
<td>€25,000</td>
<td>€15,000</td>
<td>€25,000</td>
<td>€30,000</td>
<td>€30,000</td>
</tr>
<tr>
<td>Other</td>
<td>€10,000</td>
<td>€5,000</td>
<td>€10,000</td>
<td>€25,000</td>
<td>€25,000</td>
</tr>
</tbody>
</table>

Note 1: sufficient remediation would be satisfied through demonstration that the following PCI DSS requirements have been implemented:

1) Remove sensitive authentication data and limit data retention
2) Protect the perimeter, internal and wireless networks
3) Secure applications
4) Protect through monitoring and access controls
5) Removal of CVV2 data must be achieved within 30 days. The non-remediation penalty will apply after 30 calendar days if removal of CVV2 (or other authentication data) and cessation of storage have not been effected by card-absent merchants and merchant service providers. Subsequent fees will be applied after each 30 calendar day period until removal and cessation of storage has been confirmed in writing to the Visa Europe Compliance Department.

The merchant may also incur hidden costs of non-compliance such as increased transaction fees. Different charges apply depending on a wide range of factors, including an assessment of a merchant’s exposure to card fraud. For even a large level 1 merchant, even an increase of 0.01% could make a noticeable dent in your bottom line.

In addition, a significant card data breach may attract fines from the Information Commissioners Office under GDPR.
Withdrawal of service

Ultimately a merchant's non-compliance or a refusal to become non-compliant, can lead to the card processing services being revoked as a last resort. This would be crippling to the merchant and is not in the commercial interest of the card brands.

Referring to the clause 14.6 in the example contract extract in the section Contractual Obligation, the suspension of card processing services by immediate effect is a clearly defined possibility for not achieving compliance.

However the reality of suspending card processes can happen in extreme circumstances as is illustrated by the events in Vatican City in 2013.

Italy bans card payments in Vatican over money laundering

Italian authorities have stopped all electronic payments inside the Vatican City after the Bank of Italy complained that it had failed to bring in new procedures to prevent money laundering.

The Bank of Italy suspended all bank card payments on Vatican territory from the start of the year and ordered Deutsche Bank Italia, which manages electronic payments for the world’s smallest country, to turn off its systems.

Italian newspapers reported that the action was taken after officials at the Italian central bank became worried that the Vatican was not prepared to implement new anti-money laundering rules.

The suspension of card services means that the Vatican museum, along with the territory’s pharmacy and post office, have all been unable to transfer money and accept payments.

A spokesman for the Vatican told the Italian press the state hoped to find a non-Italian bank to provide it with access to payment services “quite soon” and that the problem would be
“short-lived”. The Vatican has not commented directly on the Bank of Italy’s concerns.

*Five million tourists visited the Vatican last year and spent €91.3m (£74m). However, until its payment systems are restored the Vatican said that all transactions, including buying tickets for its world famous museum, would have to be done in cash.*

*Source Telegraph Online - 2013*

- **Risk**

Fraud & theft is one of the unpleasant realities of commerce, it will not go away and as such there will always be a need for PCI DSS or similar programmes to deal with the issues. As figures from Financial Fraud Action UK illustrate the potential incomes that can be generated from card fraud make it a financial viable criminal activity.

Breach of contract, fines and loss of the ability to process cards are the core drivers for encouraging the merchant to become compliant with PCI DSS.

- Can a merchant who isn’t engaging with PCI DSS truly have confidence in the security their customer’s card hold data, when it is being used or received by their organisation?

### Plastic card fraud: £618 million (2016)

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>Total Estimated Fraud Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Not Present</td>
<td>£432.3 million</td>
</tr>
<tr>
<td>Counterfeit Card</td>
<td>£36.9 million</td>
</tr>
<tr>
<td>Lost or Stolen Cards</td>
<td>£96.3 million</td>
</tr>
<tr>
<td>Card ID Theft</td>
<td>£40.0 million</td>
</tr>
<tr>
<td>Card non-receipt</td>
<td>£12.5 million</td>
</tr>
</tbody>
</table>

“Plastic card fraud encompasses ‘cardholder not present fraud’ (the theft of genuine card details that are then used to make a purchase over the internet, by phone, or by mail order), ‘counterfeit card fraud’ (a fake card using compromised details from the magnetic stripe of a genuine card), ‘lost and stolen cards’ and ‘card ID theft’ fraud.

The latest figures published by Financial Fraud Action UK indicate that total fraud losses on UK cards have increased to £618 million during 2016; a 9% increase compared with losses in 2015.

*Source: Financial Fraud Action UK*
PCI and GDPR

Both PCI DSS and GDPR aim to ensure organisations secure personal data. The PCI DSS focuses on payment card and cardholder data, while the GDPR focuses on European residents’ personal data. Cardholder data is a subset of the overall personal data GDPR protects.

GDPR is less prescriptive than the PCI DSS. GDPR provides guidance on what needs protecting but does not provide an approach. Conversely, the PCI DSS details clearly what needs to be achieved and provides a clear methodology for securing cardholder data.

In the context of card holder data, PCI DSS can be used to directly support GDPR across a number of its 99 articles. An example of this can be seen in Article 5.

Article 5 Principles relating to processing of personal data

1. (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

For card holder data, PCI DSS when implemented will directly meet section 1.f of the requirement.

Final thoughts

The intention of PCI DSS is to reduce the opportunity of fraud through the introduction of a standard best practice towards securing and managing card holder data within the merchant’s organisation.

PCI DSS is both a standard and contractual obligation the merchant must comply with if they wish to continue to take payment via credit/debit cards. In addition PCI DSS the standard when implemented can contribute directly to an organisations GDPR obligations for card holder data.

Rather than trying to avoid PCI DSS the merchant should be embracing it as an opportunity to improve security, reduce the threat of fraud and re-evaluate elements of their business with a view to reducing costs and providing a better service to the card holder customer.

Once compliance is achieved it has to be maintained, whereas the reporting of compliance is annually. So for those who think they are secure just because the organisation has submitted a report on compliance; then think again, it takes diligence, continuous execution and monitoring of the controls of the organisation’s processes, people and supporting technologies.

References


5. https://www.eugdpr.org/

6. Barclaycard 2014 publication