worldpay

Payment Security Report

2015

Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a set of standards designed to keep credit and debit card payment data safe and secure. It was created by the five major international card schemes – American Express, JCB, MasterCard, Visa and Discover – to combat the problem of card data theft and fraud.

PCI DSS compliance is the minimum level of card data security for any business that accepts credit and debit cards, regardless of size, and any organisation which stores, processes and/or sends card data. The 12 core steps of PCI DSS are designed to keep an organisation safe from most types of attack.

Compliant organisations demonstrate good behaviour and a commitment to payment security.

Failure to secure payment systems can be a costly mistake either in lost custom, bad publicity and industry penalties, or in being left out of pocket when customers purchase goods and services using stolen card details. In March 2015, Worldpay saw over 133,000 fraudulent transactions reported, which translates to stolen card details being used every 20 seconds.

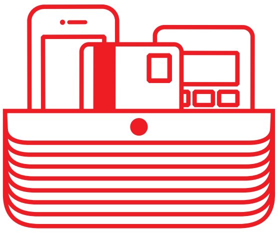
Worldpay helps to protect its customer's systems from compromise, aiming to secure businesses by getting them to comply with PCI DSS. However, there is no such thing as a fully secure payment system. If attackers are determined enough, they will succeed - and when they do, we are here to help.

Although there are a number of reports on card data security released every year, this study is different. It focuses only on UK businesses that have had a card data breach during 2011-2014. The data has been derived from Qualified Security Assessor reports and card scheme data for Worldpay's UK customers.

British businesses should read this report to assess their vulnerabilities, and learn from those organisations which were unfortunate enough to suffer a card data breach.

Worldpay is the leading payments provider in the UK and Europe. In 2014, Worldpay processed 44% of all UK card transactions*

TIMOTHY LANSDALE
Head of Payment Security, Worldpay



*Based on market data provided by the UK Payments Administration.

PCI DSS requirements

PCI DSS helps protect sensitive consumer card data through imposing industry standards surrounding the storage, transmission and processing by businesses, of card data.

There are 12 high level requirements, which fall into the following categories:

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect card data

3. Protect stored data (use encryption)
4. Encrypt transmission of card data and sensitive information across public networks

Maintain a vulnerability management programme

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement strong access control measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to card data

Regularly monitor and test networks

10. Track and monitor all access to network resources and card data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Understanding a business' PCI Level:

Different standards need to be met depending on the number of card transactions a business accepts. The following levels apply:

1 **PCI Level 1:** 6m+ transactions per year per card scheme

2 **PCI Level 2:** 1m-6m transactions per year per card scheme

3 **PCI Level 3:** 20,000 – 1 million online transactions per year per card scheme

4 **PCI Level 4:** Less than 20,000 transactions per year, per card scheme

PCI DSS compliance trends

Over the last four years, PCI DSS compliance in the UK has improved, but the rate of attacks and subsequent card data breaches has varied according to the size (PCI DSS level) of the business.

1 **PCI Level 1:** 6m+ transactions per year per card scheme

In the **Level 1** space, where large corporate businesses lie, Worldpay has seen a

179%

increase in the number of customers achieving PCI DSS compliance.

As a result of their increased efforts in maintaining PCI DSS compliance, there have been minimal attacks on large corporate businesses in the UK.

2 **PCI Level 2:** 1m-6m transactions per year per card scheme

In the **Level 2** space, Worldpay has seen a

29.4%

increase in the number of customers achieving PCI DSS compliance.

It is difficult to explain exactly why the Level 2 space has seen a relatively small increase over the four year period. A contributing factor for many is that the original scope of their PCI DSS audit was incorrectly limited, and as such it will take time for these businesses to reassess themselves and reach the same level of compliance again.

Over the last four years, alongside a small increase in PCI DSS compliance, Worldpay has also seen a small increase in card data breaches among Level 2 organisations.

Whilst the increase in attacks, and subsequent card data breaches, is an issue for Level 2 organisations, it has raised awareness of the importance of PCI DSS, and encouraged these businesses to become more secure as a result.

Regardless of business size, it is important businesses continually challenge their own PCI DSS compliance, and where vulnerabilities are discovered, this should be recognised as a good thing, as they can be resolved.

Figures are based on card data breaches which occurred for Worldpay UK customers during 2011-2014.

PCI Level 3: 20,000 – 1 million online transactions per year per card scheme

Whilst Worldpay has seen a

62%

growth in PCI DSS compliance amongst Level 3 organisations, card breach investigation data shows the **Level 3** space is still a challenge.

Typically companies of this size are large enough to use a range of payments functionality, yet at the same time, may be too small to have a mature and well funded information security team. Additionally, Worldpay data shows Level 3 businesses are most likely to fail Approved Scanning Vendor (ASV) scans, or fail to submit results on a quarterly basis, so many are non-compliant at any given time.

Between 2011-2013 Worldpay observed a steady increase in attacks against Level 3 companies, until 2013 where there was a near convergence between the number of Level 3 breaches and Level 4 breaches. The likely reason behind this trend is that online Level 3 businesses can process up to 1 million transactions per year – giving the attacker a potentially far greater return on investment than they would get by targeting a smaller business.

Last year Worldpay expected this trend to continue but analysis shows Level 3 breaches decreased in 2014. Whilst it is difficult to pinpoint the exact reason for this sudden change, a sharp increase in in Level 4 breaches has been linked to the compromise of a large ecommerce platform, possibly diverting the hacker's attention from Level 3 companies.

PCI Level 4: Less than 20,000 transactions per year, per card scheme

Over the past four years, PCI DSS compliance rates amongst Level 4 organisations, have improved somewhat, but raising them further remains a challenge as there seem to be a number of small businesses who are either not interested, not aware, or don't understand how to become PCI DSS compliant.

Since the launch of a new SaferPayments programme in summer 2014, Worldpay has helped over

30,000

Level 4 customers certify that they are PCI DSS compliant. By the end of March 2015 Worldpay had 260,000 customers enrolled in its SaferPayments programme to help make confirming PCI DSS compliance simpler and quicker.

Figures are based on card data breaches which occurred for Worldpay UK customers during 2011-2014.

PCI DSS technology trends

Payment security technology has also improved significantly, most notably with Point-to-Point Encryption (P2PE), which will likely be used to help protect the payment systems of virtually all businesses in the future. P2PE is a process of securely encrypting transaction data from the point-of-sale entry to the payment processor. Data is encrypted when entered into the point-of-sale hardware and is decrypted offsite by the payment processor. As the data is encrypted hackers are unable to read it should they gain access to the network.

The beauty of P2PE is that it not only de-scopes vast amounts of an organisation's network from PCI DSS, minimising the compliance burden, but it also means that if data is breached it should be rendered unreadable, and therefore useless, to hackers.

What's more, with increasing numbers of businesses moving into multiple retail channels, P2PE can be used in conjunction with 'tokenisation' to keep payment data secure across those channels.

Elsewhere, increasing interest in hosted payment pages has helped improve ecommerce security, especially amongst Level 4 businesses, although it is still important for businesses to monitor the security of third party suppliers.

However, despite improvements in technology Worldpay has noticed an increase in attacks targeting smaller businesses who are not investing in payment security as much as larger, better resourced companies.

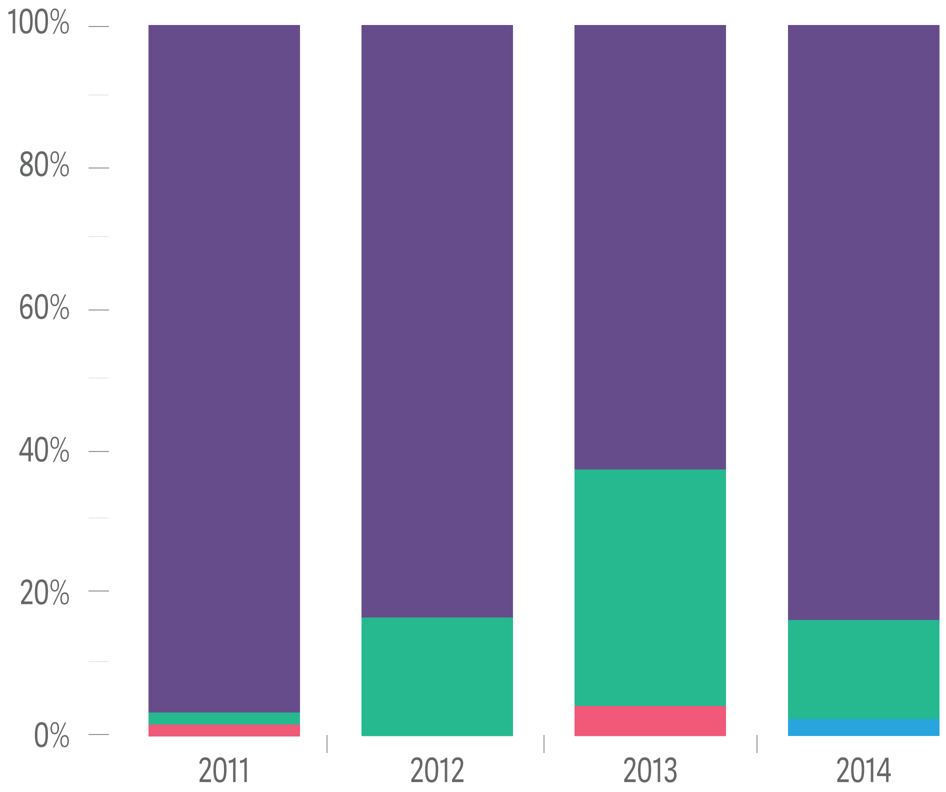
What's more, attacks aren't necessarily getting more sophisticated; in fact the majority of breaches still occur via known vulnerabilities and commonly used attack techniques such as SQL injection or malicious web shells.

It is clear that the means to launch such attacks have become more accessible in recent years. No longer does an attacker have to be technically proficient – as the know-how and malware can be found on underground online forums and in attack toolkits. Such is the extent and maturity of the cyber criminal community that hacking exploits can even be bought and launched "as a service" in a similar way to legitimate software-as-a-service.

Card data breaches

This graph shows the number of investigations into card breaches (i.e. known breaches) amongst Worldpay customers, by business PCI DSS level during 2011-2014. There were a total of 140 investigations held during this period.

The graph reveals an overall decrease in Level 4 breaches up to 2013, which is being off-set by an increase in Level 3 breaches. The turnaround in 2014 was due to an ecommerce platform breach and a number of small Level 4 businesses suffering card data breaches as a result.



Key:

1 **PCI Level 1:** 6m+ transactions per year per card scheme

2 **PCI Level 2:** 1m-6m transactions per year per card scheme

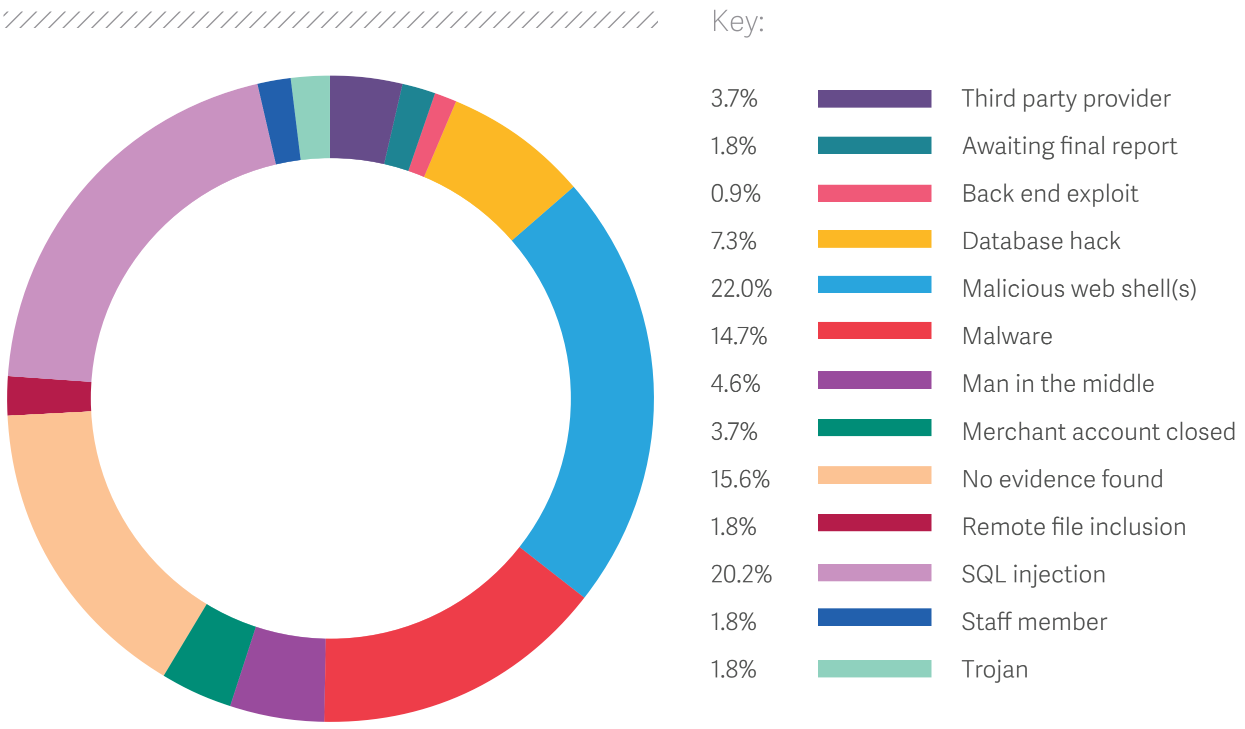
3 **PCI Level 3:** 20,000 – 1 million online transactions per year per card scheme

4 **PCI Level 4:** Less than 20,000 transactions per year, per card scheme

Figures are based on card data breaches which occurred for Worldpay UK customers during 2011-2014.

Causes of card data breaches

These graphs show the causes of card data breaches amongst Worldpay customers, during 2011-2014. There were a total of 140 investigations carried out during this period.



	2011	2012	2013	2014
1	=Database hack 13.1%	SQL injection 50%	No evidence found 29.1%	=Malicious web shells 23.3%
2	=No evidence found 13.1%	=Malware 16.7%	Malicious web shells 25%	=Malware 23.3%
3	Malicious web shells 9.9%	=Malicious web shells 16.7%	SQL injection 20.8%	SQL injection 13.9%

Card data breach causes were established in 60% of cases, and these are displayed where known. It is important to note that investigations which resulted in 'inconclusive', and 'report not seen' results have been omitted. Inconclusive reports are due to the investigation being a 'lite' version for small businesses, which focused on outsourcing payment pages rather than determining the cause of the breach. For 'Report not seen', a business will have more than one relationship with a payment processor, and it was another payment processor who led the investigation.

Figures are based on card data breaches which occurred for Worldpay UK customers during 2011-2014.

SQL injection

On websites there is normally a free search text box you can use to enter words, with the expectation this will return pages on the website relating to the word(s) entered. Usually this search function queries the SQL database that sits behind the website to find matches.

If proper controls are not in place hackers can enter SQL commands into the search text box on your website and create error messages. The information in these error messages can enable hackers to start piecing together how an SQL database is configured, allowing them to ask more directed queries to extract card data from the website. To prevent this type of attack businesses can use what is known as 'input validation'. This restricts what can be entered into the search text box so hackers can't use malicious SQL commands.

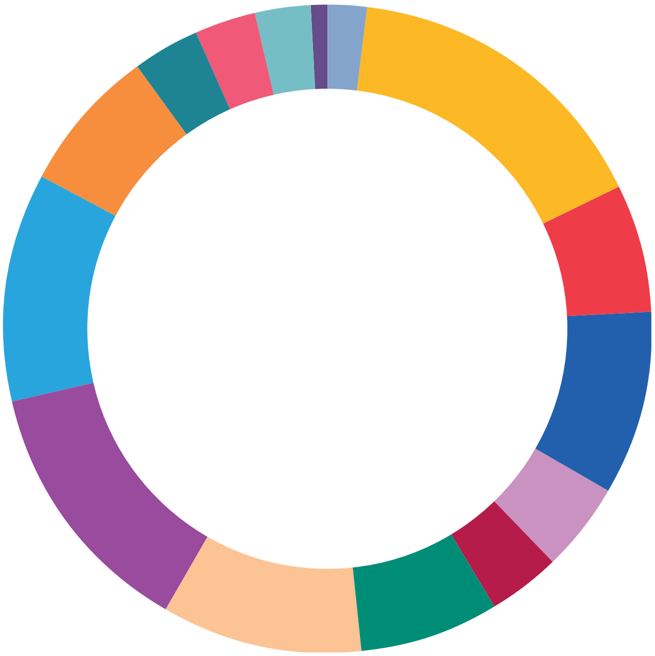
Malicious web shell(s)

Malicious web shells are difficult to spot, as hackers exploit vulnerabilities in a website to insert a piece of 'PHP' code unnoticed. Like a sleeper agent, this software remains hidden, until it receives an activation message via a hidden URL. The malicious web shell then harvests card data and transmits it to the hacker. Using a reputable PCI DSS-compliant web hosting provider can help a business to protect itself from this type of attack.

Industries affected by card data breaches

These graphs show the industries most affected by card data breaches, as a result of the breaches reported by Worldpay customers during 2011-2014. There were a total of 140 investigations carried out during this period.

Clothing and Footwear has been the most breached industry sector for the past four years. In 2013 it was temporarily superseded by Pharmacy and Beauty.



Key:

2.1%	🟦	Art and Leisure
15.7%	🟨	Clothing and Footwear
6.4%	🟥	DIY and Home decorating
9.3%	🟦	Electronics
4.3%	🟪	Entertainment
3.6%	🟥	Food and Grocery
7.1%	🟩	Hobbies and Specialities
10.0%	🟧	Motoring
12.9%	🟪	Pharmacy and Beauty
11.4%	🟦	Retail
7.1%	🟧	Services
3.6%	🟩	Specialty retail
2.9%	🟥	Sports Activities and Wellbeing
2.9%	🟦	Travel
0.7%	🟪	Wholesale

	2011	2012	2013	2014
1	Clothing and Footwear 16.4%	=Clothing and Footwear 16.7%	Pharmacy and Beauty 25%	Clothing and Footwear 18.6%
2	Electronics 14.8%	=Hobbies and Specialities 16.7%	Motoring 12.5%	Retail 13.9%
3	Pharmacy and Beauty 13.1%	Mix of others	Mix of others	Hobbies and Specialities 11.6%

Figures are based on card data breaches which occurred for Worldpay UK customers during 2011-2014.

Managing a card data breach

A card data breach is the suspected or confirmed loss/theft of any material or records containing account/transactional information. It is important to remember that attackers do not only target ecommerce infrastructure, computer networks or databases holding card data at businesses and service providers. Attacks against Chip and PIN entry devices, Point of Sale systems and anywhere else card data is stolen or lost from may also be classed as a card data breach.

Discovering a breach

Worldpay is usually made aware of a card data breach via:

- Business identification and self-reporting – a customer may contact Worldpay if it has seen suspicious activity on its systems, or received calls from customers who have suffered fraud on their credit cards following a genuine purchase at their business.
- Card issuers – may notice fraud patterns suggesting card data has been sourced from a single point.
- Financial Fraud Action UK – which issue and receive intelligence alerts from the payments industry and other stakeholders.
- Card schemes – which may contact Worldpay to share their concerns.

Investigating a breach

There are two triggers for determining if an investigation is needed:

1. Notification of a suspected breach from one or more of the card schemes.
2. A fraud to sales ratio of >1% and/or where more than 15 cards are believed to have been compromised.

Worldpay also investigates any circumstances that may otherwise account for a spike in fraud, such as seasonal trading, discounting, or major events such as Black Friday, as these can create trading abnormalities that may confuse monitoring tools.

In all cases Worldpay will notify the customer, and offer guidance to those having difficulty with PCI DSS compliance.

Supporting a customer though a breach

In the event of a data breach, Worldpay provides guidance on what a customer should and should not do, e.g. a business should not access or change compromised systems. The customer should also not 'turn off' any compromised systems. These should be isolated from the network by removing the network cable, preserving all logs and recording all actions.

Worldpay works closely with its customers to guide them through investigation, remediation and finally PCI DSS certification.

Worldpay also acts as a conduit between a customer and third parties, such as: a PCI DSS Approved Forensic Investigator (PFI), a Qualified Security Assessor, card schemes, web hosts, acquirers and law enforcement. The first 48 hours after a breach is discovered is vitally important. It is essential that all parts of a business work together on disaster recovery: including Marketing, IT, Legal, Risk, Customer Service.

With all essential internal stakeholders working closely together a business can be best prepared to face the stormy waters ahead. It is important not to underestimate the drain on time and resources that working through a breach will have on an organisation. A business should expect to be under constant scrutiny, whether by its customers, shareholders or industry regulators.

Financial costs

There is no such thing as a 'standard' investigation, and costs can vary wildly between seemingly similar businesses. Costs depend on the payment channel under investigation, the number of servers and how interconnected those servers are. Most important is the need to employ a forensic investigator with relevant experience – as this can make a huge difference in the time taken to resolve the issue. Worldpay has seen businesses pay between £25,000-£50,000 for a PCI Level 2 investigation and £100,000 for a Level 1 investigation.

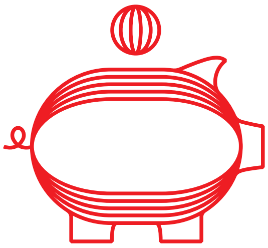
A breach in the PCI DSS Level 1 and 2 spaces can attract large financial penalties. The privacy watchdog the Information Commissioners Office also has the power to fine up to £500,000 for serious breaches of the Data Protection Act, in addition to fines levied by the card schemes.

Card schemes have the power to penalise payment providers, who in turn pass these costs on to the customers that experienced the card data breach. The largest set of card scheme penalties Worldpay managed in recent years for a single breach was £246,500, which was reduced from £1.09m though good data breach management.

Last year, Worldpay's UK businesses could have faced penalties of £315,000, but Worldpay reduced this to £195,000 through good breach management.

Another cost which must be considered is remediation. PCI DSS was designed to reduce data breaches by imposing mandatory obligations on businesses to improve card data security. The card industry can be forgiving if a business can show it is working towards compliance. However if a breach occurs during this time then an organisation will be required to get compliant within 90 days, which could cost millions to deliver for larger organisations.

Those certified as compliant are more likely to have penalties waived. However, in some cases failure to have up to date security controls in between auditing periods, or an oversight by their original assessors may put a business at risk. It is for these reasons that it is important to perform appropriate due diligence on the Qualified Security Assessor before selection, and to incorporate PCI DSS in business-as-usual operations, rather than taking a project-based tick-box compliance approach.



Intangible costs

Whilst the damage to an organisation's reputation is generally well understood, it is difficult to quantify.

Often the aftermath of a card data breach results in IT security team changes, necessitating costly and time-consuming recruitment processes. Significant additional investment will also be needed to revise current marketing strategies and execute these quickly.

Case study

A third party service provider

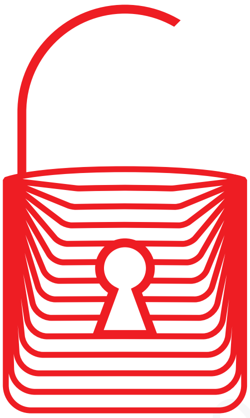
This software and hardware supplier had worked with a number of high-profile brands to provide their in-store payments.

It was not well-known in its own right, but processed payments on behalf of organisations that were very brand aware. The supplier was aware of PCI DSS, and had a funded and well managed programme in place. It had decided to build an entirely new, compliant platform and switch businesses over from the old platform once work on the new platform was completed.

Unfortunately it was the old, non-compliant platform which was compromised.

The attack came via an X25 connection through which the hacker gained access to the network. The X25 line connected to a redundant testing server which, although no longer used, had not been decommissioned. All the attackers then needed to do was deduce a four digit router password to access the internal network.

They used a single server to scan others for vulnerabilities and were able to gain root access to other servers containing card data. Malware installed on these payment servers identified and extracted track2 (magnetic stripe) data and sent it to an external accomplice. The forensic investigation was able to identify a very clear picture despite the hacker using a number of techniques to delete log files and modify time and date stamps for using malicious software.



Points of Interest:

1. Whilst the attacker was highly competent, it was easy to break a four-digit router password, allowing them access.
2. The testing server was no longer being used but was exploitable.
3. Hackers go to great lengths to deploy counter measures and hamper forensic efforts.
4. Although the hackers could access EMV (Chip and PIN) data, this was not used for fraudulent payments.
5. This supplier took PCI DSS very seriously and was making all the right moves in developing a new secure platform. Unfortunately it had largely forgotten about the old one.

Lessons learnt:

The supplier should have segregated the machines in their test environment from their 'live' machines. The passwords used were not strong or complex enough, which made them too easy to crack. Inadequate firewall protection also left this supplier vulnerable to attack.

Additionally, the 16 digit card number data should have been stored in an encrypted format. Internal and external vulnerability scanning was not put in place until after the event. This may have prevented the incident.

It took the supplier around two months to complete the forensic investigation and a further five months to become PCI compliant.

This was a particularly interesting case because it highlighted the need for businesses to monitor their suppliers. In addition, the intrusion method was unusual and the data set extracted by the hackers was 'cardholder present' data rather than the usual ecommerce data. There was also a degree of human error and poor timing, which coupled with the other factors led to a prolonged and painful investigation.

The future of payment security

With a myriad of alternative payment methods, new players emerging across the industry, and the exponential rise in mobile commerce it is clear that businesses will have a substantial amount of work to do in achieving and maintaining stringent payment security standards across all manner of payment infrastructure and systems in the future.

PCI DSS version 3.0 was released earlier this year, so businesses should ensure they reference the latest evolution of the standards in their compliance plan. Also, with an increasing focus on payment regulation now emerging in both UK domestic and European markets, businesses should be constantly monitoring new developments and shaping their PCI DSS programme accordingly.

The following trends are shaping the future of payment security in the UK:

Cloud computing:

The UK is yet to see its first major breach involving the cloud and card details – but if businesses cannot prove the appropriate due diligence and controls in place for managing their cloud and service provider, then regulators and/or card schemes may see using cloud computing as an aggravating factor when assessing fines.

Financial penalties:

The financial penalties for suffering a card data breach in future may increase significantly. PCI DSS compliance will remain a benchmark for regulators and card schemes when ascertaining the fines to impose in the event of a breach, and forensic reports will state if the business was compliant before the breach.

M-commerce:

Current digital wallets use a user name and a password or other authentication to make a payment – rather than inputting the card number – so that card details are not passed through businesses. This reduces the risk and therefore consequences of a breach. Many payment service providers also offer a selection of API's and software development kits to enable businesses to take card payments without needing to see the 16 digit card number – as the details are entered directly onto payment service provider systems rather than through individual businesses.

Notifying consumers of a card data breach:

As detailed in the European Banking Authority's guidelines 'The Security of Internet Payments Across the EU', it is likely that from August 2015 there will be a requirement to quickly notify consumers if a data breach occurs. This will drastically change the dynamics of any breach, and associated remediation plan.

Payment capture:

Faced with increasing breach costs, more businesses will opt for outsourcing payment pages to a card processor. Worldpay data shows that 97% of data breaches occur in online businesses processing payments themselves*. From a risk-based approach, outsourcing payment capture is the single biggest improvement a business can make in payment security (particularly when used in conjunction with File Integrity Monitoring to protect against a 'man-in-the-middle' attack). In addition, as payment providers come under further scrutiny from regulators in managing risk, limitations may be imposed on high-risk payment capture methods.

Point to Point Encryption (P2PE):

Validated P2PE solutions will continue to evolve. The modularised validation process will help to support overall adoption as solution providers tailor products more easily. However, many Level 1 businesses, whilst using P2PE security, will likely continue to use their bespoke non-validated solutions. This is due to the cost and constraints associated with returning their old Pin Entry Devices to manufacturers (in order to meet the current chain-of-custody audit requirements).

Tokenisation:

Use of a token card number, where only part of the card number is stored, can reduce the risk and therefore consequences of a breach. Token card numbers can be used to provide more than payment channel separation, as each token card number can have an associated set of constraints which may be used to limit where it may be used. For example if an organisation issued a token card number to be used as a card on file, then the token would be constrained for use by that organisation only, for e-commerce transactions.

*Figures are based on card data breaches which occurred for Worldpay UK customers during 2011-2014.

Best practice tips for payment security

It is vital to take payment security seriously. Businesses need to understand how they store, process and/or transmit card data.

Businesses should:

- Outsource any work to build a payment environment to a PCI DSS compliant third party that agrees to accept responsibility for the security of card data under its control as required by PCI DSS.
- Install the latest patches for all servers, operating systems, applications, frameworks (Java, .NET etc.), content management systems and anything else running the business. This should reduce the majority of SQL injection, PHP exploit, Malicious web shell and other vulnerabilities.
- Avoid running unnecessary technology or systems – as these could be forgotten until hackers target payment systems.
- Avoid storing unneeded confidential data – as this will bring added risk.
- Change any internal system log-ins from their default and use strong passwords. Also ensure systems are only accessible from a limited number of sources by, for example, approved static IP addresses only.
- Maintain log files for as long as is practical, at least a year.

Whilst there are no guarantees against hackers, taking these steps will help limit the risk of an organisation suffering a card data breach.

It is clear that prevention is better than cure. There are an abundance of security solutions available, to help make a business less appealing to hackers. British businesses should invest in security infrastructure, to help avoid suffering a card data breach in future.

Worldpay customers who believe they may have been subject to a card data breach should contact Worldpay for guidance.

paymentsecurity@Worldpay.com

Worldpay UK Limited

www.worldpay.com/uk

This report was compiled by Tim Lansdale, Head of Payment Security, and Graham Hutchings, Senior Data Breach Manager at Worldpay, who between them have over 14 years investigating card data breaches.

This document is for information purposes only of the intended recipient. We have taken care in the preparation of the information in this document but will not be responsible for any losses or damages including loss of profits, indirect, special or consequential losses arising as a result of any information in this document or reliance on it (other than in respect of fraud or death or personal injury caused by negligence). Terms and conditions apply to all our services.

worldpay

worldpay.com

Worldpay (UK) Limited. Registered in England No. 07316500. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AF. Worldpay (UK) Limited is authorised by the Financial Conduct Authority under the Payment Service Regulations 2009 (No. 530923) for the provision of payment services and is authorised and regulated by the Financial Conduct Authority for consumer credit activities.
Worldpay, the logo and any associated branding names are all trade marks of the Worldpay group of companies.