

safe and sound

processing online card payments securely

a white paper from Barclaycard
leading the way in secure payments

April 2010

Executive summary

The following information and guidance is intended to provide key payment security advice to new or existing merchants who trade online. This information highlights the key areas you need to address in order to be secure when processing card payments, and how best to protect your business and your customers from the risks of fraud.

Barclaycard are developing a range of further guidance that will provide greater detail on this and other related issues, that will be made available during the course of 2010.

Less than 10% of merchants trade online, yet these account for 98% of all data compromises

Audience

This information and guidance is aimed at Company owners, Financial Directors, and web developers of small to medium ecommerce merchants.

Purpose

The primary objectives of this paper are to highlight the practices that should be adopted by all e-commerce merchants with regard to card data security in general, their responsibilities towards compliance with the Payment Card Industry Data Security Standard (PCI DSS), and how these responsibilities can be impacted according to how an ecommerce trading operation is deployed. These responsibilities and practices apply to all businesses, and form an integral part of Barclaycard's Terms and Conditions with merchants.

Why online card payment security is important

Modern day criminals want our data: be it credit, financial, payment card or personal. There is a strong black market in each, and identity thieves are more inventive than ever. The annual cost of identity theft to the UK economy is estimated to be £1.2bn.

Every year we share more of ourselves online - a trend that is set to continue as we spend more money on e-commerce sites. Each time we do this, we place our data and our faith in the security measures taken by the businesses that manage these e-commerce sites.

The Payment Card Industry Data Security Standard has been introduced to help protect everyone against card fraud; to protect you as a business and to protect your customers' card data. Your business is dependent on your customers' trust. If e-commerce security is not high on your agenda then you may lose more than you think.

The risks of trading online

The following examples illustrate the consequences faced by small and medium sized businesses as a result of a data compromise:

Example 1

A medium sized specialist UK retailer with an annual card payment value of £2.4m was compromised in 2009. They received penalties of £89,950 and may also be liable for fraud reported against the compromised cards. The forensic investigation cost circa £12,000 and there was significant disruption and cost to the business whilst remediation work was carried out.

This retailer accepted card payments via their website, by four high street shops, and via mail order and telephone. The merchant was not processing their web payments securely as highlighted by the following points:

- The website used a non PCI DSS compliant web host
- Stored customer data, including card data such as the Primary Account Number (PAN), Card Verification Value, expiry date etc. unencrypted (in plain text) in a database
- Parts of the cardholder details were stored as part of the transaction logs in clear text

The hacker managed to compromise the web and database servers and install malware which allowed the attacker to obtain the card data.

Example 2

A small sports retailer with an annual card payment value of £300,000 was recently compromised. They received a penalty of £8,768, the forensic investigation cost circa £5,000 and the business will have been disrupted whilst the forensic investigation was undertaken.

The retailer accepted card payment details via their website, in their shop, via mail order and over the phone; however all payments were processed on a card terminal. The specific cause of the breach has not been proven because of inadequate log records which could have been deleted by the hackers. However the merchant still suffered the consequences, costs and inconvenience of the breach as he was not processing customer card payments securely as highlighted by the following points:

- using a 3rd party where the web server and database servers were shared
- stored cardholder data on the shared server (including Card Verification numbers)
- several staff used default administrator logins
- log files were inadequate to pinpoint the cause of breach

As these merchants have been compromised they are now required to validate their compliance through the services of a Qualified Security Assessor, which costs an average of £1,000 per day.

TOP TIP: The risk of the above compromises happening could have been significantly reduced by following the do's and don'ts advice given in our 'Important recommendations' section.

The threat of hacking

Exploiting vulnerabilities using techniques such as SQL injection is a method currently in favour with hackers and data thieves. SQL injection attacks exploit vulnerabilities at the web application layer to access sensitive data in back-end databases. These web-based attacks can pass undetected through firewalls and other perimeter defences, including intrusion detection and intrusion prevention systems, then hijack the application server to gain access to underlying database records.

This threat is rising, and according to a data breach report published by the Verizon Business RISK team, 75% of all breached records came from compromised database servers, while other IT assets such as laptops and back-up tapes accounted for less than 0.05% of compromised data.

The definition of sensitive data has broadened. Dates of birth, addresses, personal histories, the details of daily lives - all this data is useful to a fraudster, and may be the first steps towards more complete identity theft.

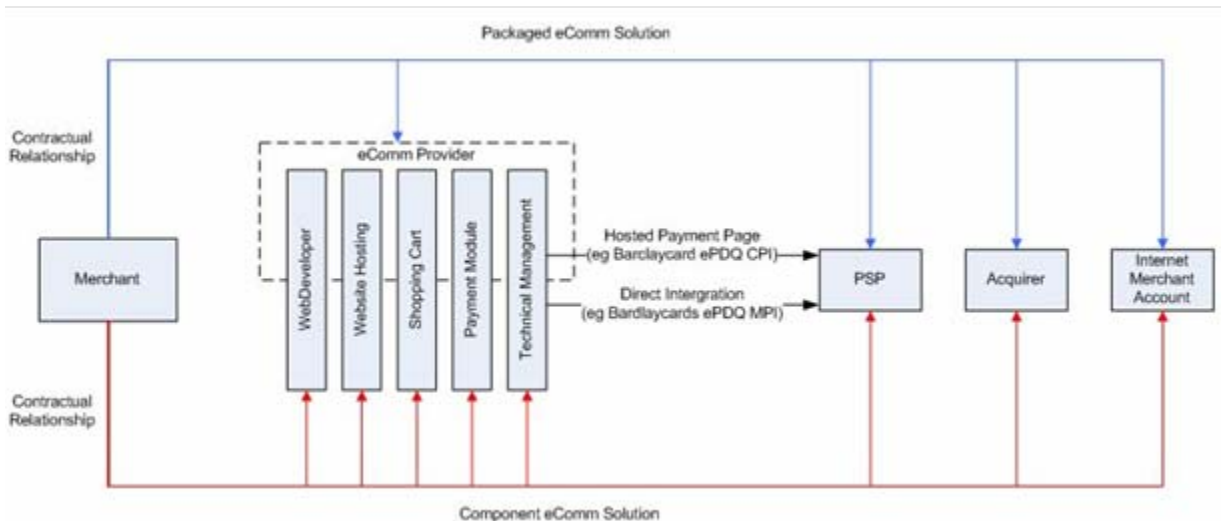
All businesses need to understand that any and all personal data is valuable, and that it is imperative that it is stored securely.

Online trading deployment options

The following diagram illustrates how the deployment of online trading solutions can affect your data security and PCI DSS compliance responsibilities:

There are two basic options - a hosted payment page, such as Barclaycard's ePDQ CPI solution, where the merchant links to a payment page hosted by the third party PSP; or Direct Integration, such as Barclaycard's ePDQ MPI solution, where the payment page is fully integrated within the merchants' own web site.

PCI DSS Compliance responsibilities – packaged vs component ecommerce solutions



TOP TIP: By adopting a packaged approach to your card payment security requirements, you can reduce your number of commercial relationships, which can help provide clearer responsibility and accountability for the PCI DSS compliance and security of your online shop.

Risk comparison of e-commerce solution deployment options

Risk comparisons by ecomm solution

Hosted payment page

Direct integration

Packaged ecomm solution	<p style="text-align: center;">Lowest risk</p> <p>Need to understand detail of solution</p> <ul style="list-style-type: none"> ✓ Delegate responsibility to supplier ✓ Not storing sensitive card holder data ✓ Fewer supplier management relations ✓ PCI DSS compliant packaged solution ✓ Less in-house technical expertise ✓ Reduced PCI DSS footprint ✓ Reduced technical management ✗ Easy to forget compliance responsibilities 	<p style="text-align: center;">Next highest risk</p> <p>Need to understand detail of solution</p> <ul style="list-style-type: none"> ✓ Less in-house technical expertise ✓ Reduced technical management ✗ Increased PCI DSS footprint ✗ Greater reliance on provider for security ✗ Easy to forget compliance responsibilities ✗ More due diligence ✗ Risk of storing sensitive card holder data
	<p style="text-align: center;">Next lowest risk</p> <p>Need to understand detail of solution</p> <ul style="list-style-type: none"> ✓ Not storing card data ✓ Reduced PCI DSS footprint ✗ Multiple suppliers/points of ownership ✗ Blurred boundaries of responsibilities/ ownership ✗ Risk of technical/compatibility issues ✗ More in-house expertise 	<p style="text-align: center;">Highest risk</p> <p>Need to understand detail of solution</p> <ul style="list-style-type: none"> ✓ Can create own payment page ✓ Ability to tailor to individual needs ✗ Multiple suppliers/points of ownership ✗ Blurred boundaries of responsibilities/ ownership ✗ Risk of technical/compatibility issues ✗ More in-house expertise ✗ Increased PCI DSS footprint ✗ Storing card data
Component ecomm solution		

E-commerce solution deployment options explained

Packaged e-comm solution / Hosted Payment Page - Offers advantage of simpler provisioning of an ecommerce environment. Good for merchants with little IT capability. Web sites using Hosted Payment Pages need to be adequately protected to ensure that they remain outside of scope of PCI DSS. It is Barclaycard's recommendation that the packaged e-commerce solution provider is PCI DSS compliant as a Level 1 Service Provider.

Component e-comm solution / Hosted payment page - Merchant chooses multiple parties to work with or does this through a web developer. Merchant should have good IT / web technical skills to understand the implications of what has been implemented on their behalf. Merchant is left managing multiple relationships. Barclaycard recommends that the relevant components of the e-commerce solution are PCI DSS compliant as Level 1 Service Providers e.g. web host. Could be perceived as a lower cost alternative to Packaged ecomm solution / Hosted Payment Page but at higher risk.

Packaged e-comm solution / Direct integration - Offers advantage of simpler provisioning of an e-commerce environment but at a higher risk to the Hosted Payment Page option because the web site and associated infrastructure handles card data and therefore is in scope of PCI DSS. Direct integration can deliver a more seamless integration with the Internet Payment Service Provider. Web sites using a direct integration with the IPSP fall within scope of PCI DSS and require strong protection to prevent them leaking card data. The packaged ecommerce Provider is required to be PCI DSS compliant as a Level 1 Service Provider.

Component e-comm solution / Direct integration - This option should only be considered by large e-commerce merchants (say processing more than 1m payments a year) who need extreme flexibility over the way the web site looks and works. Should only be attempted by organisations who have strong web development and Information Security functions. Site is fully in scope of PCI DSS and relevant external parties are required to be PCI DSS compliant as a Level 1 Service Provider

TOP TIP: A hosted payment page offers a simpler and easier to secure solution and reduced scope for your PCI DSS compliance requirements. The ecommerce solution, with the lowest risk that we would recommend all new ecommerce merchants to adopt, is a packaged solution with a hosted payment page.

Important recommendations to secure your online shop

Do's:

- Use an Internet Payment Service Provider (IPSP) such as Barclaycard's ePDQ service to process card payments from your online shop
- Make sure servers are hardened. Only necessary services and protocols should be supported, all other functionality should be disabled. All default accounts should be either changed or removed as a priority (see fact sheet at www.visaeurope.com/documents/ais/sql_factsheet.pdf)
- Keep software up to date, e.g. shopping carts, operating systems, infrastructure applications eg web servers etc
- Ensure regular checks are carried out of your website to detect any new or unknown web pages or files. In particular, you need to regularly check the code that redirects customers to a hosted payment page is the same code that was provided by the service provider and has not been modified
- Use strong passwords and unique user IDs (*see References*)
- Keep logs, e.g. web server logs, operating systems, fire walls etc.
- Use PCI DSS compliant suppliers (*see References*)
- Carry out regular network security scans (Operating Systems, Applications, networks)
- Carry out penetration tests
- Ensure contractual agreements are in place. It is advisable to include PCI DSS liability clauses in those agreements to enable you to pass on any fines or costs should a breach occur as a result of vulnerability in the third party environment. Barclaycard can help you with these.
- Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.

Don'ts:

- Capture card data on the ecommerce site and subsequently re-enter in a card terminal.
- Send unencrypted card data via email or other electronic means
- Use default user IDs or passwords
- Capture card data in any logs, e.g. transaction, error etc.

References

Barclaycard payment security and PCI DSS Information
www.barclaycard.co.uk/pcidss

Payment Card Industry Security Standards Council
www.pcisecuritystandards.org/index.html

Visa downloads and resources (where vulnerability guidance can also be found)
www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp

Vulnerability Guidance

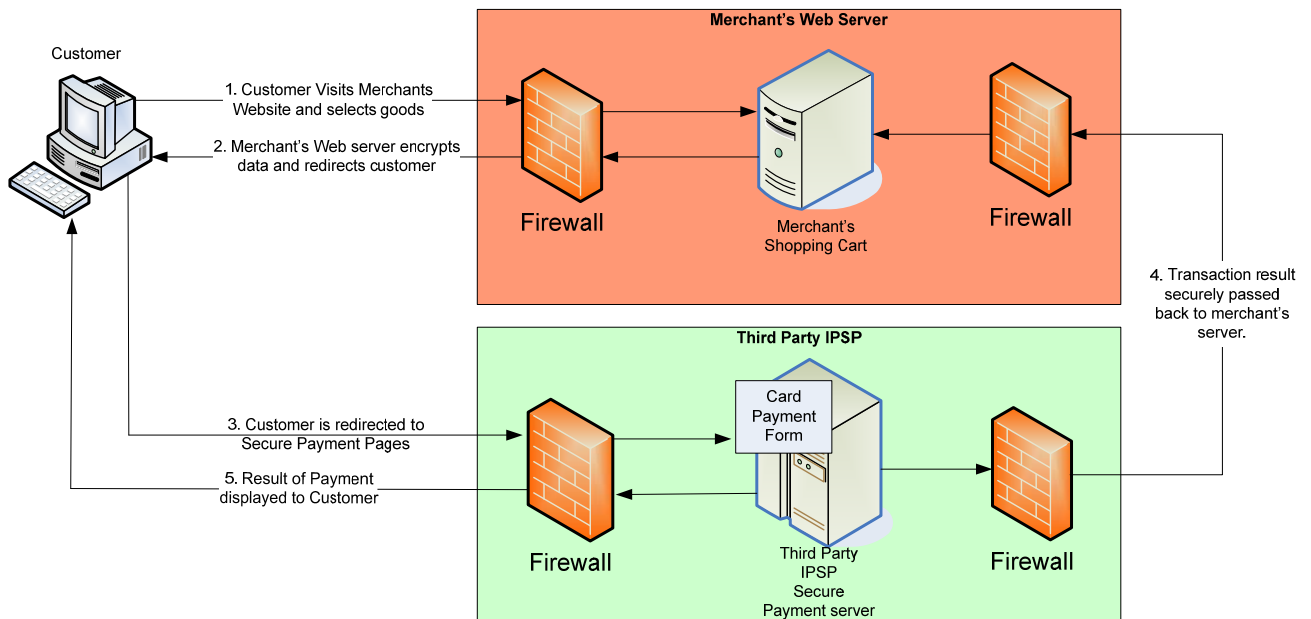
i) SQL Injection Attacks
www.visaeurope.com/documents/ais/sql_factsheet.pdf

ii) Default Passwords
www.visaeurope.com/documents/ais/ds_factsheet.pdf

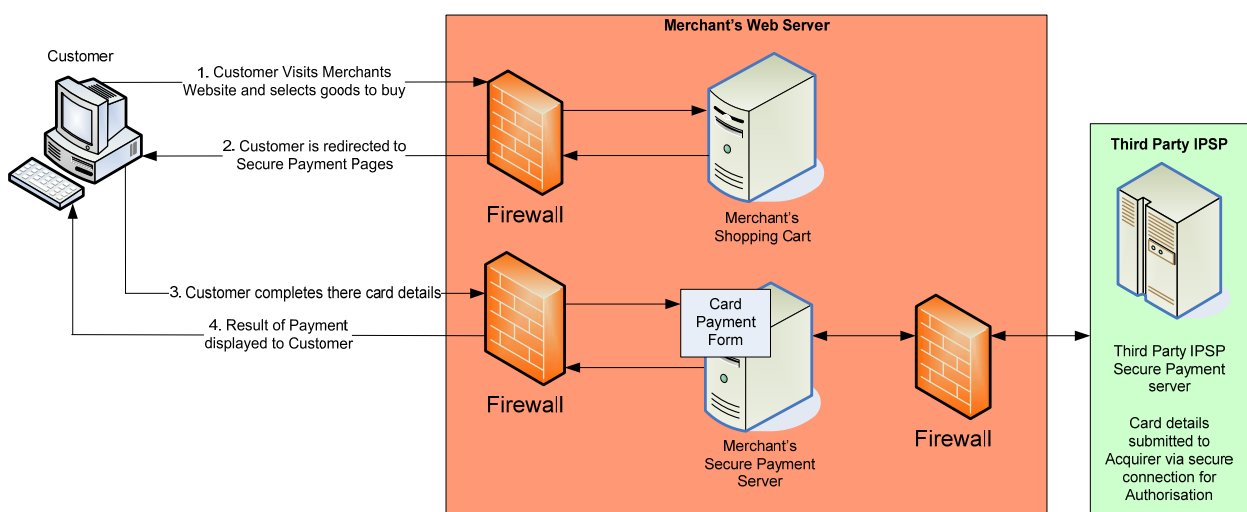
Appendix

The diagrams below highlight the differences between an ecommerce solution using a hosted payment page and a solution using direct integration.

i) Hosted payment page



ii) Direct integration



Useful terms and definitions

Acquirers

An acquiring bank (or acquirer) is the bank or financial institution that accepts credit and or debit card payments for products or services on behalf of a merchant. The term acquirer indicates that the bank accepts or acquires transactions performed using a credit card issued by all banks within the card association scheme. The best known (credit) Card Association schemes are Visa, MasterCard, American Express, Diners Club and JCB.

Card Schemes

Card Schemes refers to Visa, MasterCard etc, as the owners of the payment scheme, into which a bank or any other eligible financial institution can become a member. By becoming a member of the scheme, the member then gets the possibility to issue or acquire the transactions performed within the scheme.

Common attack vectors

i) SQL Injection

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

ii) Man in the Middle Attack

A security attack in which an attacker intercepts and possibly modifies data that is transmitted between two users. The attacker pretends to be the other person to each user. In a successful MITM attack, the users are unaware that there is an attacker, which is intercepting and modifying their data, between them.

Internet Payment Service Provider (IPSP)

An internet payment service provider (IPSP) offers merchants online services that enable the acceptance of electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking.

Merchant

A merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of the PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an Internet Service Provider (ISP) is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

Network Security Scan

Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.

Payment Card Industry Data Security Standard (PCI DSS)

i) What is it?

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide series of measures introduced by the Card Schemes (Visa and MasterCard) to help combat the increasing risks and costs associated with fraud through improvements to the security and storage of sensitive card holder data.

Compliance with the PCI Data Security Standard is mandatory and auditable, and we at Barclaycard do everything we can to help our merchants to achieve compliance, not only to help protect them and their customers from the risks of fraud, but also from the potential financial penalties they could face if they suffered a data compromise and were found to be non-compliant with the Standard.

Validation of compliance can be performed either internally or externally, depending on the volume of card transactions the organisation is handling, but regardless of the size of the organisation, compliance must be assessed annually. Organisations handling large volumes of transactions must have their compliance assessed by an independent assessor known as a Qualified Security Assessor (QSA), while companies handling smaller volumes have the option of self-certification via a Self-Assessment Questionnaire (SAQ). In some cases these SAQs still require sign-off by a QSA for submission.

ii) Why does it exist?

The standard was created to help organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organisations which hold, process, or pass cardholder information.

Penetration Test

Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.

Service Provider

Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.

Shopping cart/basket

A shopping cart or basket is a term used to describe the software used in e-commerce to assist people making purchases online. The software allows online shopping customers to accumulate a list of items for purchase, described metaphorically as "placing items in the shopping cart". Upon checkout, the software typically calculates a total for the order, including shipping and handling (i.e. postage and packing) charges and the associated taxes, as applicable.

Web hosting company

A web hosting service is a type of Internet hosting service that allows individuals and organisations to make their own website accessible via the World Wide Web. Web hosts are companies that provide space on a server they own or lease for use by their clients as well as providing internet connectivity, typically in a data centre. Web hosts can also provide data centre space and connectivity to the Internet for servers they do not own to be located in their data centre, called co-location.

Barclaycard: innovation and responsibility

- Barclaycard is innovative - First to introduce credit cards in 1966 & contactless technology in 2007
- Trusted brand with 11.9 million customers, and one in five credit cards in the UK in our portfolio
- We continually invest in technology in order to remain ahead of our competitors and enhance our service to customers
- We are a responsible lender, adapting and improving our products and services to help our customers.
- We help retailers acquire payments and help them meet their business objectives with easy to set up and cost-effective acquiring package.
- Leading the way in payment security:
 - PCI Security Standards Council Board of Advisors member
 - PCI SSC Participating Organisation
 - Dedicated Payment Security Team
 - Online resources
 - Publications
- We are a responsible business by treating our people, our local communities and the environment well.

Contact us

For more information on this paper and other payment security matters please email PCIDSS.Guide@barclaycard.co.uk



This document is available in large print, Braille and audio by calling [0844 811 6666](tel:0844 811 6666)

*Calls may be monitored or recorded to maintain high levels of security and quality of service. For BT business customers, calls to 0844 811 numbers will cost no more than 5p per minute, min call charge 5.9p (current at April 2010). The price on non-BT phone lines may be different.

Barclaycard is a trading name of Barclays Bank PLC. Barclays Bank PLC is authorised and regulated by the Financial Services Authority. Registered in England. Registered No. 1026167. Registered Office: 1 Churchill Place, London E14 5HP