

## Should you be “bovered”?



**PCI DSS** – more letters, what do they mean? And should you be bothered? Well, the acronym means Payment Card Industry Data Security Standard; and if you accept even one electronic or manual credit or debit card payment you **SHOULD** most definitely be bothered!



PCI DSS is intended to protect cardholders' credit and debit card accounts and transaction information. The Standard is universal across all major payment card brands – Visa, Mastercard, American Express, JCB and Discover.

### The Standard

The Standard addresses 12 key security areas, providing a consistent framework for securing and monitoring cardholder data. Those organisations who do not comply can be subject to severe sanctions ranging from the levy of fines to the withdrawal of authorisation to accept payment cards. Figures issued by Visa in January 2010, reveal that just 9%

of the U.K.'s Level-1 retailers (those handling more than 6 million card transactions a year) have managed to achieve PCI DSS compliance, and none of those are traditional bricks-and-mortar operations. Online-only retailers without physical stores have largely been successful in meeting the Standard. In the first half of 2009, £200,000 a month was being collected in fines for non-compliance.

PCI data security requirements apply to all merchants and service providers that store, process or transmit cardholder data. The security requirements apply to all manual processes, system components, network components, servers or applications included in, or connected to, the processing of cardholder data.

### What must you do?

Any organisation which accepts credit and/or debit cards for payment **MUST** comply with the PCI Data Security Standard. Further, that compliance must be validated on a regular basis. The actual validation requirements are set within pre-determined levels, which vary according to the number of card transactions processed annually. There are 4 levels of payment brand validation for merchants and 2 levels for service providers; Level 1 being the most onerous. Merchant verification as to your required

compliance level should be sought from your acquiring bank or entity used to process your card transactions. Service provider level verification will need to be determined by the controlling organisation specific to their role within the card processing lifecycle.

However, if you have IT equipment which is PCI-relevant, as a minimum, a quarterly external network vulnerability scan must be conducted by an accredited security firm. Level 1 and 2 organisations are also required to have an annual on-site security audit, although in some cases a self-assessment questionnaire may suffice, or indeed there may be no requirement at all.

### Are you bothered yet? Or do you still think PCI DSS doesn't apply to you?

Well, if you don't accept debit and/or credit cards for any payments and you are not a PCI service provider e.g. transaction authoriser, payment gateway, plastic card embossing company, then you have no need to be bothered. If you do accept cards (i.e. you are a merchant), or are a service provider, that stores, processes or transmits cardholder data then bothered you do need to be!

The PCI DSS is undoubtedly a

complicated Standard and is subject to a number of validation criteria based on: the brand of payment card; the number of card transactions processed annually; and whether or not your IT systems have been “hacked”. However the compliance requirements are the same for everyone.

Any cardholder data sent to anyone else (including by e-mail) must be made unreadable to prevent unauthorized persons intercepting and reading it.

However the key things to remain focussed on are the necessity for an appropriate security policy, adequate protection of the IT software and infrastructure against unauthorised access, antivirus measures, regular monitoring and testing of IT systems e.g. vulnerability scans, amongst a number of other key requirements. Access to card account information must be restricted on a need-to-know basis, and must be tracked. These requirements apply to **ALL** organisations accepting or processing payment card data (electronic or manual), irrespective of the size of the organisation or the number of transactions.

## PCI DSS Goals

The goals of the PCI DSS however are much simpler to comprehend. They are:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

There are 12 DSS mandatory requirements which support the 6 goals.

## So what does PCI DSS really mean for you?

All merchants and service providers must comply with the requirements of the PCI DSS. Verification of compliance, as a minimum, is required as follows.

### Level 1

1. Annual on-site review by a Qualified Security Assessor (QSA) – more on that later.
2. Quarterly network scan by an Assured Scanning Vendor. (An ASV is a PCI approved organisation who conducts external vulnerability scanning services).

### Level 2 & 3

1. Annual self-assessment questionnaire.
2. Quarterly network scan by an Assured Scanning Vendor.

### Level 4

This level is the same as level 3, but compliance only has to be reported if it is required by the bank providing card processing support.

## PCI DSS Compliance

As a merchant you should ask your acquiring bank (the one that initiates and maintains the relationship for acceptance of card payments), and as a service provider you should ask your controlling organisation (which could also be a bank) to confirm what level your organisation is and what reporting they will need to see.

You also need to arrange to validate your compliance against the Standard, and where necessary provide reports in the PCI standard format. This may involve hiring the services of a QSA firm to assist with your compliance and test the security of your computer

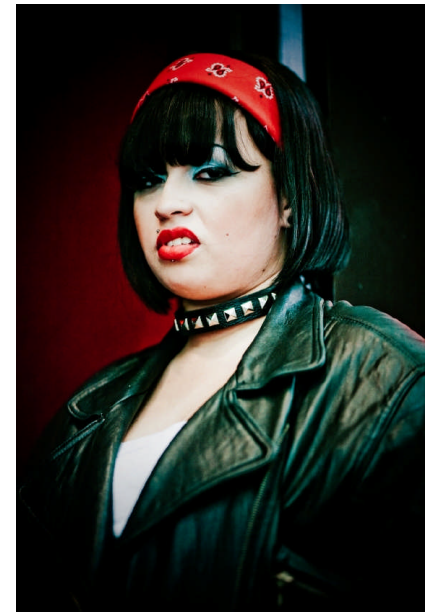
systems.

Compliance against the Standard must usually be validated and where required, reported on a regular basis. The reporting requirements can be complex and will vary according to the determined validation level.

## The consequences of non-compliance

Unlike the complexities of the Standard, this bit is simple to understand: failure to comply with the Standard is likely to result in you being held responsible for reimbursing any resultant losses due to fraud. In addition, you may be subject to more severe sanctions ranging from fines to being prohibited from accepting any payments by card, or operating as a service provider.

## Are you still yeah, but no but yeah but....?



## Well read on; we can help

The PCI Data Security Standard is **NOT** “something that applies to everyone else except you.” You **NEED** to familiarise yourselves with the requirements of the Standard and the elements that apply to you. Kingston Smith Consulting LLP is an accredited Qualified Security Assessor (QSA) firm, with trained and experienced

professionals who are qualified to provide education, advice and PCI data security assessments, regardless of the level of your PCI obligation. We are also in a position to provide approved vendor scanning. We can undertake current state assessments of your PCI DSS obligations, we can provide remediation advice to support you in meeting the requirements of the Standard and we are also qualified to provide PCI accreditation

and reporting if required. Following the recent announcement from Mastercard regarding the utilisation of qualified internal audit staff to conduct PCI assessments, Kingston Smith Consulting LLP are ideally placed to support and assist Level 1 and 2 firms; whether this is through supplementing the existing IA team and/or providing training and awareness etc.

**NOW** is definitely the time to be bothered about whether your organisation complies with the PCI Data Security Standard; but with the help of Kingston Smith Consulting LLP we can ensure that you are **NOT BOTHERED** by the payment brands for being non-compliant.

---

### About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

### Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010  
[info@kscllp.co.uk](mailto:info@kscllp.co.uk) [www.kscllp.co.uk](http://www.kscllp.co.uk)

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD