

# Plastic Security

## Tim Wright demystifies the PCI's Data Security Standard

The PCI Security Standards Council was founded in 2006 jointly by all the major payment card brands. The idea was that it would be an independent body looking after security standards in all jurisdictions where card payments were made.

To be clear, the payment cards we're talking about here comprise debit, credit and prepaid cards from any of the American Express, MasterCard, Visa, JCB and Discover brands. If you have any connection at all with payment cards or cardholder information, you must comply with the PCI Data Security Standard (DSS). From January 2011, version 2.0 became mandatory.

The Security Standards Council accredits organizations known as Qualified Security Assessor firms, and regularly verifies the quality of their work. The Council also accredits individual employees of these QSA firms as Qualified Security Assessors. Such individuals must undergo annual training and re-examination in PCI security standards. It might be worth pointing out that there is no freelance contractor market

in QSAs. If an individual is not a full-time employee of an accredited QSA firm, they cannot practise as a Qualified Security Assessor. The names of all these accredited firms and individuals are listed on the Council's website at

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). It follows that if you require the services of a QSA, you should verify that the firm you engage and the individuals they provide are properly accredited.

It's well worth having a look at the Council's website; there is a lot of free-to-download very useful material, including the Data Security Standard itself, explanatory notes and guidance, and so on.

There is a common misconception that the Security Standard doesn't apply to small organizations. In fact, it applies to small businesses equally as much as to the largest.

By far the majority of affected organizations are merchants, who sell products or services and accept payments by card – whether in person, over the phone, by mail order or online.

But the Standard applies equally to what are called Service Providers. These comprise pretty much anyone else involved in the card payment industry: plastic card manufacturers, payment gateways, banks, outsourced data centres, etc.

Especially for smaller firms, the burden of compliance is sometimes relatively high. One solution for reducing or even eliminating that burden altogether for ecommerce businesses is to outsource card transactions to a third party. Of course, if payments also come in by mail order you'll have cardholder data on your premises, and then the Standard swings into action again. It's concerned with physical security just as much as with logical; and pieces of paper are just as much within its ambit as digital data.

Cardholder data is the information printed on the physical card as well as the data on the magnetic stripe or chip. It includes what we will generically call the "Security code". This is usually the last three digits printed on the signature strip on the back of the card, although in

the case of American Express it's four digits embossed on the front of the card. The only data you should be saving anywhere are the Primary Account Number, cardholder name, and the expiry date.

It is *never* permissible for a merchant to store the security code in any form. You should also remember that if your organization receives orders by mail, you cannot store any part of the paperwork that contains the security code – it must be destroyed. This requirement also gives some headaches to those who record telephone conversations where the security code is asked for!

Merchants who process many transactions annually must usually have an annual on-site security review by a Qualified Security Assessor firm. That review will look at every control in the Standard. Those who process fewer transactions don't usually have to have the on-site review by a QSA firm, but may have to complete an annual self-assessment questionnaire instead.

You may well ask, given all this overhead, why should you bother

to comply? There are basically four reasons.

First: with any personal data, in most jurisdictions there is data protection or privacy legislation. These laws usually include an element of security; and by complying with the PCI's Data Security Standard, you may well satisfy those requirements as well.

Second, there are contractual obligations – if you look at your agreement with your bank, you will find that you have signed up to comply with this Standard whether you like it or not.

Third: if you are found to be in breach of compliance, the card brands may impose fines which can be quite large – or even withdraw your facility to accept card payments at all. For some organizations, that could be fatal.

But finally, common sense should prevail. These information security controls are good practice for any organization whether or not they take card payments. Information is everyone's most valuable asset and frequently too little is done to protect it. If you attack this subject with a "let's just satisfy

PCI and tick the box" attitude, in my view you are doomed to fail.

So here is a logical route to achieve PCI compliance.

First, make an inventory of all the reasons and places you store this data. If the data doesn't serve a valuable business purpose, consider eliminating it. If you don't need it, don't store it!

Then apply relevant security measures to cover the external perimeter of your cardholder data environment, any internal networks in scope, and any wireless networks you have.

Next in importance is to address the security of any applications which process cardholder data. Implement adequate access controls to all IT infrastructure, systems, applications, databases; and include measures to monitor that access.

Don't forget the physical security measures surrounding your cardholder data environment. And then, consider what is left in the Security Standard and put that in place as well.

**Tim Wright is a Qualified Security Assessor working for Kingston Smith Consulting LLP.**

---

#### **About Kingston Smith Consulting LLP**

Kingston Smith Consulting is the specialist consulting practice of 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 [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