

## **PCI Compliance – do you know enough?**

There is still some confusion over the role of PCI in the retail industry. How it works, what it means, and the effects of non-compliance are yet to be made as clear. In this article, Umer Ayub, Director of Risk at Transaction Network Services (TNS) provides the low-down on what PCI means to those involved in the payment card chain.

PCI stands for Payment Card Industry. The recent alignment of Visa's Account Information Security (AIS) and MasterCard's Site Data Protection (SDP) Programmes has led to the formation of a worldwide standard for consumer data protection across the payment industry, known as the Payment Card Industry Data Security Standard (PCI DSS).

Failure to protect account and transaction information may result in financial and/or reputation loss due to fraud or a decrease in business caused by lower consumer confidence. Fraud and the reporting of fraud cases, such as the compromising of up to 40 million credit card accounts by a US-based payments processor in July 2005, has put consumers on high alert. Fighting hard not to lose consumer confidence, the payment card industry has introduced several methods of fraud minimisation, not least of which is the PCI DSS. The purpose of PCI DSS is to ensure that card scheme members and their merchants and payment service providers improve their data security measures to safeguard cardholder account and transaction information.

Still in its infancy and up against stiff competition for attention as Chip & PIN remains high on the agenda, PCI DSS is nonetheless an important global security standard, which retailers of all sizes and their service providers can ill afford to ignore. The requirements affect all companies that store, transmit or process Visa or MasterCard cardholder data.

## **Regulation**

Although the original deadline for compliance with PCI DSS was set as 30th June 2005, the number of certified companies remains low, with even some major acquirers not yet PCI DSS certified. This could be due to a lack of clarity throughout the industry as to who is responsible for education and enforcement of the standard.

Regulation falls to the card schemes, being Visa and MasterCard. However, the card schemes' members – the banks that sign merchants up as Visa retailers, for example – also have a role to play in ensuring that their sponsored merchants are PCI DSS certified. In addition, these members and merchants in turn should only buy payment related services from PCI DSS certified service providers.

Visa and MasterCard may choose to impose financial penalties on members who are non-compliant with PCI DSS. In extreme cases, these card schemes may prohibit companies from accepting their payment cards.

One of the benefits of PCI DSS for card scheme members and their merchants and service providers is that it provides a benchmark for assessing their data security and that of their business partners. In addition, PCI DSS provides a single process to comply with Visa and MasterCard data security programmes. This should result in lower compliance costs and effort, leading to a wider acceptance of standard security requirements for the industry.

## **Certification**

The compliance requirements of PCI DSS, as set out by Visa and MasterCard, not only apply at entity level but also at system components level. This includes any network components, servers, or applications included in, or connected to, the cardholder data environment. So, if you're a member, merchant or payment

service provider thinking about security, you need to make sure that all of your systems involved in payment card processing are PCI DSS compliant.

While all in scope companies must comply with the same PCI DSS rules, the extent of audit required to prove compliance varies according to the size of the company. The smallest merchants may only have to self-certify, whereas the members and the larger merchants and payment service providers must arrange an annual external audit and quarterly external network scans of their hosts with a Visa-approved Qualified Security Assessor (QSA).

The PCI DSS requirements, as defined by Visa and MasterCard, involve:

- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management programme
- Implementing strong access control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy

What is important for in scope companies is how the Visa and MasterCard cardholder data in their possession is stored, transmitted and processed. With the broadband revolution enabling organisations to take better advantage of alternative solutions for their communications infrastructure, global data security standards, such as PCI DSS, will always be high on the corporate agenda.