

# Industry voices concerns over PCI DSS compliance regime

Jun 02 2011

By Wietske Blees, regulatory analyst, Australia & New Zealand

Cardholder security is too complex a topic to be left to merchants, industry figures have warned, as the deadlines for Payment Card Industry Data Security Standard (PCI DSS) compliance begin to loom for businesses that handle credit card transactions. According to Jost Stollmann, chief executive at Tyro Payments in Sydney, it is too much to ask small-to-medium-sized businesses to develop the in-house expertise required to guard against sophisticated methods of fraud and data collection.

"The banking industry is wrong, if it thinks that it can shift the burden and risk of data security and compliance to the merchant community, when even the security specialists struggle. The banks' recent efforts go into this direction and presuppose that merchants can and will become experts in SSL connection, firewalls and encryption," he said.

In recent months, data breaches at a number of companies — ranging from electronics giant Sony, to an undisclosed Australian merchant, which forced a number of the four majors to cancel and re-issue thousands of credit cards — have illustrated that card security remains a vital component of risk and compliance. Similarly, news that security solution expert RSA itself was subject to an "extremely sophisticated cyber-attack", which comprised the organisation's own internal anti-hacking software, shows that hackers are often one step ahead of security experts.

Fraud on payment cards is a multi-million dollar problem that shows little signs of slowing down, according to the Australian Payments Clearing Association. APCA says that fraud on all payments cards across Australia has risen from 33 cents to 35 cents in every A\$1,000, although this is still low by international standards. With a constant flux of new innovations in the payments space, resulting in an increase in data storage locations, protecting a business against data fraud is becoming increasingly complicated.

At the moment, the main line of defence is an industry forum dubbed the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc in 2006. The forum has established a set of standards which form the technical requirements of the data security compliance programs with which banks and merchants will be required to comply. Although not legally enforceable, the credit card companies in question are able to fine non-conformers and cancel their access to the network if they refuse to cooperate. For businesses to lose access to all of the major card schemes' networks would be a potentially devastating blow that should ensure compliance with the standard, according to the PCI Security Standards Council.

The objective of PCI DSS is principally to bring merchants up to speed with best practice on PCI compliance, rather than dish out penalties. Any enforcement and penalties are carried out by the individual credit card brands. In terms of responsibility, it is the acquirer (typically a bank or entity that processes their payment card transactions) that is responsible for ensuring merchants meet the requirements, according to industry figures.

One Sydney-based consultant said that acquirers would need to demonstrate to the payment brands, or credit card companies, that their merchants were compliant as a "condition of use".

"PCI compliance is typically organised via a top-down approach. The payment brands develop, track and enforce compliance. The PCI Security Standards Council maintains the standards and validation requirements for PCI professionals. Acquirers are responsible for their merchants compliance, they ensure merchants understand PCI DSS compliance; tracking, mandating and report status on compliance, and can incur fine or penalties for non-compliance from payment brands. The merchant must maintain on-going PCI compliance of their systems, policies and operational procedures via annual validation, where required by Qualified Security Assessors (QSA)," the source explained.

But according to Stollmann the extent and sophistication of the problem is such that it cannot be left to merchants to guard against fraudsters. Instead, the onus should be on banks to provide safer EFTPOS methods and electronic payment solutions that do not expose sensitive data beyond the banks' secure sphere, he said.

"Banks should focus on making the product safe. One obvious example would be to limit the number of locations in which data is stored, and to store the data in a place where it can be adequately protected. In simple terms, that means that sensitive cardholder data should stay within the bank's secure sphere. Integrated EFTPOS, online and mobile payments must be designed in a way that quarantines financial transaction traffic. This would in turn protect sensitive cardholder data from exposure to the merchant's POS system, computer network and other networked devices," Stollmann added.

According to the consultant in Sydney, the PCI DSS requirements will end up being beneficial to merchants as well as the credit card industry in general. He agreed with Stollmann, however, that data storage was a greater area of vulnerability than the data transmission stage.

"I wouldn't call the requirements a burden — they are part of conducting a responsible business and it is possible to outsource or minimise PCI compliance requirements, by web payment hosting, tokenisation or simply not storing, processing or transmitting the Primary Account Number. However, given that business network configurations are more complex with a need to have greater systems integration, a higher degree of security measures are needed at various strategic points to safeguard sensitive data. There is no doubt that a solution that ensures a merchant does not need to store data would significantly reduce fraud risk. That, in turn, would limit the amount of time and effort a merchant would need to spend on remaining PCI compliant," the source said.