

Retailers and banks face security deadline

Visa sets February deadline for payment card security regime

By Stephen Bell Wellington | Monday, 17 November, 2008

Banks and retailers will need to bring their technology and payment processes up to date to manage a looming credit card security deadline early next year.

Visa has set a deadline of February for Australian and New Zealand merchants accepting credit cards to adhere to a security standard promulgated in the US in late 2006. The payment card industry data security standard (PCI DSS) was formulated two years ago by five major credit-card companies.

PCI DSS sets standards for the merchant's site for network security, protection of stored cardholder data, anti-virus and anti-spyware precautions and security of applications, physical and computer access control measures, monitoring and testing of networks and information security policy.

Merchants are required to regularly self-assess compliance in some areas and have a quarterly network scan undertaken by an independent security company. Merchants processing more than six million transactions a year must file an annual compliance report.

Local banks and merchants, however, appear relaxed about the issue. Computerworld's inquiries over the past two months about PCI DSS have met with no comment from banks or a bland assurance in the case of National and ANZ banks that they are "working with merchants and service providers to ensure compliance".

The Bankers Association, meanwhile, said in September that it "does not actively manage any work programme in this area".

Visa says it will require confirmation by 30 September, 2009, that merchants processing more than one million transaction a year "do not retain sensitive payment card data such as full magnetic stripe (also known as track data), security codes or PIN data after transaction authorisation."

Visa spokesman Andrew Woodward says the card companies are bringing standards into line across the world. Standards have existed before, but have been different in their detail in different regions, he says.

The Retailers' Association has been informed, he says, and will approach its members on PCI DSS, but the association could offer no comment on the detail of such an exercise by Computerworld's deadline.

Penalties for non-compliance are a matter between banks and retailers, says Woodward, but may include fines and a shifting of responsibility on to the retailer for fraudulent transactions.

"Compliance with PCI DSS is vital to ensuring the integrity of the global payments system," says Mike Smith, Sydney-based regional head of Risk Management, Asia Pacific for Visa.

"Aligning compliance programmes across the Visa regions is the latest step in our commitment to safeguarding cardholder data. In Asia Pacific, apart from implementing these new global mandates and launching a registry of service providers, Visa has run several merchant and client training sessions — most recently in Australia and Japan — to bring local partners up to speed with the new compliance requirements."