

topstory



Printed June 24, 2008 02:28pm AEST

Finance companies slap fines on retail

Karen Dearne | June 24, 2008

CREDIT card companies have begun fining local retailers who do not comply with the Payment Card Industry's data security standard, an industry expert says.

Howard Glavin, manager of IBM/ISS's PCI service delivery, said fines for non-compliance in Australia had started at \$5000 per company, per month, with a \$75,000 monthly fine levelled against one merchant.

There had been no public disclosure of the fines to date, because of commercial confidentiality requirements imposed under card scheme rules.

Until now, Mr Glavin said, the banks and the acquirers - intermediaries between card companies and the merchants - had been absorbing the costs.

"In the US, fines are right now running at about \$50,000 per company, per month, and they'll go on increasing," he said.

"If you're a big company, that may not be a whole lot of money, but if you're a medium-size company it may be the difference between profitability and going out of business."

The card companies intended to keep increasing the pain until banks could no longer afford the fines and pushed merchants to improve their customer information handling, he said.

Commonwealth Bank industry and alliance general manager Stuart Woodward said the bank was unaware of any fines being levied by card schemes.

"It is our understanding that merchants not able to demonstrate compliance by the end of this year may risk being fined in 2009," he said. "We are unaware of any specific program to do so."

"Reviews of merchant compliance are quarterly, and if an assessment was made, the fine would be levied quarterly, and the amount would depend on the volume of transactions."

Mr Woodward said the Commonwealth Bank had been successful in engaging merchants in PCI compliance.

A MasterCard spokesman yesterday said it could not provide details "regarding the frequency or amount of assessments it levies".

"We have received, and continue to receive, interest and support from local merchants, and uptake has been positive so far," he said.

However, a hint of the coming pain has been revealed by Visa in its latest financial statement. Visa reports an additional \$US14 million in revenue over the six months to March 31, "from fines associated with our Cardholder Information Security Program for acquirers whose merchants have not yet met compliance standards".

Visa Australia manager Ian McKindley said the card firm had focused on e-commerce merchants, particularly those handling more than 20,000 transactions a year. "They've made good progress," he said.

"We've also been working to achieve compliance among payment service providers."

Visa recently announced that 84 payment providers handling Visa account information in Asia and the Pacific have been certified as fully compliant with PCI DSS, up from 31 last year.

Rick Logan, NetIQ's chief technical specialist on data security compliance, said there had been a "renewed focus on PCI-related projects" in the past two months. "Some companies have been able to absorb smaller fines because it's cheaper than putting in a proper solution," he said.

"Obviously, people don't want to share the fact they're paying fines, but some certainly want to get PCI as quickly as possible."

To comply with the PCI standard - developed by Visa, MasterCard and American Express and mandated through contractual obligations - merchants have to adhere to a 12-point security plan and undergo rigorous audits. Retailers, e-commerce sites and customer facing businesses such as telcos should already be compliant with PCI version 1.1, introduced in September 2006. Version 1.2 is due for release in October.

Mr Glavin said Australia had not yet experienced a serious exposure of card data, "but one large breach and paranoia will hit very quickly".

According to the database maintained by the Privacy Rights Clearinghouse, more than 230 million records held by US businesses and government agencies have been exposed in breaches there since early 2005.

An ANZ spokeswoman said the bank provided support to ensure its merchants' systems complied with requirements.

Retail giant Coles said a card security compliance program had been in place there for several years.

Copyright 2008 News Limited. All times AEST (GMT +10).