



Briefing 27 May 2011

Tyro warns against merchant ‘witch hunt’ – Cardholder security is foremost a banking problem, not a merchant problem

Last week, the media reported that a data breach at a merchant forced CBA, NAB, Westpac and St George to cancel and re-issue thousands of credit cards. The attention then turned to finding which merchant was to blame.

The banking industry has undertaken efforts to heighten security, successively replacing their legacy EFTPOS terminal fleets with a new generation of terminals and integration software that encrypt the data. Additionally, they now issue their credit and debit cards with new chip technology that greatly improves security. Visa and MasterCard have also introduced new security features for online acquiring.

But security is a moving target. Fraudsters are constantly adapting and finding new weaknesses to attack, becoming more sophisticated in the process.

The challenge now posed by security was highlighted by Sony PlayStation Network’s huge data breach. Recently, the world’s leading security solution provider, RSA, admitted to an “extremely sophisticated cyber-attack” compromising the own internal anti-hacking technologies.

On top of this, recent announcements have foreshadowed new payment solutions that capitalise on the increasing preponderance of smartphones and ever-present broadband access. The predicted torrent of new devices and new applications, together with the massive accumulation of data, could all be used to allow targeted marketing and electronic payments, anytime and anywhere. But who will be responsible for collecting, transporting, holding and protecting the data?

Tyro believes 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.

However, standards, compliance and penalties on merchants are not the answer. The problem of cardholder and financial transaction data security belongs to the banks, not the merchants. Banks must offer their merchants safe EFTPOS products and electronic payment solutions that do not expose sensitive data beyond the banks’ 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.

“In the banking industry, we have to recognise that cardholder security is our problem. We own it and we have to think hard about how best to protect merchants and consumers against the growing number of vulnerabilities uncovered as payments become more complex and integrated, more online and mobile”, said Jost Stollmann, CEO of Tyro Payments.

tyro payments limited
abn 49 103 575 042
125 york street
sydney nsw 2000
p+61 2 8907 1700
f+61 2 8907 1777
h+1 300 966 639
www.tyro.com



About Tyro Payments Limited

Tyro is Australia's EFTPOS innovation institution and is the first new entrant into the EFTPOS business in over 14 years. Tyro holds an authority under the Banking Act to carry on a banking business as a Specialist Credit Card Institution (SCCI) and operates under the supervision of the Australian Prudential Regulation Authority (APRA). Under this authority Tyro provides credit, debit, EFTPOS, gift and loyalty card acquiring and Medicare claiming and rebating services, but may not take money on deposit.

Tyro's transparent payment solutions are uniquely merchant focused, enabling reduced fees, greater productivity, better cost management and a superior payment experience for consumers.

Tyro is a wholly Australian-owned company with no external venture capital. The company has been fully funded by the Executives, Directors, independent and strategic investors.

Fiona Stollmann

+61 2 8907 1772

+61 424 369 632

fstollmann@tyro.com