SUBMISSION NO. 12

MembersEquity Bank

Members Equity Bank Pty Ltd ABN 56 070 887 679
Level 16, 360 Collins Street Melbourne VIC 3000
GPO Box 1345 Melbourne VIC 3001
t 03 9605 6000 f 03 9605 6999
w www.membersequitybank.com.au
AFS Licence: 229500

26 June 2009

The Secretary
House of Representatives Standing Committee on Communications
R1-109, Parliament House
PO Box 6021
Canberra ACT 2600

BY EMAIL: coms.reps@aph.gov.au

Submission – Inquiry into cyber crime

Thank you for your letter dated 26 May 2009 seeking Members Equity Bank's (MEB) views in relation to the terms of reference of the above inquiry by the House of Representatives Standing Committee on Communications.

We appreciate the opportunity to provide our input into this inquiry. Online or electronic banking services are an extremely important part of our business model in terms of its acceptance and usage by our current and future customers. In addition, MEB is an interested stakeholder from the perspective of its liability for any associated fraud losses.

Our thesis is that the real threat from cyber crime in relation to electronic banking is at the consumer's end (eg personal computers or mobile devices). Banks are equipped to defend against this threat, however the challenge is with consumers being able to do the same.

MEB's assessment of the overall impact for customers, as well as recommendations to address are described below in the context of the terms of reference for the inquiry:

a) **Impact of malicious software such as viruses and trojans**

MEB is able to block a large amount of spam email from entering the organisation's internal network by employing security gateways at the perimeter. The vast majority of emails are blocked at the gateway through a method of determining the reputation of the sender. The percentage emails that actually contain malicious software is unknown as further analysis of the email is unnecessary once a bad reputation is determined. As a consequence, MEB detects and reports a very small number of viruses at the gateway.

MEB is aware that its customers are regularly targeted by malicious viruses and trojans. Typically, these attacks have resulted in relatively small claims for compensation against MEB. As the criminal network expands and becomes more professional, consumers are going to become increasingly susceptible to complex and targeted attacks from viruses and trojans. As a consequence, banks are under increasing pressure to protect their customer's online transactions rather than the traditional method of just bolstering defences in their own data centres and systems. It is likely to become increasingly challenging to provide a seamless and simple to use banking experience that attracts and maintains customer usage of the online service and ensure that the services can be used securely.

b) The growing economic and security impact of botnets

Similar to other institutions, botnets used for malicious purposes have an impact on MEB in the form of spam email and/or denial of service attacks. Banks have no control over the amount of infected email reaching their customers that contains malicious software links.

In many cases, customers will be subject to a social engineering attack that ultimately causes their workstation to become part of a botnet. This is difficult to control for the reasons stated above and again relies on customer awareness and willingness to protect themselves when online.

The proliferation of spam from botnets has also had an effect on the banking industry in the form of methods of communication. Many banking institutions now attempt to differentiate themselves as legitimate communication by never sending links or functional code in an email. This limits the low cost marketing opportunities that email offers.

c) Awareness of e-security risks in the Australian community

The general awareness of the risks associated with online banking is well known throughout the community, although a deeper understanding of the issues is still very much lacking. This has a two fold effect:

- Consumers will not use online banking because they perceive it to be completely unsafe.
- People will use online banking but not be secure.

Government initiatives such as e-security awareness week have educative merit and MEB believes the advertising reach of this initiative has room to expand to encompass the wider community.

d) Measures currently deployed to mitigate e-security risks by Australian consumers

MEB sees its primary role as protecting consumer funds put on deposit, loss of which can come from either direct attacks against MEB itself or its customers.

To guard against direct attacks, MEB has a dedicated Information Technology security function staffed by industry experts. This department is responsible for maintaining an awareness of current and emerging threats and ensuring that ME is well placed to defend such threats.

MEB's approach to the customer threat has been to warn our customers through general awareness initiatives as well as awareness initiatives relating to specific threats. However, technologies and methods to protect the customer outside of the bank's realm of control are still largely the responsibility of the end user and their willingness to keep abreast of the issues remains the biggest challenge.

e) Future initiatives to mitigate e-security risks (includes also (f) emerging technologies)

The complexity in securing one's workstation or mobile device can often be overwhelming for someone not familiar with the technology or threats that they face online. The process of securing must be as simple as possible to ensure a high level of uptake. This could be achieved by embedding security within applications and operating systems that protect online transactions. This approach could essentially enforce a minimum level of security used by customers and avoids them not having any level of security at all.

MEB believes that some form of two factor authentication will become the norm for all banking institutions within the next few years. However, a higher level of security will be achieved through invoking a 'sandbox' environment while the customer is transacting online that disallows all running

services except those explicitly required for the online banking session. This appears to be the best method of protection against viruses, trojans and other malware and the expectation is that the uptake of this technology will increase as it matures.

Smaller financial institutions often rely on the larger banks to implement new and innovative security technologies to test acceptance in the market. Communication lines between government and financial institutions is a critical aspect in e-security risk mitigation as this would foster stronger development of initiatives that meet requirements demanded by online banking customers.

Further information
ME Bank would be pleased to provide any further information or clarify on any aspect of this submission.

Yours sincerely

David Tennant
Chief Risk Officer
Members Equity Bank Pty Ltd