SUBMISSION NO . 52

ASIC
Australian Securities & Investments Commission

No. 1 Martin Place, Sydney
GPO Box 4866 Sydney NSW 1042
DX 653 Sydney

Telephone (02) 9911 2680

Malcolm Rodgers
Senior Executive, Strategy

1 July 2009

Mr Jerome Brown
Acting Committee Secretary
House of Representatives Standing Committee on Communications
Department of the House of Representatives
By email: coms.reps@aph.gov.au

Dear Mr Brown

Inquiry into cyber crime

Thank you for inviting The Australian Securities and Investments Commission to make a submission to the Inquiry into cyber crime and its incidence and impact on consumers. We do not propose to make a submission to the inquiry, but below is some general background information that may assist the Committee.

Nature and prevalence of e-security risks, including financial fraud and theft of personal information

The Australian Consumer Fraud Taskforce (ACFT), of which ASIC is a member, commissioned the Australian Bureau of Statistics (ABS) to conduct a survey of personal fraud in Australia in 2007 (the results were published on 27 June 2008). The final sample was 14,320 persons (with a response rate of 89%), so we regard the result as reliable.

The ABS concluded that phishing and related scams affected 57,500 victims in Australia. Identity fraud accounted for nearly half a million Australian victims, 77% of whom were a victim of credit or bank card fraud, although the majority of these frauds were still committed in person or by telephone rather than through the internet. Identity theft accounted for 124,000 of the 499,500 victims of identity fraud.

The full results of the ABS's research are available from the ABS website under catalogue number 4528.0.

ASIC's involvement with the ACFT goes back to 2005, when the ACFT was formed with nineteen government consumer protection agencies from Australia and New Zealand, who work together with partner agencies from the private, public and community sectors to conduct annual information campaigns on consumer fraud.

Measures currently deployed by ASIC to mitigate e-security risks faced by Australian consumers

Website on identity theft

ASIC has, with the Australian Bankers Association and the Australian High Tech Crime Centre (AHTCC), developed a website on identity theft to combat identity theft and help Australian consumers protect their finances. This website contains advice on simple security steps, fact sheets and an online quiz to educate consumers about protecting themselves online.

FIDO website

ASIC maintains a consumer information and education website called FIDO. FIDO's page on identity theft includes tips on protecting financial identity, information for consumers who have suffered identity theft and links to the 'Protect Your Financial Identity' website. FIDO's page on fraudulent emails provides information about how email fraud works, spyware, and trojans as well as safety checks. In addition, ASIC sends a FIDO e-newsletter alert to over 15,000 consumers every month. Consumers can register online to receive this email alert.

EFT Code

ASIC administers the Electronic Funds Transfer (EFT) Code, which regulates consumer ATM and EFTPOS transactions, card-not-present credit card transactions, telephone and internet banking, stored value cards and other stored value products. The EFT Code is a voluntary industry code of practice covering all forms of consumer electronic payment transactions. Thus, the Code only applies to businesses that subscribe to it. The great majority of banks, building societies and credit unions do subscribe. ASIC's role in administering the Code includes periodically reviewing it and associated administrative arrangements. ASIC is currently reviewing the Code.

The Code protects people who are victims of online fraud involving their credit cards. This regime for allocating liability for alleged unauthorised transactions is central to the Code. Currently, the principal burden is borne by the institution rather than the consumer, on the basis that institutions are better placed to reduce system insecurity at the lowest cost. Consumers have an incentive to take reasonable steps to protect the security of their passwords, as they may lose the 'no fault' threshold of $150 if they do not. This liability regime is one of the most closely scrutinised areas in the Code, so as part of ASIC's review of the Code we consulted on whether the liability regime should be adjusted in view of the growth of online fraud directed at individual users and their equipment.

ASIC released a Consultation Paper in January 2007 (CP 78: *Reviewing the EFT Code*) which addressed the issue of whether consumers should be exposed to additional liability for unauthorised transactions arising from malicious software or 'phishing' attacks. ASIC strongly supports the current rules with respect to liability for unauthorised transactions. Submissions on the CP from consumers, external dispute resolution schemes and industry all supported the current regime and opposed modifying the rules for allocating liability for unauthorised transactions. Reasons for maintaining the current liability rules include:

- Home computers were not designed as secure platforms, so it is impossible to prevent all online fraud;
- Unlike subscribers, consumers do not necessarily have the skills or resources to implement adequate online security;
- Determining liability would involve extensive forensic analysis that would outweigh any benefit; and
- Imposing additional liability on consumers would undermine community trust in online banking.

External dispute resolution schemes

Consumers who have a dispute with their Authorised Deposit-taking Institution (ADI) about unauthorised transactions may complain to a free ASIC-approved external dispute resolution scheme, the Financial Ombudsman Service (FOS). Before resorting to the FOS, the consumer must lodge a complaint with their ADI and allow 45 days for a response. The types of disputes heard by the FOS and the available remedies are set out in its terms of reference, which are currently under review by ASIC.

ASIC is happy to provide any further assistance the committee might require. Please contact Ailsa Goodwin on (03) 9280 3439 if you require further information.

Yours sincerely

Malcolm Rodgers
Senior Executive, Strategy