

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
ATTORNEY-GENERAL'S DEPARTMENT

Output 2.1

Question No. 54

Senator Ludwig asked the following question at the hearing on 24 May 2006:

In relation to the article in the *Australian Financial Review* of Thursday, 20 April 2006 discussing cybercrime:

- (a) What activities are underway in any specific response to the article?
- (b) Has the Australian Communications and Media Authority been contacted?
- (c) Are any new offences or criminal justice issues being considered in this area from the AG's perspective?

The answer to the honourable senator's question is as follows:

- (a) The Australian Government is aware of the ebay sponsored report 'Addressing Phishing: A Multi-Layered Approach' as mentioned in the article.

The Australian Government has developed a multi-faceted national strategy to combat hi-tech crime, including internet banking fraud, credit card fraud, and related identity crime (including 'phishing'), in partnership with industry and the community. These activities are ongoing.

A key challenge of the national strategy is to put in place rigorous procedures and practices that minimise cybercrime while still facilitating legitimate business operations.

The Minister for Justice and Customs regularly holds meetings with representatives of the finance sector as part of an effective partnership to enhance the security of Australia against credit card and internet banking fraud. These meetings have resulted in a number of significant legislative and operational initiatives. These meetings have proved to be a critical forum for developing innovative responses to emerging fraud threats.

Key Government agencies, including the Attorney-General's Department (AGD), the AFP, and the Australian High Tech Crime Centre (AHTCC) are working closely with the financial sector to develop more effective measures to protect Australians from credit card and banking fraud. A Joint Government and Financial Sector Information Security Taskforce is looking at a range of security and communications issues. These include procedures for government, law enforcement agencies and the financial sector to receive early notification of credit card breaches.

Recent responses to international breaches of credit card accounts have highlighted how well this partnership and financial fraud prevention processes work in Australia. The investment in prevention and detection systems in Australia has helped to uncover data compromises of credit card information which have occurred in a number of countries overseas, thereby reducing the risk to Australian cardholders.

On 20 May 2004, Australia launched the Joint Banking and Finance Sector Investigations Team (JBFSIT). This team is a public/private partnership between the ATHCC and the banking and

finance sector to investigate instances of high tech financial crime. The JBFSIT comprises of police investigators, intelligence analysts and seconded personnel from each of the five largest Australian banks. The Government believes this is the most comprehensive national response to internet banking fraud initiated worldwide.

In March 2005 Australia established the Australasian Consumer Fraud Taskforce (ACFT) to provide a national coordinated response to prevention and enforcement action around consumer related fraud. The ACFT is composed of 18 Commonwealth, State, and Territory government regulatory agencies and departments, and is chaired by the ACCC.

In February/March 2006 Australian governments (through the ACFT) launched a national consumer fraud awareness campaign as part of the International Consumer Protection and Enforcement Network (IC PEN) Global Fraud Prevention Month. Nineteen Private sector organisations were also partners in the campaign – they included all the major banks, credit card companies, credit unions and major insurance companies, together with 13 community groups. (Further details can be found on the ACFT website www.scamwatch.gov.au). This will be an annual event with a different focus for each year.

(b) The Australian Communications and Media Authority is a member of the ACFT. The ACFT is aware of the report ‘Addressing Phishing’ as part of its coordinated response to consumer fraud.

The purpose of the ACFT is to work to enhance the Australian and New Zealand Governments’ enforcement activity against frauds and scams by:

- undertaking an annual coordinated consumer fraud awareness and prevention campaign, in partnership with the private sector, timed to coincide with Global Consumer Fraud Prevention Month
- developing innovative and coordinated approaches to preventing and responding to incidents of consumer fraud when they do occur, and
- raising the profile of consumer fraud in terms of developing, commissioning and conducting research into the problem.

Member agencies of the ACFT include:

Australian Government

Attorney-General’s Department
Australian Bureau of Statistics
Australian Communications and Media Authority
Australian Competition & Consumer Commission (Chair)
Australian Institute of Criminology
Australian Securities & Investment Commission
Australian Federal Police (represented by the Australian High Tech Crime Centre)
Department of Communications, Information Technology & the Arts

New Zealand Government

NZ Commerce Commission
Ministry of Consumer Affairs

State and Territory Governments

Australian Capital Territory Office of Fair Trading
Consumer Affairs Victoria
New South Wales Office of Fair Trading
Northern Territory Department of Justice
South Australian Office of Consumer & Business Affairs
Tasmanian Office of Consumer Affairs & Fair Trading
Western Australian Department of Consumer & Employment Protection

(c) The Australian Government is continuing to undertake a number of ongoing activities, as outlined above, to combat cybercrime and internet banking fraud. The Australian Government has introduced a range of legislation to help combat fraud, including the recent introduction of personal financial information offences.

A person who dishonestly obtains or deals in personal financial information to access funds, credit or other financial benefits within Australia is now subject to the offences contained in Part 10.8 of the *Criminal Code Act 1995* introduced in the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2004* – which came into force on 28 September 2004.

Australia's new *Proceeds of Crime Act 2002* came into operation on 1 January 2003, and provides a scheme to trace, restrain and confiscate the proceeds of crime against Commonwealth law.

The Act provides for two streams of recovery action: a conviction based stream, and a civil based stream under which recovery action can be taken independently of the prosecution process. The new Act also provides a scheme that provides for confiscated funds to be provided back to the Australian community, in an endeavour to further prevent and reduce the harmful effects of crime in Australia.

Other relevant legislation Australia has recently introduced to prevent and combat the effect of fraud on the Australian Community include:

- the *Spam Act 2003* and the *Spam (Consequential Amendments) Act 2003*
- the *Cybercrime Act 2001*, and
- the *Commonwealth Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*.