PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSON

(Inquiry into the Future Impact of Serious and Organised Crime on Australian Society)

Senator Bishop asked the Attorney-General's Department, upon notice, on 5 July 2007 for additional information on what data relating to incidences of finance fraud over the internet is available.

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

The Australian Bureau of Statistics has undertaken to conduct a survey of Personal Fraud victimisation in Australia on behalf of the Australasian Consumer Fraud Taskforce. The questions aim to answer data needs relating to the prevalence and impact of identity theft and scams in Australia, such as phishing, lotteries, pyramid schemes and chain letters. The Personal Fraud dress rehearsal was conducted in February-March 2007, and the survey will be in the field between 1 July 2007 and 31 December 2007. Preliminary data is scheduled for release by 31 March 2008, with final data expected to be released by mid-2008.

In 2004, the Australian Institute of Criminology (AIC) undertook a survey investigating the extent of online credit card fraud against small businesses in Australia. That report is available online at: http://www.aic.gov.au/publications/rpp/60/executiveSummary.html

Later this year, the AIC will be undertaking a survey of 20,000 businesses across all industry sectors in Australia to determine the extent and impact of computer security incidents. This study, Project ABACUS, will be the first representative study of its kind and will collect information specific to the experiences of Australian businesses on computer security. The study will be conducted during August and September 2007. Further information about Project ABACUS is available online at http://www.aic.gov.au/research/projects/0133.html.

Other Australian surveys which include some information on Internet-related fraud (broadly defined) are listed below. It should be noted that these articles are broadly related to internet fraud, though they may focus specifically on computer facilitated financial fraud, credit card fraud or on computer fraud more generally.

- Australasian Consumer Fraud Taskforce *Online Survey, March 2006* – Information on this survey is available in the following article; Smith, Russel G. (AIC) 2007. 'Consumer scams in Australia: An overview', *Trends and Issues in Crime and Criminal Justice, No. 331*. This publication can be accessed at http://www.aic.gov.au/publications/tandi2/tandi331.html

- Quantum Market Research, *AustraliaSCAN 2006: Monitoring Cultural Change*. Melbourne. This publication is available via subscription from http://www.qmr.com.au/australiaSCAN.html

- BDO Chartered Accountants and Advisers, 2006. *BDO Not-for-Profit Fraud Survey*. Brisbane: BDO. This can be accessed by contacting http://www.bdo.com.au/services/forensic-accounting/resources/notforprofit

- Information on the *2004 International Crime Victim Surveys* is available in the following article;
  Krone, T. & Johnson, H. 2006. 'Internet purchasing: perceptions and experiences of Australian households'. *Trends and Issues in Crime and Criminal Justice. No 330*. This publication can be accessed at http://www.aic.gov.au/publications/tandi2/tandi330t.html

- Information on the *2000 International Crime Victim Surveys* is available in the following article;
  Muscat, G., James, M. & Graycar, A. 2002. 'Older People and Consumer Fraud'. *Trends and Issues in Crime and Criminal Justice, No 220*. This publication can be accessed at www.aic.gov.au/publications/tandi/ti220.pdf

- Moustakas, Nick. 2006. 'Going, Going, Gone: Online Auctions, Consumers and the Law'. Melbourn: Communications Law Centre Ltd. This publication is available at http://www.comslaw.org.au/auction/GoingGoingGoneEXECUTIVESUMMARY26.7.06.pdf

---

Mr Kerr asked the Attorney-General's Department, upon notice, on 5 July 2007 for additional information on the regulatory frameworks surrounding telecommunications carriers cooperating with law enforcement agencies.

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

In giving evidence to the Committee, Assistant Commissioner Gregson of the Western Australia Police questioned the width of the legislation that obliges telecommunication carriers and carriage service providers to co-operate with law enforcement agencies. In particular, the Assistant Commissioner suggested that the legislation does not go far enough to oblige carriers and carriage service providers to provide assistance in a timely manner.

Section 313 of the *Telecommunications Act 1997* provides that carriers and carriage service providers must give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for enforcing the criminal law or safeguarding national security, among other purposes. Implicit in this is a requirement that the carrier or carriage service provider must provide any required assistance within a reasonable time, or within such a timeframe that permits the enforcement of the criminal law. If a carrier or carriage service provider unduly delayed the provision of any required assistance, then that carrier or carriage service provider would not be providing such help as is reasonably necessary for the

enforcement of the criminal law, and would therefore be in breach of the requirement of section 313.

Section 314 provides a basis for determining the terms and conditions on which help is to be given under section 313. Section 314 sets out the cost-sharing principle that a carrier or carriage service provider must comply with the requirement to give reasonably necessary help on the basis that it will neither profit from, nor bear the costs of, giving the help. Furthermore, section 314 provides that a carrier or carriage service provider must comply with the requirement to give reasonably necessary help on such terms and conditions as are agreed between the carrier or carriage service provider and the law enforcement agency or, failing agreement, as are determined by an arbitrator.

Neither the *Telecommunications Act 1997* nor the *Telecommunications (Interception and Access) Act 1979* (nor for that matter the Telecommunications ((Interception and Access) Amendment Bill 2007 which is currently before Parliament) include provisions that oblige all carriers and carriage service providers to provide assistance to law enforcement agencies within a particular set timeframe.

If a carrier has an obligation to provide help within a particular set timeframe it is because they have negotiated that timeframe as part of an agreement with the law enforcement agency on the terms and conditions on which help will be given, or because that timeframe has been set by an arbitrator who has determined the terms and conditions on which help is to be given.

(The Department of Communications, Information Technology and the Arts was consulted in the preparation of this answer).

Senator Bishop asked the Attorney-General's Department, upon notice, on 5 July 2007, how the privacy issues associated with law enforcement data being held on a single national database are different to the issues associated with that same data being held in six separate databases and being accessed.

Senators McDonald asked the Attorney-General's Department if these issues were related to the individual States and Territories having individual privacy legislation that is not compatible.

The answer to the honourable senators' questions are as follows:

The proposal to centralise a variety of law enforcement information into a single database raises a number of privacy issues. Dr Herriot from the Attorney-General's Department identified many of these issues at the hearing, and I refer the committee's attention to the evidence she provided.

"Certainly different jurisdictions have different privacy regimes. There are also issues of the purpose for which personal information was collected and concerns around possible data matching. They would all go to the underlying privacy. There

are different audit and accessibility requirements […]. There is also the time period within which certain information may be required to be destroyed if it had been collected for a certain reason. There is a nexus of issues. Certainly, gathering personal records in an administrative database for one purpose and then using them for an entirely different purpose would create privacy issues."

In response to the question raised by Senator the Hon Ian Macdonald, although the Australian Government's preference is for the harmonisation of privacy regimes and possible uniformity between jurisdictions, this has not been achieved to date. The Australian Law Reform Commission is currently reviewing the *Privacy Act 1988* and, as part of its terms of reference, is considering relevant existing and proposed Commonwealth, State and Territory laws and practices. It is likely that recommendations flowing from that consideration will be relevant to the question of a national regime.

Senator Parry asked the Attorney-General's Department, upon notice, on 5 July 2007:
How soon do you see this coordinated approach of databases communicating with databases interagency being completed?

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

The Department is not in a position to indicate to the committee when this process will be complete. However, a recent report to the NCTC confirmed that the range of strategies being employed to improve the flow of information for the purposes of law enforcement are already contributing to improvements in information and intelligence sharing.

Significant work has already been undertaken to improve information sharing processes. This work has arisen, in part, from the *Review of Information and Intelligence Sharing in the Aviation Sector* (Ford Review) which is being overseen by the National Counter Terrorism Committee (NCTC). The Ford Review found that the impediments to information sharing were primarily cultural rather than legislative. For cultural change to occur, legislative and policy impediments must be removed and processes and practices improved to encourage appropriate information and intelligence sharing.

In this context, the core recommendations of the Ford Review relate specifically to information sharing practices—including improving the use of existing databases, the development of interconnectivity in a secure environment, as well as the development of common formats for the collection and exchange of information. The NCTC has established a working group, chaired by Tasmania, to develop a plan for the coordinated implementation of these recommendations. As the recommendations have implications which are broader than the aviation sector, implementation is being considered in relation to the law enforcement environment more generally, with a range of short, medium and long term strategies being considered.

In particular, work is underway to improve the use of existing databases across the law enforcement community, most notably the Australian Criminal Intelligence Database (ACID). The utility of existing databases depends upon the extent to which participating agencies upload information. The Heads of Commonwealth Law Enforcement Agencies and the NCTC have agreed to support the use of ACID as the major system for sharing intelligence between Commonwealth, State and Territory law enforcement agencies. While the use of ACID is substantial and growing each year, it could be better utilised by some agencies, and work is underway to address this. Better utilisation of ACID will improve the sharing of intelligence with immediate effect, with ongoing work to raise awareness, and provide training where it is required.

Interconnectivity between databases is another initiative which is being progressed to improve information sharing. A number of law enforcement databases are already connected. Interconnectivity is a complex matter which needs to be considered on a case by case basis, as there is no 'one size fits all' solution to devising retrospective engineering solutions to interconnect disparate systems. The authority under which agencies collect, hold and use the information, including disclosure to other agencies, must also be considered.