Submission on 2009 Inquiry into Cybercrime

26 June 2009

Australian Bankers' Association Inc. ARBN 117 262 978
(Incorporated in New South Wales). Liability of members is limited.

Table of Contents

Inquiry into Cybercrime

1. Terms of reference

The House of Representatives Standing Committee on Communications is conducting an inquiry into:

"the incidence of cyber crime on consumers:

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans;

b) The implications of these risks on the wider economy, including the growing economic and security impact of botnets;

c) Level of understanding and awareness of e-security risks within the Australian community;

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

i) Education initiatives

ii) Legislative and regulatory initiatives

iii) Cross-portfolio and inter-jurisdictional coordination

iv) International co-operation;

e) Future initiatives that will further mitigate the e-security risks to Australian internet users;

f) Emerging technologies to combat these risks."

2. Introduction

The Australian Bankers' Association ("**the ABA**"), the peak body for banking in Australia, is pleased to contribute to the House Standing Committee on Communications' Inquiry into Cybercrime.

3. Scope and Overview of ABA's Submission

The ABA's submission focuses on matters relating to items "d" and "e" of the Terms of Reference.

We have noted the other items and believe that many of the matters may have already been addressed by the Government's E-Security Review.

The primary objective of our Members in this submission is to identify where the banking sector can work with Government to support a framework that will facilitate a more effective environment in which both Government and our Members can work to detect, prevent and respond to Cybercrime incidents affecting Australian internet and telecommunications users, such as our Members and their customers.

The ABA makes submissions to the Inquiry under the following key points:

- Implementation of the 2004 Cybercrime Inquiry's Recommendations;
- Framework for combating Cybercrime (national and international) (including imposition of penalties for the commission of Cybercrime);
- Education and Awareness Campaigns by Government;
- Government collaboration with the banking industry;
- Identification of emerging threats and allocation of sufficient budget by the Government for combating threats, including strategic risk planning by the Government.

4. Definition of Cybercrime

Cybercrime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime.

Cybercrime could also broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

In the Council of Europe's *Cybercrime Treaty*[1], Cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. This wide definition of Cybercrime overlaps in part with general offence categories that need not be ICT-dependent[2], such as white-collar crime and economic crime.[3]

The Australian Institute of Criminology ("**the AIC**") has provided a definition of Cybercrime as including two main categories:

- crimes in which information and communications technologies are the target of offences (eg computer vandalism and viruses), and
- crimes in which technologies are used as tools to commit an offence (such as computer hacking).

The important thing is to recognise that a Cybercrime may be just one component of a much broader course of criminal conduct, some of which may well fall outside the range of offences provided for at the Commonwealth level (and may be regulated either by other sovereign states or by the Australian States). We do not believe that this has been sufficiently recognised by Australian Governments (both State and Federal) to date.

---

[1] (ETS No. 185).
[2] Information and Communication Technology.
[3] As described in Grabosky P & Sutton A, *Stains on a white collar,* Sydney, Federation Press, 1989.

5. Recommendations from the 2004 Cybercrime Inquiry and Report should be implemented by the Government

The ABA made detailed submissions to the 2004 Parliamentary Inquiry on Cybercrime ("**the 2004 Inquiry**").[4]

We believe that a number of the recommendations made by that Inquiry and contained in the Committee's Report were not implemented and that, if implemented, would deliver significant benefits to the Australian public, including our Members and their customers.

We highlight the following recommendations in particular:

> ***"Recommendation 3***
>
> *The Committee recommends that the Commonwealth Attorney-General liaises with the State and Territory Attorneys-General to ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime, which is in accordance with Australia's international obligations.*
>
> ***Recommendation 5***
>
> *The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service.*
>
> ***Recommendation 6***
>
> *The Committee recommends that the Australian Crime Centre, in consultation with the Australian High Tech Crime Centre (AHTCC), Austrac and other law enforcement agencies give priority to developing a national intelligence gathering strategy for cybercrime in the banking industry. Further the ACC should seek to fill any gaps in intelligence holdings that are identified.*
>
> ***Recommendation 7***
>
> *The Committee recommends that the Government include in its cybercrime strategy, directed training for law enforcement agencies, and the development of a whole of government approach in which individuals can gain expertise which can be shared between those agencies.*
>
> ***Recommendation 8***
>
> *The Committee recommends that the Australian Crime Commission continue its current level of involvement in cybercrime investigation, and intelligence gathering, as well as further developing its international liaison role.*

---

[4] Parliamentary Joint Committee on the Australian Crime Commission Report on Cybercrime, March 2004.

Recommendation 9

The Committee recommends that the Australian Crime Commission ensure its information sharing strategies, including liaison with the Australian High Tech Crime Centre, maximise the opportunities for giving and receiving accurate and timely information about cybercrime methods and technology.

Recommendation 10

The Committee recommends that the Australian Crime Commission seek out opportunities to participate in appropriate public/private sector cybercrime projects, to promote the sharing of information, and the efficient prevention and investigation of cybercrime offences.

Recommendation 11

The Committee recommends that the Australian High Tech Crime Centre act as a clearing house for information on cybercrime, in order to explore initiatives to combat it."

Each of these recommendations highlighted that there are critical interdependencies in the fight against Cybercrime on Australia's institutions and the community at large.

We believe that the Government must implement the recommendations from the 2004 Inquiry that remain outstanding and take a leadership role in the fight against Cybercrime both in Australia and offshore. To date, that has not occurred.

With respect to Recommendation 8 from the 2004 Inquiry, we recommend that the Australian Crime Commission increase its level of involvement to meet the threat. That involvement should also be reviewed on an annual basis.

6. Framework

The current framework covering Cybercrime may not be sufficiently effective in combating particular instances of Cybercrime.

6.1 National Issues

At a national level, the difficulties encountered do not appear to be so much based on legal (jurisdictional) restrictions relating to power to exercise functions (under the Constitution or as between agency based on their respective enabling statutes and powers conferred thereby) so much as they do to differing priorities between agencies on prevention, detection and prosecution activities (none of which are currently coordinated by any centralised mechanism).

So much was acknowledged by the 2004 Inquiry[5] and implementation of the recommendations from the 2004 Inquiry is, we believe, overdue.

[5] See the Parliamentary Joint Committee on the Australian Crime Commission's Report on Cybercrime, March 2004.

We believe that the current lack of coordination has a significant impact on the way in which Government and law enforcement agencies in Australia operating in this area approach the fight against Cybercrime.

In particular, there appears to be a need for more coordination and cooperation between agencies in sharing vital information and intelligence on risks (that is, prevention strategies).

We believe that, at present, the resources of both the Commonwealth and the States and Territories are not being used in the most effective manner to benefit Australians.

6.1.1 Consolidation of legal principles and policy approach and addressing jurisdictional issues

The 2004 Inquiry noted there were thirteen Commonwealth Acts of Parliament which had some regulatory relevance to Cybercrime in addition to the Legislation of the various States and Territories of Australia in the area.

The Committee noted that the legislation was not uniform, either in offence provision or in penalties.[6]

We do not believe that any review has taken place to date. Various provisions of the Model Criminal Code have, we believe, been sporadically and not necessarily consistently implemented across the Australian jurisdictions.

6.1.2 Penalties imposed in Australia

We believe that the current regulatory regime for dealing with Cybercrime is fragmented and complex. It lags behind the sophistication of criminal activity in this area and imposes penalties which are not proportionate to the benefits able to be obtained from being a party to a Cybercrime.

In 2004 Inquiry concluded:

> *"The Committee notes that there are at least two bodies which could address this lack of consistency, and promote a more focussed and unified approach to the investigation, detection and prosecution of cybercrime. They are: the Standing Committee of Attorneys General, and the Police Ministers' Council.*
>
> *The Committee is concerned that while there is no common cybercrime regime in Australia, there is an increasing likelihood of this weakness being exploited by criminal elements."*[7]

We agree with the Committee's view.

6.1.3 National Sentencing Database

We recommend that the Commonwealth lead the way in the roll out of the National Sentencing Database, not just for Federal offences (including Federal offences prosecuted in State jurisdictions) but also for State offences related to Cybercrime to ensure a consistent approach in sentencing on similar criminal

[6] 2004 Inquiry report at [2.53].
[7] 2004 Inquiry report at [2.55-2.56].

offences throughout Australia and to ensure an adequate and easily accessible record of the imposition of penalties for Cybercrime offences throughout Australia for the judiciary, practitioners and the general public.[8]

We note that, to date, the use of the database by the judiciary is reported as having had an impact on improving consistency in sentencing for federal offences.[9]

The database had the support of the then Minister for Home Affairs, the Hon. Bob Debus, was discussed during the Government 2008 review of the Federal Criminal Law[10] and was one of the key recommendations for implementation by the Federal Government made by the Australian Law Reform Commission to the Government in its 2006 Report on Sentencing.[11]

There was strong support in 2006 by the numerous groups consulted by the ALRC in the preparation of its report (including Government, academia, the judiciary and prosecuting agencies) for allowing access to the database to the general public[12] and the ALRC supported that view.[13]

At the federal level, the national sentencing database has been developed and is accessible to the judiciary. The database was launched by the Minister on 9 February 2008.[14]

---

[8] Including, potentially, through incorporation of current sentencing databases already in existence (for example, in both New South Wales and Victoria) and in operation in each State into a national database through an export of data for comparable State offences.

[9] For example, see comments by judicial officers participating in the National Judicial College of Australia's professional development programs positive comments on the benefits of computer-based sentencing databases to the administration of justice at National Judicial College of Australia, A National Sentencing Database on Commonwealth Offences? (2005) unpublished manuscript, 1.

[10] See the Minister's speech to attendees at the NJCA conference on 9 February 2008: available at: http://www.ag.gov.au/www/ministers/ministerdebus.nsf/Page/Speeches_2008_9February2008-SentencingConference2008.

[11] See ALRC 103 (2006): *Same Crime, Same Time: Sentencing of Federal Offenders*: Recommendations 21-1 and 21-2.

[12] See ALRC 103 and submissions reported as received as follows: Commonwealth Director of Public Prosecutions, *Submission SFO 86,* 17 February 2006; Attorney-General's Department, *Submission SFO 83,* 15 February 2006; G Mackenzie, *Submission SFO 80,* 14 February 2006; Chief Judge P McClellan, *Submission SFO 77,* 10 February 2006; Justice P Johnson, *Submission SFO 73,* 10 February 2006 (this submission was endorsed by 10 other judges of the Supreme Court of New South Wales); Australian Taxation Office, *Submission SFO 72,* 10 February 2006; M Beadle, *Submission SFO 56,* 1 December 2005; Sisters Inside Inc, *Submission SFO 40,* 28 April 2005; Australian Securities and Investments Commission, *Submission SFO 39,* 28 April 2005; New South Wales Legal Aid Commission, *Submission SFO 36,* 22 April 2005; Welfare Rights Centre Inc (Queensland), *Submission SFO 29,* 15 April 2005; JC, *Submission SFO 25,* 13 April 2005; Australian Taxation Office, *Submission SFO 18,* 8 April 2005; BN, *Submission SFO 17,* 8 April 2005; A Freiberg, *Submission SFO 12,* 4 April 2005; LD, *Submission SFO 9,* 10 March 2005; Attorney General's Department of NSW, *Consultation,* Sydney, 27 February 2006; Justice T Connolly, *Consultation,* Canberra, 13 February 2006; Chief Judge at Common Law P McClellan and Others, *Consultation,* Sydney, 2 February 2006; Law Society of the Northern Territory, *Consultation,* Darwin, 29 April 2005; M Johnson, *Consultation,* Darwin, 27 April 2005; Deputy Chief Magistrate E Woods, *Consultation,* Perth, 18 April 2005.

[13] See ALRC 103 at [21.21]: *"In the interests of facilitating research on federal sentencing and promoting better understanding of sentencing by the public, the database should also be made available for use by researchers and members of the public."*

[14] See the Minister's speech to attendees at the NJCA conference on 9 February 2008: available at: http://www.ag.gov.au/www/ministers/ministerdebus.nsf/Page/Speeches_2008_9February2008-SentencingConference2008.

Although the project has been funded up to 2010, we believe that it should be funded beyond that date and include further development as proposed in this submission.

We believe that, were the database to be made public and to be extended to recording of comparable State-based offences, there would be a significant benefit to be obtained by the community in having access to statistical information on the range and frequency of penalties imposed by courts for Federal and State-based offences and would enable a range of users to obtain comparative sentencing information.

Further, there appears to be no reason why a national database of all relevant Commonwealth and State offences could not be provided in relation to specific offence types in a relatively short period of time and with limited funding.

In a report provided to the House of Representatives' Standing Committee on Legal and Constitutional Affairs in September 2008 most Australian jurisdictions were reported as having such databases already in existence.[15]

6.2 International Issues

At an international level, we believe that the Federal Government and its agencies could do more to engage other nations and their law enforcement agencies with respect to Cybercrime, particularly in relation to financial and identity crime. The Australian Government needs to be more pro-active on the international stage in this area.

As the 2004 Inquiry noted:

> *"...in the Committee' s view the inter-jurisdictional and international nature of cybercrime* ***demands not only a co-ordinated and unified national strategy but one placed in the international context****...much unacceptable Internet activity originates outside Australia, which makes detection and prosecution difficult without some form of international co-operative detection and prosecution system.* ***Tracing and eliminating cybercrime requires a legislative framework that is consistent both domestically and internationally.****"*[16] (emphasis added)

The Committee shared our concern at the time related to the seeming lack, at an international level, of the development on an international framework for the detection and enforcement of this crime type,[17] both by Australia and other States.

6.2.1 The United Nations' Convention on Transnational Organized Crime

Australia is already a signatory to the United Nations Convention on Transnational Organized Crime ("**the Convention**") which entered into force in September 2003 (and ratified by Australia on 27 May 2004).

---

[15] *Ibid.* Including NSW, Victoria, Queensland, Tasmania and the A.C.T.
[16] 2004 Inquiry report at [2.42-2.43].
[17] 2004 Inquiry report at [2.44].

The Convention deals with a range of matters relating to co-operation between Sovereign States who are signatories to the Convention in the detection, investigation and prosecution of serious crime (as defined). The Convention does not necessarily cover all crimes that could be classified as 'Cybercrimes'.

The Government should seek, through diplomatic channels, adherence by all signatories to the Convention.

Anecdotal evidence suggests that some signatory States are not observing their obligations under the Convention, particularly with respect to co-operation with law enforcement agencies and prosecution of offenders.

In the first instance, we recommend that the Government undertake its own review of (and report upon) Australia's and other State's compliance with the Convention. The United Nations Office on Drugs and Crime (UNDOC) is the responsible UN agency to assist signatory States in monitoring compliance with the Convention. We recommend that the Government approach UNDOC to undertake such a review immediately and report on outcomes and provide recommendations to Member States (including details of the outcomes of the fourth session held in Vienna in 2008 and decisions made thereto[18]) and Australia should provide input to and report on the outcomes of the Working Groups set up by the fourth session in this respect.[19]

The Government should undertake its own immediate analysis on whether any Cybercrime impacting (or expected to impact upon Australia) is not covered by the Convention or other multilateral or bilateral agreements to which Australia is a party and, to the extent that the same agreements as those in the Convention are not in existence, should lobby for their creation on the international stage.

We note in particular that the Working Group established at the Fourth Session has already expressed concern relating to the manner in which an analysis of compliance with the Convention is being undertaken.[20]

Further, we do not believe that a self-reporting (particularly without sanction) framework is a useful model and the Australian Government should be pro-active in suggesting so in this forum.

To the extent of inconsistencies in States' self reporting and knowledge of the Government to the contrary, Australia should be clearly voicing its concerns regarding the discrepancies.

We also note that, at its second session in October 2005, the Conference of the Parties to the United Nations Convention against Transnational Organized Crime adopted decision 2/2, "Implementation of the international cooperation provisions of the United Nations Convention against Transnational Organized Crime".

---

[18] *Fourth session of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime and its Protocols*: see CTOC/COP 4 Decisions reported at http://www.unodc.org/unodc/en/treaties/ctoc-cop-session4-decisions.html

[19] As noted at http://www.unodc.org/unodc/en/treaties/CTOC/working-groups.html

[20] See Report of the Secretariat on the development of tools to gather information from States on the implementation of the UN Convention against Transnational Organized Crim and each of the Protocols thereto, CTOC/COP/2008/2 available at http://www.unodc.org/documents/treaties/organized_crime/CTOC_COP_2008_2_final_E.pdf

In that decision, the Conference decided to establish at its third session an open-ended working group, to hold substantive discussions on practical issues pertaining to extradition, mutual legal assistance and international cooperation for the purpose of confiscation.

The open-ended Working Group of Government Experts on Extradition, Mutual Legal Assistance and International Cooperation, established pursuant to decision 2/2 of the Conference of the Parties, convened its first meeting during the third session of the Conference of the Parties, which was held in October 2006. The outcome of the related discussions of the working group is reflected in decision 3/2, "Implementation of the provisions on international cooperation in the United Nations Convention against Transnational Organized Crime".

In its decision 3/2, the Conference of the Parties decided that an open-ended working group on international cooperation will be a constant element of the Conference of the Parties.

We support implementation of the decision. The Government should take a pro-active role in ensuring that the decision is implemented.

Australia should also review its current co-operation schemes with other international enforcement agencies in this area outside of the Convention, including supporting a centralised focus to Australian Government agencies engaging their counterparts in friendly and unfriendly countries.

We recommend that the Government approach UNDOC to undertake such a review immediately and report on outcomes and provide recommendations to Member States (including details of the outcomes of the fourth session held in Vienna in 2008 and decisions made thereto[21]) and Australia should provide input to and report on the outcomes of the Working Groups set up by the fourth session in this respect.[22]

6.2.2 Other Cybercrime not covered by the Convention

The limits of the UN Convention on Transnational Organized Crime obviously relate to the fact that they are limited in their operation to "organised crime" and "criminal offences" as defined by Article 2 the Convention.

The Government should undertake its own immediate analysis on whether any Cybercrime impacting (or expected to impact upon Australia) is not covered by the Convention or other multilateral or bilateral agreements to which Australia is a party and, to the extent that the same agreements as those in the Convention are not in existence, should lobby for their creation on the international stage.

We recommend that the Government implement a broader arrangement for dealing with 'Cybercrime' generally at the international level.

---

[21] *Fourth session of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime and its Protocols*: see CTOC/COP 4 Decisions reported at http://www.unodc.org/unodc/en/treaties/ctoc-cop-session4-decisions.html

[22] As noted at http://www.unodc.org/unodc/en/treaties/CTOC/working-groups.html

The Government may need to give consideration to the implementation of a treaty on Cybercrime[23] and bilateral treaty arrangements with complying Member States to the UN Convention.

6.2.3 Penalties imposed internationally

We also recommend that the Australian Government approach UNDOC (as part of the review suggested above) carry out a similar assessment of the imposition of sanctions by Member States for Cybercrime offences prosecuted prior to the next meeting of the UNDOC in Vienna this September. In particular, the Australian Government should clearly be in a position prior to that meeting to clearly express its views as to the reality of compliance by Member States with the Convention, particularly with respect to the Mutual Assistance provisions.

7. Education

All Australians (including our customers) have a role to play in protecting their own and Australia's security interests and banks do and will continue to provide public education programs including Cybercrime self-protection. The Government needs to better coordinate and pool its resources for its education campaigns to ensure Australian internet and telecommunications users better understand how they can protect themselves.

Government (at both State and Federal level) and its agencies have a vital role to play in providing education programs to ensure that all Australians better understand their responsibilities in protecting their own interests when using modern technologies to help them avoid becoming the victims of a range of Cybercrimes, from money muling to assisting organised crime (including assisting terrorists, paedophiles and drug dealers).

At present, education programs run by Government are not sufficiently coordinated and exhibit duplication, with little evidence of positive impacts on online behaviour. As the Federal Government has the power to legislate with respect to crimes conducted through the use of a telecommunications device, we believe that it appropriate that the Federal Government exercises leadership in this area.

Our Members would like to see a whole-of-Government approach to such education campaigns rather than the fragmented approach adopted to date and the duplication of work and associated unwarranted costs of such duplication. This includes coordination not just of Federal Government activities in the area, but State Government initiatives as well. The Federal Government should display leadership in this area.

As noted by the 2004 Inquiry, there does appear to be a lack of coordination of Government media programs (again both at a Federal to Federal agency level and at a Federal to State level).

While we believe that messages for consumers regarding how they should protect themselves on-line can never be 'over-delivered' by the Government, it does seem that there would be benefit to be gained from a whole-of-Government

---

[23] Perhaps similar to the European Convention on Cybercrime: ETS No.:185.

approach (media schedule) to such campaigns, which would include benefits that could be obtained through the pooling of respective agencies' budgets and resources with respect to key messaging in relation to the safe use of internet and communications devices.

Also, we believe that law enforcement agencies across Australia would benefit from nationally coordinated training on Internet Banking Fraud, including how to obtain evidence from victims when crime is first brought to their attention to ensure that cases are not lost or are unable to be prosecuted due to a lack of evidence that could have easily been obtained during the early stages of an investigation.

Our Members would be happy to assist in the provision of such training if the Government is interested in pursuing this with our sector.

There remains a significant role for Government in educating the general public on their responsibilities in relation to preventing themselves from becoming the victims of Cybercriminals. These efforts and funding for them should be pooled and better coordinated at both a Federal level and between the Federal Government and the States and Territories.

8. Collaboration with industry

The banking industry is a vital component of the critical infrastructure that underpins the whole of the Australian economy and all levels of Government in Australia should assist banks and other key stakeholders in protecting this national asset through improving the fight against Cybercrime on Australia. The reality of the method of this crime type is that one weak link in the chain gives criminals a foothold which will continue to have broader impacts on Australian society unless Government and relevant industries work more closely together to prevent criminals from hitting what will, in time, be considered to be a soft target.

We set out below the measures that we believe the Government needs to adopt to allow Australia to properly defend itself against Cybercrime risks.

We note that the resources available to Australian agencies and firms should place Australia in a much better position than many other countries (who have already undertaken initiatives similar to those suggested below with success) in protecting Australia and Australian internet users.

The ABA and its Members are eager to see a shift in the political will to enhance collaboration for the benefit of Australia.

The Government's current approach to combating Cybercrime threats to Australia needs to brought up to date with the magnitude and complexity of the threat.

In particular, information and intelligence gathering, analysis and sharing is shared between a many Government organisations and agencies. No formal sharing of information or intelligence (even at a generic level) takes place with our Members. No governing body currently exists to allow strategic threats to be continually assessed between the public and private sectors (other than in the area of Critical Infrastructure) in this area. Given the inter-dependency of the public and private sectors, this places Australian institutions in both the public

and private sectors at a disadvantage when it comes to protecting Australian internet users.

There needs to be coordination of State and Federal Government and Federal Government agency projects in this area, particularly in respect of the sharing of generic intelligence and data.

The 2004 Inquiry described these problems as follows:

> *"Law enforcement will usually be in a reactive rather than an active position, but the Committee considers that with the right strategic development, agencies will be well placed to at least meet, if not anticipate the increasing challenges of rapid technological development. There appears to be a considerable amount of work being undertaken: there is legislation being prepared by the Attorney General's Department, numerous Committees and interagency discussions,* ***but the Committee considers that this activity needs a well resourced co-ordinating body.***"[24] (emphasis added)
>
> *"The Committee considers that the proliferation of working parties, focus groups, interagency committees and similar groups has the potential to be more effective if there is an agency which can act as a co-ordinator of information and direct resources appropriately."*[25]
>
> *"...[t]he Australian Crime Commission (ACC) in conjunction with the Australian High Tech Crime Centre (AHTCC) are in a position through their intelligence activities to provide general information about fraud trends to financial institutions. This information could be provided through a third party which could collect and disseminate all available information on a regular basis."*[26]
>
> *"Success in the detection and prosecution of cybercrime will depend on cooperation between Commonwealth and State Law Enforcement agencies, the financial institutions, as well as other agencies (such as AUSTRAC).* ***The Committee considers that the formation of partnerships between these parties is crucial, if banking and monetary cybercrime is to be dealt with efficiently. In particular, government and private sector partnerships should be sought to disseminate important information regarding protection from financial fraud.***"[27] (emphasis added)

The recommendation made by the 2004 Inquiry to remedy the situation was:

> *"The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service."*[28]

---

[24] 2004 Inquiry report at [2.88].
[25] 2004 Inquiry report at [4.87].
[26] 2004 Inquiry report at [4.20].
[27] 2004 Inquiry report at [4.89].
[28] See Recommendation 5 of the 2004 Inquiry report.

Our Members have seen no evidence of the implementation of these recommendations to date and believe that this now needs to occur if the Australian Government is to meet its commitments under the Convention and achieve the objective of reducing the risk of Cybercrime to Australians.

Given that the vast majority of Cybercrime is transnational, we believe that the Federal Government must demonstrate a clear leadership role in this area and appropriately engage industry. It has not done so to date.

9. Emerging risks

Apart from the recommendations made by the 2004 Inquiry, our Members have identified further initiatives to mitigate E-Security risks to Australian internet and telecommunications users.

9.1 National Broadband Network

Our Members believe that the Government must act now on addressing Cybercrime threats that will arise with the roll-out of the National Broadband Network ("**NBN**") and believe that a budget for security needs to be allocated now by the Government to address those threats.

The ABA and its Members remain willing to provide any assistance in this area in helping Government identify and addressing the potential threats (not just for the banking industry but for Australia as a whole).

9.2 Phone porting

Risks arising from "mobile phone porting" and the transfer of email accounts (transfers without the knowledge or consent of the account holder) need to be addressed by the Government through collaboration with carriage service providers. To the extent that this does not occur, ordinary Australians' risk of identity takeover and related identity crimes will continue to increase.

We believe that the Government can play an important role in the setting of processes to be adopted by telecommunications providers, internet service providers, industry and consumers. In some cases, those processes could include guidelines on when service providers should provide more support to their customers who have become victims of Cybercrime.

9.3 Wire transfers

In respect of the transfer of funds offshore through money wire transfers, we believe that the Government and its agencies could also improve engagement of providers of those services on this issue.

Whilst the providers of international wire transfer payment services should now be regulated by the provisions of the *Anti-Money Laundering and Counter Terrorism Financing Act* 2006 (Cth), we believe that the Government should be taking a more pro-active role in engaging newly regulated providers and establishing processes to ensure stolen funds are not transferred offshore.

10. ABA Recommendations to Government

The Commonwealth Government should:

(1) Implement Recommendations 3, 5, 6, 7, 8, 9, 10 and 11 from the 2004 Inquiry;

(2) Set up a framework for national co-operation of all law enforcement agencies and departments who work on Cybercrime issues within the next 3 months (including all relevant Federal and State agencies);

(3) Implement a roll-out of the National Sentencing Database to include State-based offences related to Cybercrime and the database be made available to the public;

(4) Review the adequacy of penalties imposed for Cybercrime and related offences at both the Federal and State level;

(5) Undertake its own review of (and report upon) Australia's and other State's compliance with the Convention within the next 3 months;

(6) Approach UNDOC to undertake a review of actual implementation of the Convention by signatory states and to report on outcomes and provide recommendations to Member States;

(7) Provide input to and report on the outcomes of the Working Group set up by the Fourth Session (Working Group on implementation of the Convention);

(8) Undertake its own immediate analysis on whether any Cybercrime impacting (or expected to impact upon Australia in the next 5 years) is not covered by the Convention or other multilateral or bilateral agreements to which Australia is a party and, to the extent that such agreements are not in existence, lobby for their creation;

(9) Raise concerns before and at the next Working Group session in 2009 on implementation of the Convention, particularly with the regime of self-reporting as a means of assessing implementation of the Convention. The Government should lobby for the creation of a different mechanism of assessment for assessing implementation of the Convention. The Government should be voicing concerns regarding the extent of inconsistencies in States' self reporting and knowledge of the Government to the contrary;

(10) Support and participate on the open-ended Working Group on practical issues relating to implementation of the Convention;

(11) Review its current co-operation schemes with other international enforcement agencies in the area of Cybercrime (outside of the Convention), and should provide support to a centralised focus to Australian Government agencies engaging their counterparts in friendly and unfriendly countries;

(12) Implement a broader arrangement for dealing with 'Cybercrime' generally at the international level than that currently covered by the Convention;

(13) Approach UNDOC to carry out an assessment of the imposition of sanctions/penalties by signatory States for Cybercrime offences under the Convention prior to the next meeting of the UNDOC in Vienna this September;

(14) Implement a mechanism for coordination of education and awareness campaigns at both a State and Federal level;

(15) Establish a dialogue with the banking and other relevant industries to work collaboratively with industry, particularly with respect to the sharing of generic threat and intelligence information on Cybercrime;

(16) Address emerging risks that will be created by the roll out of the NBN and plan for and allocate budget to deal with those risks prior to their becoming a reality;

(17) Engage relevant providers with respect to specific threats such as phone porting and international wire transfers within the next 3 months.