COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

Reference: Cybercrime

FRIDAY, 18 JULY 2003

SYDNEY

BY AUTHORITY OF THE PARLIAMENT

INTERNET

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **http://www.aph.gov.au/hansard**

To search the parliamentary database, go to: **http://search.aph.gov.au**

JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

Friday, 18 July 2003

Members: Mr Baird (*Chair*), Mr Sercombe (*Deputy Chair*), Senators Denman, Ferris, Greig, Hutchins and McGauran and Mr Dutton, Mr Kerr and Mr Cameron Thompson.

Senators and members in attendance: Senators Denman, Ferris, Hutchins and McGauran and Mr Baird and Mr Sercombe

Terms of reference for the inquiry:

To inquire into and report on:

Recent trends in practices and methods of cybercrime with particular reference to:

1. child pornography and associated paedophile activity;
2. banking, including credit card fraud and money laundering; and
3. threats to national critical infrastructure.

WITNESSES

Committee met at 9.05 a.m.

McLEOD, Mr Scott, Coordinator, National Cybercrime Unit, Australian Crime Commission

MILROY, Mr Alastair, Chief Executive Officer, Australian Crime Commission

CHAIR—Welcome. I declare open this public meeting of the parliamentary Joint Statutory Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee when it reports wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

The committee prefers that all evidence be given in public but, should you at any stage wish to go in camera, if you advise the committee we will consider your request and then proceed in camera. I would like to thank you for your comprehensive submission. You addressed a number of the issues that came forward in our discussions yesterday, so I found it very useful. Obviously there are questions we would like to follow up. We ask you to make an opening statement, and then we will proceed to questions.

Mr Milroy—I appreciate the opportunity to appear before the parliamentary joint committee to provide evidence on the submission on cybercrime provided by the Australian Crime Commission, which was submitted on 2 June 2003. I am accompanied today by the manager of the cybercrime unit from the Crime Commission, Mr Scott McLeod, to whom, with the committee's agreement, I may if necessary refer some questions of a technical and detailed nature—if that is considered appropriate.

CHAIR—Sure.

Mr Milroy—As Australia's national criminal intelligence agency, the ACC is well placed to make an important intelligence contribution to the national response to cybercrime. The commission also has a capacity to provide forensic and technical services to support its own operations and those undertaken with partner agencies, subject to Australian Crime Commission board determinations. Inherently, cybercrime investigations are highly complex as well as resource and expertise intensive. A high proportion of cybercrime investigations also have significant jurisdictional issues. The Australian Crime Commission is well suited to bring a national perspective and specialist capabilities to this multijurisdictional work.

The commission is a small agency with an important role for criminal intelligence in Australia. It cannot hope to do an effective job of assessing national criminal intelligence priorities and underlying data without having close and intelligent liaison and involvement in operational work with the law enforcement and regulatory community, as well as a very good partnership with the private sector and, in particular, overseas agencies. Cybercrime intelligence can only hope to promote success through the developing and sharing of knowledge. As you would realise, knowledge of a subject matter gives you a competitive advantage, and we have to obtain that knowledge to be successful.

In maintaining a holistic approach to combating cybercrime, the Australian Crime Commission has identified four key areas in which it and the law enforcement community should assign priority. These include international and national cybercrime intelligence collection and analysis, partnerships with Australian and overseas government agencies and industry, maintaining a technical response capacity and, of course, policy and legal reform.

Our submission proposes a number of practical steps which are intended to enhance law enforcement capacities. Our focus will include the collection and coordination of cybercrime intelligence, the provision of services such as the national criminal intelligence database to facilitate information sharing, and partnerships, particularly with the Australian High Tech Crime Centre and various jurisdictions' cybercrime task forces. It will also include enhancing the electronic Internet intelligence gathering and data interception capability of the Australian Crime Commission and increasing the national criminal intelligence capacity of the Crime Commission in order to improve the service of information and intelligence—for example, by incorporating transnational Internet paedophile intelligence—and will also involve reviewing laws, for possible reform, for law enforcement agencies to conduct lawful interception of criminals' data via electronic search warrants.

In order to keep pace with the intelligence responsibilities associated with the criminal use of intelligence, the Australian Crime Commission proposes to continue to develop information management plans with state and territory jurisdictions to enable a rapid, nationally consistent collection of cybercrime related intelligence; to pursue working partnerships with other domestic and overseas agencies, along with private enterprise, to improve the scope and flow of cybercrime related intelligence; and to improve the electronic Internet intelligence gathering and analysis capacity of the ACC. Information has to be collected on a worldwide basis, and in this way pre-emptive action can be taken. To be effective in countering cybercrime, a more focused and responsive intelligence capability which would involve all law enforcement, government and industry needs to be our primary objective.

CHAIR—Yesterday we had a presentation by Victoria Police. One of the recommendations they brought forward was the need to have a centralised role in terms of cybercrime so that there is one group with national responsibility for cybercrime which could then provide details to the various police forces around Australia. It is an evolving area and various groups are looking at it—you are looking at it, the Australian High Tech Crime Centre is involved and there are other cybercrime task forces as well. To what extent do you believe it is being effectively coordinated now? Is there a need for establishing a special unit just for cybercrime, perhaps taking the Australian High Tech Crime Centre into that? It certainly came forward in the recommendation of Victoria Police yesterday. Could you comment initially on the degree to which we need greater coordination, centralisation and focus on this on a national basis?

Mr Milroy—I feel that the Australian High Tech Crime Centre, bearing in mind that it is strongly supported by all law enforcement commissioners, and with our added assistance in terms of international and national intelligence gathering capacity, basically provides us with the proper foundations for such a coordinated response. As you pointed out, it is an evolving process. It is a new area that law enforcement is now becoming more involved in. I believe that the foundations are there if we continue to build on that through the Australian High Tech Crime Centre and the added support of the Australian Crime Commission's intelligence gathering capability.

CHAIR—Would anybody else like to ask questions on the particular aspect of central coordination?

Senator FERRIS—Whenever we have discussed these issues in this committee and previously under the National Crime Authority parliamentary committee, issues of 'turfdom' have come up in relation to national and state based issues around this area. I am wondering whether the sharing of information by the states with the Australian Crime Commission and previously the National Crime Authority has improved, because the issue of 'turfdom' used to be very difficult for this peak body. I am wondering whether you are having as much cooperation as you believe you could get from the state agencies, who effectively have day-to-day management of these issues.

Mr Milroy—No, I believe that there has been significant improvement in coordination in relation to law enforcement. I believe that the decision to form the Australian Crime Commission Board—which as you would realise includes all law enforcement commissioners as well as other agencies—is now ensuring that this coordination, not only in cybercrime but in other areas of law enforcement, is being far better managed. So I believe that the issue of sharing information is going to be far more prevalent in the future. In particular, with the national criminal intelligence priorities and our collection plans, which have been approved by the Australian Crime Commission Board and have been accepted as a working tool for all agencies, we will be collecting information in relation to cybercrime. That information will be put into the national database, which is available for all agencies as well as, of course, for partnerships with the private sector, which is critical. I feel fairly confident that, if we continue down this path of cooperation, as it has been exhibited by the board and its state officers, the foundations are there for the future.

Senator FERRIS—I am reassured by your answer.

CHAIR—It is obviously an area that we would like to focus on, especially in terms of your role in this area.

Senator DENMAN—As regards the search warrants for looking at these sites, are they able to be issued across a number of states at the same time? If you are suspicious of someone in New South Wales using a site and you know that someone in, say, Victoria is doing the same thing, can you issue a warrant in all states?

Mr Milroy—I think it is important to point out that the work that the Australian Crime Commission does is determined by the decisions made by the board. The menu of work that we have at the moment does cross a lot of areas of criminality, which means we are authorised to use our coercive powers as well as warrants if we are actively involved in federally criminal activity. In relation to the specific issues you are talking about, of course that will depend on what we are authorised to pursue.

Senator HUTCHINS—Is there any area where you are concerned that there might not be enough coordination? For example, is there potentially a unit somewhere looking at, say, child sex offences, credit card skimming or the tax on infrastructures, where the information that they have collected should be in some system that is not there? Is there any area that could be done a little better that you think we need to address?

Mr Milroy—My understanding at the moment is that the information that you speak of is being collected by our department. I think it is important and there is a lot more awareness, in the private sector and in law enforcement, of the urgency and the need for cooperation. Yes, we can always improve the framework of ensuring that we are capturing the information across industry, law enforcement and all sectors to ensure that we have the appropriate knowledge. That can always be improved, and I think it is important that the partnerships that are being developed at the moment continue to be enhanced.

Senator HUTCHINS—What about internationally? Is that a problem in South-East Asia, particularly, say, in relation to credit cards?

Mr Milroy—These offences are a problem in a lot of jurisdictions. As you know, technology criminals pick up on the new methodology in some countries and are successful, and eventually that flows to other countries. It is important that we in this country, through partnerships with the various financial and industry groups who come out of multinational organisations, are tapping into what they are encountering overseas. We are building up relationships, through the Australian Federal Police liaison officer network, with various jurisdictions in a number of countries to ensure that we are receiving up-to-date information on areas of criminality, not only in this area but across the board, so that we are kept up to date so we can take some pre-emptive action. But I think it is a process: you have to be vigorous, you have to continue pursuing the various areas and you have to be alert to the changing technology and the changing area of criminality so that you can pursue gathering that information in the right areas. It is an ongoing process.

Senator HUTCHINS—Does that include child pornography as well in old Russia and eastern Europe? I read one of the submissions which said that it did not appear that Russia and eastern Europe had the same approach to scrutinising the broadcasting, I suppose, of child pornography that a number of the Western nations have.

Mr Milroy—I am sorry; I cannot comment on that. I am not up-to-date with what specifically is going on in other countries in relation to whether they are doing a good job or not.

Senator HUTCHINS—I know. I just meant in relation to coordination, that is all.

Mr Milroy—We are trying to establish coordination as much as possible around the world. You do rely on the information that you gather from your various contacts, and that needs to be continually developed and enhanced to ensure that we are not missing out.

CHAIR—Firstly, on that point, it was suggested to us yesterday that there is often a lag in terms of sharing information particularly in Europe, as they share it amongst themselves in the EU, or in the United States but we are at the end of the chain in getting information regarding work that is being carried out in paedophile rings or wherever. Do you see that as a problem? Secondly, are we regularly sending people overseas to participate in Interpol discussions on these issues et cetera?

Mr Milroy—It is something that you have to really continually work at. The expansion of the Australian Federal Police liaison network into other countries allows the Australian Crime Commission—I can only speak for ourselves—to be able to go through that process to ensure

that we are actually touching base in the right areas on the right subject matter to gather information. Yes, we have established relationships with a number of agencies, which we would probably keep confidential at the moment, in relation to ensuring that we are receiving information on various issues of criminality. But I believe that is something you have to keep continually pursuing vigorously. I believe that that foundation is there at the moment and we are building on it.

CHAIR—If I could move to the question of search warrants, you propose that electronic search warrants are appropriate for investigating cybercrime. Under the ASIO bill this is only allowed under special circumstances in terms of national security. Do you think there is justification for taking what some would see as a fairly significant step in terms of these cyber search warrants?

Mr Milroy—As I indicated in my opening remarks, we are reviewing the law for possible reform. So it is something that we are looking at and we are conscious, of course, that there are the privacy issues to consider and other such factors. It is only in the review stage at the present moment and I cannot comment on the specifics of the ASIO legislation but I believe it is something we have a responsibility to look at. If it is appropriate for us to put up a submission for consideration and all those factors are taken into consideration then, of course, we will have to be conscious of the actions of criminals and we will have to have a balance between the privacy of individuals and what we need to ensure security.

CHAIR—The Victorian Bar association expressed their concern with those proposals while they saw that if hacking was taking place that would affect national security—albeit that it might be related to our water or electricity supplies—then that would meet the criteria of section 25A of the ASIO Act. Are you aware of these concerns that have been brought forward regarding the use of these cybercrime warrants?

Mr Milroy—Not personally, no—unless Scott has further information.

Mr McLeod—We are aware of civil liberties issues and privacy issues that may be involved in this type of legislation. As Mr Milroy stated, we are not advocating these particular types of warrants; we are just scoping into the future of electronic policing requirements maybe five or 10 years away. Certainly, when ASIO asked for these powers, I am sure a lot of the same issues were canvassed. We are not saying that the ACC should have these powers; we are just saying that this is another law enforcement tool that in the future may be directly related to electronic crime investigation.

Mr SERCOMBE—Underpinning the issue is whether, operationally, the powers you have presently are sufficient for the tasks you are being asked to perform. In the context, say, of a search warrant regime, are the arrangements adequate for your purposes or is there a need to look at additional powers?

Mr Milroy—As you would be aware, the Crime Commission is a new agency, and we have been given wide-ranging powers. Only in May, after six months of operations, the board made the determination for us to work on a wide range of areas—to look at established criminal networks, South-East Asian crime and other areas to do with money laundering, amphetamines and vehicle rebirthing. We are just starting to use the powers we have at the moment, so I believe

it is premature for us to make any comments about their adequacy, but we are conscious of these issues as we learn from our operational activities. We are constantly reviewing the law as we progress and, if we feel that our powers are not adequate or could be improved in the future, then we will take the appropriate action and refer them to the appropriate authority for consideration.

Mr SERCOMBE—On this issue of the special powers you have, in your submission you talk about the partnership between the ACC and the Australian High Tech Crime Centre and say that the AFP centre will have access to the ACC's multijurisdictional special powers. Given the sensitivity of that issue in the debate about establishing the ACC, are you able to provide any further information on how you anticipate the ACC special powers will function in the context of cybercrime, particularly with regard to extending the capacity for their use within the framework of the High Tech Crime Centre?

Mr Milroy—The only authority for us to use our coercive powers is, clearly, where the board has made a determination. The matters in which we are currently authorised to use our coercive powers are money laundering, South-East Asian crime, established criminal networks and illegal firearms. Where cybercrime crosses over into those areas, where it is justified and where the relevant applications are appropriate then we would use the coercive powers—but only in those areas that have been approved by the board. A more practical explanation is that, where we are involved in an investigation that touches on money laundering, for example, and it is quite clear that we could use our coercive powers to examine a witness who may have adequate knowledge of the use of computers in facilitating some money laundering, then it would be appropriate for us to do so. But there is a very rigorous process to go through before we actually use the coercive powers.

Where we are working with a partner agency in an authorised joint operation across those matters that have been so determined, that partner agency would have to comply with our fairly strict arrangements for the use of the coercive powers. So we would have the final say as to whether it was justified in using them, and it would only be in an authorised operation. So the partner agency would come in under the umbrella of the Australian Crime Commission, and not come to the authority and require coercive powers for their own use. They would not be approved unless it was so determined by us.

CHAIR—Can I turn to the question of child sex offenders? We are interested in the initiatives that you have taken in relation to child sex offenders and what impact there has been from your activities in this area. Also, I want to look at the question of what effect you have been able to have on the trade of Internet material involving sex offenders, especially when a lot of the material comes from overseas. I want to focus on the question of child sex offenders in particular.

Mr Milroy—I will open, and Scott can provide some additional information. As you would be aware, Internet child pornography and CSOs are not an ACC board investigation operation. The Australian Crime Commission, however, continues to support various law enforcement agencies in the development of best practice models for investigation and intelligence management relating to the child sex offender networks with cross-jurisdictional and international membership. We also promote the use of the ALEIN database in Project Egret and the ACID in the fight against child pornography and Internet child sex offences. We continue to liaise with the AFP high tech crime team, and we provide support on CSO Internet use as required in our

partnership with them. Perhaps Scott can give you some more information in relation to the specific assistance that we might have provided in the last six months.

CHAIR—What has actually happened in real terms? That is what we would like to know.

Mr McLeod—As Mr Milroy stated, the investigation of child sex offenders or, in fact, Internet child sex offenders was not a National Crime Authority responsibility, nor is it specifically an Australian Crime Commission investigation operation which we are authorised for.

CHAIR—Is that a problem that, again, comes back to the old issue of coordination? You are saying, 'That is not strictly our responsibility,' and—

Mr McLeod—However, the Australian Crime Commission has an overall role of coordinating all national criminal intelligence within Australia, and some responsibilities in relation to CSOs—child sex offenders—fall under that umbrella. As the ACC incorporated the Australian Bureau of Criminal Intelligence, we also inherited responsibility for the ALEIN information desks and the ACID, the national criminal intelligence database. As part of our role, one of the things that we have inherited is Project Egret, which is the ALEIN information desk in relation to child sex offenders, and also the coordination of any child sex offender intelligence that may go onto the secure ACID, the national intelligence database.

In relation to what we have been doing recently on child sex offenders, because we do not have a specific role in investigating Internet child sex offenders we are very restricted as to what we can investigate. What we have tried to do is complement the partnerships with other agencies, including state agencies and the Australian High Tech Crime Centre, which may be in a position or which are in a position to pursue child sex offenders online.

CHAIR—Does your role, then, relate particularly to organised crime rather than to individual people who are putting things on the Net?

Mr McLeod—As an example, we are very restricted as to what we can investigate in relation to what is board approved. However, some of those are board approved investigations. Most investigations we do nowadays have a cybercrime aspect. We are not talking about hacking, we are talking about criminals using computers to further organised crime, handguns or whatever it may be. It may be that in some of those investigations, for example in relation to South-East Asian organised crime, there may be a child pornography aspect to the investigation. It is not the focus of the investigation but it may come to light during the investigation. That is a hypothetical example where we would have a role in passing on that information to the appropriate agency, through proper dissemination, and in assisting the coordination of that intelligence, which we have picked up through one of our authorised investigations, which may relate to, say, child sex offenders.

Senator FERRIS—Mr Milroy, you have been talking about Internet sites in relation to child pornography, but I would like to take you to one that has a very practical application that was reported in the media this morning—that is, the use of a chat room for a child to subsequently be kidnapped by a person—a man—who established an ongoing relationship with the child using a pop star as the hook. He was able to entice the 12-year-old girl out of her home in England. The

answers you are giving at the moment focus on Internet sites. Chat rooms are an enormous opportunity for people who work in this area to appear to be something that they are not—for paedophiles to operate in that area. When you talk about Internet sites are you including chat rooms in that area of interest?

Mr Milroy—I might ask Scott, because that is more of a technical matter.

Mr McLeod—Prefacing my remark by saying that we do not investigate child sex offenders online or otherwise, I can answer the question in a general sense. As you know from recent media in relation to chat lines, one of the problems we have with the Internet—both in gathering intelligence and in law enforcement in general—with prosecuting offenders, whether it be for hacking or whatever, is the anonymity of the Internet. As you know, you can get on a chat line and be whoever you want to be. Because of the very nature of the Internet, there is no firm identification method to identify people, and maybe that is rightly so—to preserve freedom of speech or the privacy of individuals. Anonymity has always been and still is a problem for law enforcement when investigating matters. I can only really comment on that that chat rooms are an aspect of Internet child sex offences which law enforcement in general looks at. I cannot talk for other agencies either in camera or here.

Senator FERRIS—The Australian Broadcasting Authority are coming on next. In their submission, they have identified chat rooms as a potential source for greater activity in parent awareness. Given that they are a national organisation and they have an interest in this, is it an area you would like to raise to a higher national profile, given the difficulty that chat rooms offer people the opportunity to be whomever they wish and to target children, particularly after school when children are at home on their own on the Internet without parental supervision?

Mr McLeod—I cannot comment on the submissions that anyone else may be putting in, but our holistic approach to cybercrime is, I believe, an approach that is being taken more and more now—that is, everyone has to take responsibility for policing themselves and not putting their children in a position where they may be open to child sex offenders online. We do not advocate more regulation. I believe that some of the other submissions talked about better education programs for parents rather than restrictions on Internet service providers. There are a number of suites which range not just across law enforcement but across private enterprise and the education of parents and children in relation to those areas.

Senator FERRIS—Net Nanny and other filtering packages do not deal with chat rooms so that is a wide-open area. The ABA's submission is a public one and it might be interesting for you to have a look at it.

Mr McLeod—I have read through it; but, as I said, I cannot comment on it.

Senator FERRIS—I understand.

CHAIR—Are there any further questions on child sex offenders before we move on?

Senator HUTCHINS—I have one question following on from Senator Ferris's comments about the broadcasting authority submission. In the final part of the submission from the broadcasting authority they talk about a problem in the future in relation to mobile devices being

used. Is that something that the commission is being proactive on? Rather than playing catch up, are you looking at the next tactics people will use to try to circumvent the authorities? Would you like to comment, Mr Milroy and Mr McLeod, on being proactive?

Mr Milroy—Currently the Australian Crime Commission are carrying out a strategic assessment and one part of that assessment is looking at building on the cybercrime futures discussion. There are actually discussions being held at the present moment by analysts from my department as well as a number of other agencies looking towards 2008 and the problems that we are going to encounter. So there is an emphasis on looking ahead because, as we all know, criminals continue to move not only into the area that you are talking about but also into other areas. They use their technology and learn from experts. There is more mobility in this area which makes it far more difficult for us because they operate from various countries and can use technology to commit cybercrime offences in another country without detection. We have to try to look ahead, and that is where the futures discussions we are running at present come in. These will be part of the strategic threat assessment we are currently undertaking in addition to what our in-house cybercrime unit currently does.

CHAIR—I would like to turn to the area of banking. One of the areas we have been looking at is organisations, such as e-gold, which operate outside of normal banking and financial institutions, the extent to which they can be controlled or regulated and what impact they have in terms of money laundering.

Mr Milroy—I will ask Scott if he has any knowledge on those issues.

Mr McLeod—The short answer is that we do not have any of our financial investigators from the Australian Crime Commission here and I would hate to encroach on an area they cover. They contributed a lot of material in relation to banking for our submission. One of the areas which the submission touched on was what has been termed online money laundering—and this is probably mirrored in the submission from AUSTRAC—and the cash to electronic barrier. The cash to electronic barrier refers to a person converting cash, from drugs sales or another criminal act, into an electronic form either by placing it in a bank or going through another cash dealer to have it in a form which can then be electronically transferred overseas or used by things such as e-gold, PayPal or a number of other electronic pseudobanking type facilities available on the Internet. I cannot specifically comment on e-gold and those other facilities.

CHAIR—You may want to take that on notice.

Mr McLeod—Would you like us to do that?

CHAIR—That may be useful, yes.

Mr McLeod—Are you interested in what we believe the threat of those to be?

CHAIR—Yes.

Mr McLeod—We will take that on notice.

CHAIR—Are there further questions on banking?

Senator DENMAN—Yes, I have a question. How has self-regulation of the financial industry contributed to levels of crime? Do you know the answer or will you have to take it on notice?

Mr Milroy—We will take that question on notice.

Mr McLeod—It is a very broad question.

Senator DENMAN—I realise that. I want a broad answer.

CHAIR—I think Senator Denman's question is quite a valid one because we have actually found that, whether it be the banking area or the credit card area, which are obviously closely related and very much self-regulatory, the onus is very much on the trader, the shop owner. The question of to what extent there should be some regulation of the area comes forward if people have been stung by credit card scams. Whether it be the person or the shop owner involved, that can have devastating effects, and we had evidence of that yesterday. So do we continue with self-regulation or is there a need for some further changes?

Mr Milroy—We will take that on notice. We have been working with the ABA on a card skimming intelligence probe. That is all it is at the moment and, as somebody said, it is in its early stages. We will pick up on that and provide an answer.

Senator McGAURAN—I want to follow up the comment that you are working on a particular project at the moment. The ACCC have outlined many of the sophisticated scams coming out of, for example, Internet cafes, which are prolific. Given that your mission statement is about organised crime, how organised is it in the traditional sense? Are we looking at heroin syndicates that are set up and just as easily flip over and have an extension into these sorts of scams or ID crime? Is it the traditional syndicates or is a new type of criminal involved? Are they geeks or still from the Bronx?

Mr Milroy—I think we always find that there are criminals who stay traditionally in the areas they are comfortable in but there are others we have noticed who are quite entrepreneurial in their methods. They actually move to where the money is easily obtained and they are quite adaptable. So we have noticed that there are people who in the past would have been involved in traditional areas of criminality who have been smart enough to move with the times and embrace the e-crime areas and try their hand at the fastest method of making money. It is all about making money, so they move very quickly. We are noticing that a lot of people who are involved in drugs are involved in firearms and e-crime activities and are using identity fraud as a method as well, so we find a lot of mixture in the activities that criminals involve themselves in.

Senator McGAURAN—Would you say that the profile is one of organised crime in the traditional sense? Is that the profile, more than a new set of criminals?

Mr Milroy—No, I think it is just more to do with opportunists and people who shift from one area to another to pursue the quickest way of making money, whether it is by drugs, guns, prostitution or white-collar crime. So I think they are very diverse. I will not get involved in what we call organised crime, because I think that is a difficult area to clearly define because we look at specific areas of criminality as per the board determination, so we have set guidelines in certain areas that we are operating in. We are not engaged in all areas of criminality, because we

are only a small agency. But within the areas that we are currently looking at there is quite a lot of diversity in relation to the criminal activities.

Senator HUTCHINS—In relation to white-collar crime, do you think the penalties in the law now are sufficient to deter them? Do you think they should be stronger?

Mr Milroy—I do not think I am in a position to comment on the rights and wrongs of penalties. It is not an area that I have really looked at seriously.

CHAIR—Could we look specifically at the question of credit card fraud. You said that you have started some work in that area. Could you tell us about that?

Mr Milroy—I will ask Scott to answer that.

Mr McLeod—As you know, credit card skimming is an approved intelligence investigation by the board. As part of our role in developing card skimming intelligence, we have engaged and had talks with a number of the state law enforcement agencies, which have provided material. We have recently spoken to the New South Wales Police about their Task Force Venlo, which investigated credit card skimming in New South Wales for quite some time. Also, we have engaged some of the card companies and we are speaking to them about risks and trends and what they believe law enforcement should be looking at in relation to card skimming. With regard to organised crime and card skimming or ID fraud, in 2001 I attended the MasterCard fraud reduction task force meeting for Australasia at the Gold Coast. One of the things that was brought up was the theory of fraud migration with regard to card skimming. According to that theory, where law enforcement or private enterprise in a particular region have dealt with a problem—say, with card skimming—and they have brought in sufficient laws or powers to interdict that practice, that fraud then migrates to another region where either legislation or financial institutions have not caught up to the way the fraud is done. Back in 2001, MasterCard predicted that card skimming was endemic in South-East Asia—and it still is—but they predicted that card skimming fraud migration would move to Australia. From some of the material that we have gathered so far, it would seem that since 2001 the problem of card skimming and ID fraud has migrated to Australia.

CHAIR—So are you having discussions with police authorities in South-East Asia regarding this issue?

Mr McLeod—We have not at this stage—all our communications go through the Australian Federal Police liaison network—but we certainly will further down the track, remembering that we have only had this intelligence investigation probably for about a month and a bit now.

CHAIR—Are you finding, by the way, that the AFP and the international liaison people have restricted some of the activities you would want to get into in this area?

Mr Milroy—No. The relationship we have with the Australian Federal Police provides us with the opportunity to request—through the chair of the board, who is the commissioner of the Federal Police—for their liaison officer in the various countries to facilitate our inquiries and to put it onto the heads of the various law enforcement agencies and other experts. Where they

cannot assist us we have the ability to use our own network to pursue that sort of information across the areas that we are authorised to work in.

CHAIR—If there are no further questions in terms of credit card fraud, I will open it up to questions across the board to the ACC.

Mr SERCOMBE—One of the issues we raised with the Victoria Police yesterday was the issue of career paths for people in law enforcement with the skills required in the cybercrime area compared with the sorts of opportunities that may arise, for example, with firms of forensic accountants and the like. Is there an issue of law enforcement in Australia being able to adequately attract and retain people with the requisite specialist skills in these areas?

Mr Milroy—I might answer that initially and then Scott can speak from a practitioner's point of view. As far as the Australian Crime Commission is concerned, where we believe that we require the appropriate expertise in the short term from specialists, we are actually looking at developing a panel of experts in various fields—forensic accounting and other areas—where they will be cleared from a security point of view. The organisation can then tap into that resource for specific inquiries that relate to matters that we are currently pursuing.

As for our own cybercrime unit, as with any other discipline we would ensure that they are trained to the top level at which we require them to provide expertise in-house, as well as in our partnerships with other agencies. So we would of course encourage their training, but it is difficult because of the high level of expertise that is required in such a specialised field. One would need to continually allow such staff to be brought up to the same level of expertise as in the private sector, which is quite a costly exercise. Law enforcement agencies have to ensure that we do not duplicate this level of expertise in every police force and in two or three different national agencies, because that defeats the whole purpose. It is far better to have a coordinated and perhaps far more centralised or nationally driven level of expertise, while at the state level you have the skills that might be required for your own jurisdiction.

CHAIR—It comes back to that overall question of coordination—

Mr Milroy—That is correct.

CHAIR—and centralisation of specific skills, particularly related to cybercrime. It keeps coming back to that issue. As there are no further questions, I would like to thank you for coming today. Chances are that we will come back to you regarding some of these issues, and if you would not mind, please get back to the secretary with the answers to the questions you took on notice. As you know, you will be sent copies of the transcript to review. Thank you for coming today and for the forthright way in which you have answered our questions.

Mr Milroy—Thank you.

[10.02 a.m.]

FLINT, Professor David Edward, Chairman, Australian Broadcasting Authority

FRASER, Mr Richard James, Assistant Manager, Content Assessment Section, Hotline Manager, Australian Broadcasting Authority

CHAIR—I call the committee to order and resume this public meeting of the parliamentary Joint Statutory Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime, with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money-laundering; and threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

I welcome Professor David Flint and Mr Richard Fraser of the Australian Broadcasting Authority today. As you know, we prefer all evidence to be given in public, but should you at any stage wish to go in camera please let us know and we will move in camera. Thank you for your submission. We now invite you to make an opening statement and we will follow that up with questions.

Prof. Flint—It is widely recognised that the Internet is a valuable resource, but obviously it can facilitate inappropriate contact between adults and children. There is plenty of evidence of that, and evidence that the volume of child pornography being produced and exchanged is increasing. There is unfortunately no magic wand in relation to this problem. It requires a coherent strategy of regulatory and non-regulatory measures—government, industry and the community. The coregulatory scheme which the ABA administers has an emphasis on raising community awareness of online safety issues as a preventive measure. We work with NetAlert Ltd in this regard, and we have a hotline which plays an important part in raising community awareness of the issues. For each of the years 2001-02 and 2002-03 the ABA has investigated some 240 items of Internet child pornography or other paedophile related material.

There is—and I apologise for this—a typographical error on page 10 of the ABA submission. A heading reads ‘Complaints investigated 1 January 2000 to 31 October 2002’. It will be obvious from the content that that should read ‘Complaints investigated 1 January 2000 to 30 April 2003’. These items, these sites that we have dealt with in regard to the matters under consideration by this committee, are mainly overseas. Of particular concern to the ABA is the number of sites located in states which are successor states of the former Soviet Union, where law enforcement agencies obviously have yet to establish effective strategies to deal with this issue.

The ABA is continuing to promote community awareness of Internet safety in Australia. This is done through cooperative arrangements with a number of bodies, including state education departments. We have a web site which deals with this, and I would like to take this opportunity—with your leave, Mr Chairman—to table a number of documents which are

circulated widely. They are: *Tips to help your kids make the most of the Internet—safely!*; *Tips to help you chat safely*, which deals with chat rooms; *Tips for families on using filters for Internet safety*, which obviously deals with that issue; *Tips for dealing with spam*; a general *Cybersmart guide*; and *Help your kids make the most of the Internet—safely!*, which is a guide to our web site.

CHAIR—Who are these distributed to?

Prof. Flint—These are distributed widely. Through some of the departments of education they are going out to the schools; I believe that is happening in New South Wales and South Australia.

Mr Fraser—We are establishing cooperative arrangements with a range of education bodies to distribute those through schools and other relevant organisations.

Prof. Flint—They are designed by consultants with a view to making them attractive to children, as is the web site. They are not documents which would have been designed by a professor of law. They are meant to be attractive, readable and interesting for children but to contain those warnings which are so important and which may not be obvious to parents. For example, they warn that parents cannot rely on filters. They cannot be complacent about filters; filters have a role, but they cannot be relied on as the sole tool. They warn that there is a great advantage in having the computer in a public room rather than a bedroom—that is, the computer with the telephone connection—and that you do not hand your personal information to somebody you do not know. You do not meet somebody you do not know; you always go with an adult, and you are very careful. There are other provisions in those documents which suggest what should be done.

We are negotiating with the United States National Center for Missing and Exploited Children, which has a web site which centralises dealing with these matters in the United States and has a very large staff. It has its own complaints hotline and a form which you can fill in if you detect any material on the Internet which is completely inappropriate.

I might just briefly conclude by drawing the committee's attention to some of the regulatory issues. It has been suggested that if a complaint is made to the ABA it would result automatically in a police raid on the complainant's home. That is not so. On the other hand, the ABA suggest that it would be inappropriate to have a blanket provision which would ensure that complainants are never subjected to searches themselves, because that would be too easy an indication to those who are committing offences that just by complaining to the ABA they would gain great protection.

The police services continue to receive reports of child pornography directly. We deal with complaints about sites which are in Australia, and we do have wide powers to order a take-down of those items. When they are overseas we have, under the legislation, arrangements with the Federal Police whereby we notify the Federal Police if we are aware of some site overseas. In particular, we have an arrangement with the Federal Police which allows us to refer these matters to INHOPE.

INHOPE is an organisation which brings together a large number of regulatory and private bodies which deal with a very large number of complaints throughout the world. It centralises their resources. Rather than the complaint going to the Federal Police then being sent off to Interpol and then being sent off to the police in that country with the danger of it not being acted on as quickly as it might be, INHOPE has a charter to deal with these things immediately.

There are aspects of IT which are not caught by the legislation in terms of complaints. Complaints can only be made about matters stored on the Internet that are there semipermanently that you can go and check. It does not, for example, allow us to deal with complaints about chat rooms because a chat room—and I tested this analogy to make sure it was right because Richard is an expert in the field—is something like a conference telephone call where you have a number of people talking together on the phone. This is a number of people talking together on the Internet. I had to have it explained to me because I only send emails; I do not get into chat rooms. That is not covered by the complaints part of the legislation. You can only complain about something which is stored. However, it does fall within our brief in relation to education and we are certainly very much concerned with that, hence the publication on that and being in touch with the industry associations to ensure that they take some action in this regard. I might also mention that, because this is very much a police matter—inappropriate activity in a chat room is more a matter for the police than for the ABA—

CHAIR—It is interesting how everyone says it is somebody else's responsibility.

Prof. Flint—We think our responsibility is for education—

CHAIR—I understand.

Prof. Flint—because parliament has not given us a right. It would be very difficult. How would you find what was happening, because it is not being stored? If somebody complained to us, there would not be the evidence that we would need to deal with it. But I might draw your attention to a bill which has just been introduced into the House of Lords. It is the Sexual Offences Bill [HL], which makes a special offence in relation to this. Clause 17 of the bill is titled 'Meeting a child following sexual grooming etc.' and states:

(1) A person aged 18 or over (A)—

They make the legislation much more readable these days than they used to. (A) is a person over 18. He or she:

commits an offence if—

(a) having met or communicated with another person (B) on at least two earlier occasions,—

So the communication could be through a chat room—

he—

(i) intentionally meets B, or

(ii) travels with the intention of meeting B in any part of the world,

(b) at the time, he intends to do anything to or in respect of B, during or after the meeting and in any part of the world, which if done will involve the commission by A of a relevant offence,

(c) B is under 16, and

(d) A does not reasonably believe that B is 16 or over.

So it makes using a chat room or similar place for the purpose of engaging a child in paedophile activity a special offence.

CHAIR—It will be interesting to see whether they use it in terms of the current case that has had all the publicity.

Prof. Flint—Yes. That would be so.

Senator FERRIS—One still wonders how the evidence would be gathered for that. If the person denied having met and groomed the child in a chat room, how would the prosecution advance that case?

Prof. Flint—It would be a question of the onus of proof and, of course, the child could give evidence. Presumably there might be some records left in the computer—emails and so on—which could be tracked down. Richard would be more expert in that. It would not be beyond proving beyond reasonable doubt. Of course, having the legislation there gives notice.

CHAIR—Thanks for drawing it to our attention. We will follow that up; it sounds interesting. Do you have anything further before we proceed to questions?

Prof. Flint—Only briefly that the other part of our regulatory role involves the registration of codes of practice. We have been in contact with the associations. There are three codes of practice. They contain provisions which are there for the protection of children—for example, making filters available to all people subscribing to the Internet at cost or near cost.

CHAIR—Thank you for your presentation. We will follow it up in terms of the legislation. In terms of our inquiry, which refers to the issues of paedophilia, banking fraud and credit card fraud, the issue of child sex offences relates particularly to your area. The three aspects that concern this committee are, firstly, the transmission of pornographic images involving a child and access by children to pornographic images on the Internet, in the broader sense, and access to pornographic sites; secondly, the fact that Net Nanny seems not to effectively prevent chat rooms in particular; and, thirdly, chat rooms, which concern us and have had quite a bit of profile recently. Senator Ferris, would you like to lead off on the issue of chat rooms?

Senator FERRIS—Thank you, Chair. It is probably extremely timely to be asking you these questions, given the publicity this morning. As you were talking about the House of Lords legislation, I was reflecting that the girl involved in this chat room kidnapping in the United Kingdom is 12 years old but the fellow involved is described only as ‘a burly Bible scholar’. Unfortunately we are not able to know his age, only that he was in the Marines three years ago.

So he is clearly in the category that would be covered by the draft legislation you are referring to. On page 9 of your submission, you make the very obvious point that because chat rooms do not have content stored they are outside the scope of the ABA's complaint handling mechanism. If, for example, a chat room develops into email contact, would that fall within the area you could explore, were parents to discover this and make a complaint, or would you like to see your jurisdictional area broadened so that you were able to take into account material that begins with a chat room and progresses to other areas?

Prof. Flint—As I understand it, and Mr Fraser will speak further on it, these are not 'stored' in the sense that a site on the Internet is stored, so it is not within the intention of the legislation that we have a role there.

Senator FERRIS—But if the child develops a relationship which gets to emails, then they are stored.

Mr Fraser—Email is also a matter that is excluded from our complaint handling role.

Senator FERRIS—Currently.

Mr Fraser—Currently. That is primarily because it is seen as a one-to-one type of communication. If, for example, a person had discovered that the child was having email contact with a person, we would be referring them to a law enforcement agency, to the police.

Senator FERRIS.—It is not clear from the article I am referring to whether or not this meeting and the subsequent kidnapping of this child were based on something that developed from a chat room into face-to-face meetings and so on. You have a little pamphlet with tips to help you chat safely in which you suggest that parents should become involved, set rules and use tools. Surely that would suggest that you might like to have more jurisdiction over this? It seems to me that we are moving away from a situation where people are using Internet sites, because they know that they are being monitored and they know that law enforcement agencies are now interested in those. Chat rooms are the new opportunity for these types of people, with their various obsessions, to operate. Yet so far everybody is saying that they are not able to do anything about it, because it is not stored and so on. Is there somebody who is going to say that we need to start getting interested in this? Because children are coming home after school, their parents are not computer literate and they may be home alone, they are getting onto chat rooms. As you say in your pamphlet, they may be talking to someone who says they are a 12-year-old girl but could really be a 40-year-old man. Where are we going to go with this issue? We cannot all have our hands off it.

Prof. Flint—The problem is, of course, that these Internet sites are publicly accessible. Sometimes they may need a password but they can be accessed. With these chat rooms, it is like a phone conversation. Perhaps the engineers might be able to locate something from the computer and the computer's memory.

Senator FERRIS—Would you like to see police doing random chat room—

CHAIR—Audits?

Senator FERRIS—audits, yes, and going onto chat rooms and perhaps creating a personality to see what comes up? I just cannot see how we can all keep our hands off this.

Prof. Flint—I do not know whether that is feasible. I suppose it would be, because it is feasible to have telephone taps. You could have random telephone taps. The point is that, once you detect that something like this is going on, the police should be sent in immediately. It would be a waste of resources—and it would not achieve anything—if the ABA just issued an order to 'stop doing that'. What you need is for the man or woman in blue to go there and arrest that person or at least interrogate them.

Senator FERRIS—I am sure this mother wishes she had known that, but she did not know and this girl was able to describe this fellow as her American boyfriend and disappear with him. It must be extremely difficult. I cannot see why, just as this fellow was able to create an image on a chat room, we could not have law enforcement agencies or someone like the ABA create these identities and see what comes forward. If you created an image of a 14-year-old girl or a nine-year-old girl, for example, you might find it drew in people that agencies could then follow up.

Prof. Flint—What you really need is a dedicated squad of police to go there immediately something like this is detected. Our role should be to warn parents and children of the danger of this.

CHAIR—To what extent do you effectively do this? Because, although as parliamentarians we do not see a huge amount of television, I have never seen anything on television warning parents of the dangers. We have these brochures going out through the schools, which is good—we congratulate you on that—but in terms of community service announcements—

Senator FERRIS—Is it enough?

CHAIR—should we be doing more? You might say you do not have enough funding for it and so on, but the purpose of this inquiry is to look at these areas and see what recommendations we should make.

Prof. Flint—We are just reviewing the commercial television code of conduct. I made the heretical suggestion that perhaps, in addition to commercial television stations in Australia putting their ads in newspapers and radios about the changes in the code, they should put ads on television. That suggestion was received with some surprise. I would have thought that that would be the place where you would get people concerned about television. We do have a web site, and children who are concerned about the Internet can, we hope, look at our web site—and we hope the teachers are telling them to look at our web site, because we have been in touch with departments of education, trying to stimulate that. It would be a good idea if, in addition to that, there were television advertisements. Obviously, there would need to be a special fund for that.

CHAIR—Aimed more at mums and dads, I would have thought.

Prof. Flint—Yes, because as we know there are age questions here. As you get older, there is less likelihood that you use the Internet—because we did not have it when we were young—so easily.

Senator FERRIS—Can I take you back to your comment that perhaps there should be special branches of law enforcement agencies that carry out audits or some sort of exploratory measure in this area. Would you like to see that? Would the ABA be supportive of the establishment of special agencies who could look at chat rooms and carry out audits in that way?

Prof. Flint—I think it would be most appropriate for the law enforcement authorities—the police—at a state level and at a federal level to have specific areas involved in dealing with this issue. I am not sure whether they do; perhaps Mr Fraser might be able to tell us that.

Mr Fraser—It is our understanding that that is a technique employed by some agencies currently—they will go into a chat room to engage people in that way.

Senator FERRIS—But is that an informal thing or is that a regular audit that is in some way regulated and made public—so that, for example, parents know—and that is not a covert operation but a regular audit of chat rooms taken randomly that is carried out so that people would have some understanding that these things are not just a totally unregulated aspect of the Net?

Mr Fraser—Our understanding is that it is just part of their suite of investigation tools and that if they think it is appropriate in those circumstances they will try to engage someone in that way.

Prof. Flint—We are not aware of a random audit?

Mr Fraser—No.

Senator FERRIS—That might be something for us to explore. I was a little concerned to hear that there are only two states distributing these. Is there some resistance to the distribution of these?

Mr Fraser—It is simply a case of us being able to make contact with the relevant agencies and put the arrangements in place. We are progressively doing that, making contact with education bodies with a view to negotiating similar arrangements.

Senator FERRIS—What about places like computer shops and public libraries?

Mr Fraser—We have distributed samples of the material to all libraries, through the libraries association, and have responded to requests from individual libraries—

CHAIR—Why only two states? Is this because you have just started the program?

Mr Fraser—We are in Sydney and it made sense for us to start with the New South Wales education program.

CHAIR—Okay, so it is an ongoing program.

Senator HUTCHINS—On chat rooms, on page 9 you talk about Net Detectives. Would you explain that a bit more for us please?

Mr Fraser—Certainly. Net Detectives is an activity that has been developed by the body Childnet International, which is based in the United Kingdom. It is an online activity in which teams of schoolchildren solve a whodunnit scenario that has a chat safety theme to it. Indeed, we participated in one of these activities on Tuesday night of this week with schoolchildren in the UK. The children are given a scenario which gradually unfolds with clues from a control room of experts.

Senator HUTCHINS—Mr Fraser, do you know how old these children are?

Mr Fraser—The activity is aimed at upper primary and lower secondary students who are considered to be those who are going to be most engaged by that sort of activity. As the activity unfolds the moral of the story is that you do not know whom you are talking to online, that you should not arrange to meet without a parent someone that you have only spoken to online and that you should not be giving out your phone number, address and those sorts of details to someone whom you have chatted to online. As I said, we participated in one of these activities on Tuesday night. We have reached agreement with Childnet that we will actually run an Australian version of these activities, one in September this year and possibly a further one in November and further ones with Australian schools throughout the next 12 months or so.

CHAIR—As there is nothing further on chat rooms, we might move on to the general question of access via the Internet to pornographic sites and the adequacy or inadequacy of some filtering systems such as Net Nanny. Would you like to comment on that before my colleagues ask you specific questions?

Mr Fraser—Yes. On the issue of filtering, our advice to people really is that filters are a useful tool that they can use to help manage access to the Internet but they are not going to be 100 per cent effective.

CHAIR—Do you have information on what percentage of televisions actually have such a filtering system on them?

Mr Fraser—Sorry?

CHAIR—It was suggested to us yesterday that only one per cent of the Internet—sorry, not televisions—actually had these filtering systems on them.

Mr Fraser—No, we do not have figures on how many people are using filters. We recommend that they are a tool to be taken up if that suits people.

CHAIR—It was suggested to us that it was only one per cent so far.

Mr Fraser—Right.

Prof. Flint—The codes do require that these be made available to each subscriber. Do we not test them through the CSIRO, and then give the results of those tests to be included in the codes?

Mr Fraser—We do undertake testing of the effectiveness with a view to advising parents about what type of filter is likely to suit their circumstances. For example, if they have young children they may want to use a white list type filter, which restricts people to a very narrow set of Internet content. If they have older kids they might choose a black list filter, which works in different ways. We see our role as being one of providing that sort of information to help people make informed choices about the products that are available.

Prof. Flint—I would like to make two points. Firstly, we do insist in our advice that parents should not be complacent. They should not think that the filter does the role of supervising, because it does not. It either shoots too wide or it is too narrow. It lets in material that it should not, and it stops material that you would not be offended by if your children saw it. Secondly, when a site is found outside of the country containing seriously offensive material we notify that site to the filter corporations who then include it automatically so that it is filtered out in relation to Australians trying to access those sites.

CHAIR—So are you closing down sites that portray rape and killings? It was suggested to us yesterday that there are sites actually available that portray the absolute worst extremes of pornography. Are these sites being progressively closed down?

Prof. Flint—If they are in Australia—but they rarely are. When they are overseas, we notify the Federal Police or we notify INHOPE with the aim of getting them to close down those sites, because we cannot. In addition, we notify the filtering corporations, who then ensure that those sites are included in the filters.

Senator HUTCHINS—In your submission you talk about the difficulties with the old Soviet bloc countries. You say you are concerned that the Federal Police have difficulty getting the old Soviet bloc countries to cooperate.

Prof. Flint—That is a particular problem. A lot of these sites, I gather, are in the United States, which of course reflects the fact that the United States is such a home of the Internet. Naturally, a lot of those sites are going to be there. They can be dealt with, particularly through the centre that we have contact with in the United States and the American police. But the problem in the former Soviet Union, as you rightly point out, is that the police do not have the resources, the ability and perhaps sometimes—dare I say it—the will to progress to get these sites out of the way. I gather some of them are absolutely appalling, involving very young children in gross sexual acts. It is appalling, but it is something that is beyond the control, obviously, of the Australian authorities and only within the control of the sovereign state concerned.

Senator DENMAN—The age of consent varies from country to country, particularly in some European countries. Does that present a problem for you as well?

Prof. Flint—Not in relation to international material, because it is the most serious material which we are trying to stamp out or encourage the stamping out of. The fact that there are different ages in different countries does not really impact on us.

Mr Fraser—We deal with material as it would be dealt with under Australian laws. If it is something that needs to be referred to another country, we leave it to them to deal with.

Senator DENMAN—In your submission, on page 10, you talk about actions in categories to do with paedophilia, but you have not really made it clear how many successful prosecutions or convictions you have had.

Mr Fraser—We have certainly issued take-down notices for Australian material.

CHAIR—How often are you doing that in a year? How many times?

Mr Fraser—I do not have those figures in front of me, but on each occasion where we have issued a take-down notice to an Australian host that the material be removed, it is also referred to the relevant state or territory police force for them to investigate. In the case of overseas material, as Professor Flint explained, it is referred either to the Australian Federal Police or to another hotline body in the country in which it is hosted. Unfortunately we do not receive as much feedback as we would like from police forces about exactly what action is taken. That is something that we have flagged with the agencies—that we would like to hear more about the reports we send through. At this stage we do not receive much information back.

Senator DENMAN—Do you mean feedback from overseas or do you mean feedback from overseas as well as in Australia?

Mr Fraser—Probably overseas and in Australia.

Senator DENMAN—Thank you.

CHAIR—You have requested the computer suppliers to provide filtering equipment at no extra cost if it is requested. Do you think it should be a compulsory requirement?

Prof. Flint—I do not think so. That has been suggested, but all the advice that I have received is that it would not help—firstly, because it might make people complacent and secondly, because the filters at this stage are not perfect. They are overshooting and undershooting. There is only a chance—sometimes a high chance—that they will capture material. We do not think that a mandatory filtering would be appropriate. You would also have to examine the cost and the delay that that might incur in relation to the Internet. The industry associations tell us that this would add substantially to costs, which would then be passed on to consumers; that in addition it would slow down the system; and that finally—and I think that this is perhaps the most important—it would not capture everything that you would want to capture. Would that be so, Mr Fraser?

Senator HUTCHINS—On international liaison, in the third paragraph you say:

The ABA is represented at two of the four members meetings held each year ...

Is there any reason you do not go to the other two? You make the point that it is only two of four. If you were trying to hide it you would not mention it, I would have thought.

Mr Fraser—It is only that it is costly to attend one of those meetings. Quite often, even if we do not attend physically, we will participate by a teleconference in sessions that are of key interest to us or in which we are directly involved.

Senator HUTCHINS—And finally, you talk in your submission about convergent devices. In the final sentence you say:

The ABA also would propose that child safety concerns associated with mobile devices be addressed through codes of practice ...

Do you see those codes of practice as being voluntary, or do you see them being legislated? Either, or neither?

Mr Fraser—I suppose we would be looking at a similar model that operates for Internet service providers perhaps and for broadcasters. Our understanding is that the industry is quite keen to be proactive in this area and to take those sorts of measures to ensure that those services are not used inappropriately. So there may be quite a strong will to cooperate, even if it were only a voluntary code that was developed.

Senator HUTCHINS—It seems to me you are suggesting that this is the next area you have to tackle because, it would appear, every other area seems to be being addressed and now these mobile devices are looming and we need to do something about that. Would you like to comment on that?

Mr Fraser—It is certainly an emerging technology. From the contact that we have with bodies such as Childnet International—who have done work with Japanese telecommunications providers where 3G mobiles have been in use for some time and these sorts of safety issues have arisen—we understand they are working with providers to develop measures that address those safety concerns. Similarly in Europe, particularly in the UK, we understand the industry there is in the process of developing a code of practice that will address these and other measures. So I guess as these technologies take hold in Australia that is obviously something that we will be looking at.

Prof. Flint—These codes are halfway between a voluntary code and legislation. They are registered with us; they have some force. If we were to detect a breakdown in the codes, we do have a power to make a standard which then becomes obligatory on the service providers.

CHAIR—Following on from Senate Hutchins's comments, do you think there is need for a bit of speed in developing this? It seems from what I hear anecdotally that things are moving, particularly in the child paedophile area.

Prof. Flint—I think you are right. The only reason why 3G mobile devices, which are really phones with computers, are not widely used in Australia is the cost, and, obviously, the providers have difficulty in providing access because we are such a big country. In a country like Japan, which is a concentrated country, they have taken off. They will take off here, and they will be very big. The very big problem is, of course, that while we are saying to parents, 'Put the computer in the public room in the house,' we will soon have children wandering around with their mobiles. To the extent that they are not being supervised—and it is the way of children not

to be supervised 100 per cent of the time—they will escape from our suggested rule of putting the computer where the parents can supervise. I suppose one could ban them, but of course that is not going to happen; we do not ban technology for the reason that it is going to cause some problems.

One of the solutions, one of the ways in which we can address this, is obviously through information. I was very encouraged by what the Chair was saying about the need for a concerted and very strong advertising campaign through television, radio and so on so that parents who themselves are not computer literate are aware of these problems. There also need to be, obviously, resources in the law enforcement agencies to deal with them. They have so many things to do—if you go to the average police station, they are having great difficulty dealing with basic law and order issues, not new technical issues. So we do have a problem, and it is very important that this committee has been established, because you at least will be in the forefront of it and will be able to give advice to the nation before, suddenly, we find every second child is wandering round with a computer in his or her hand that can be misused.

CHAIR—I have a question about the closing down of sites. Do you have evidence that quite often these sites are reopened under another name? To what extent do we have that occurring?

Mr Fraser—Certainly material on the Internet does move around, and what is there today may not be there tomorrow. Yes, material does pop up time and time again.

Prof. Flint—I stand to be corrected by Mr Fraser, but I do not think we are aware of a site which we have closed down in Australia reappearing. Would that be right, or have we had some?

Mr Fraser—There has actually been one instance of that. It does present certain problems. Largely, the material that we have directed removal for has—

CHAIR—What would happen if a child pornography site on the Net were brought to your attention? Would you give formal advice to the person who put it on the Net originally and also to the police at the same time? Would they be followed up with a visit?

Mr Fraser—Are you talking about an Australian site?

CHAIR—Yes.

Mr Fraser—If it is Australian we certainly would not be in touch with the providers of the site in the first instance—we would contact the police. If we went knocking on the door, that might alert the people that —

CHAIR—Sure.

Mr Fraser—Initially it is a police matter. When we get the go-ahead from the police we would direct the removal of the material.

CHAIR—Then on what occasions would you just send letters out to the provider saying, 'Please take this off'?

Mr Fraser—If it were material that is prohibited under the act but not in the character of child pornography. For sexually explicit material we would straightaway direct removal of the content.

Prof. Flint—This is material which is non-criminal, but which is inappropriate to be accessed by children or, for some material, is considered inappropriate for adults. But it is not material which would constitute a criminal offence.

CHAIR—Is that according to the definition of the act of what is allowable pornography and what is not allowable?

Prof. Flint—The act requires us, in relation to Australia material, to seek a ruling from the Office of Film and Literature Classification in relation to material which is non-criminal.

Mr Fraser—That is based on the same guidelines that now apply to films and computer games.

Prof. Flint—I must say that we are not talking about a large number of sites—these are the sites in Australia. The great bulk of serial sites are offshore.

CHAIR—Is that predominantly the former Eastern bloc or is it the US as well?

Mr Fraser—That is mainly the United States, with the former Eastern bloc a distant second. But there is still a significant amount of material hosted in the Eastern bloc, or there is evidence that it has been produced in the Eastern bloc and has been hosted in the United States.

Prof. Flint—I must say that the American Supreme Court has made it difficult for the law enforcement authorities to exercise their fullest jurisdiction because of, what I find, their somewhat peculiar interpretations of the first amendment.

CHAIR—Yes, it does seem curious. The mixture of the Bible Belt versus civil liberties in the US is a curious mix.

Senator DENMAN—If an Australian has a site offshore in another country does that present problems under Australian law?

Mr Fraser—The process we would follow is that we would treat the material as though it were hosted overseas. But if we could tell that there was some Australian connection, such as where the domain name had been registered by an Australian person or there was other evidence that an Australian body had uploaded the material, we would be referring that to a police force in Australia. So we do have a process we can follow.

Senator DENMAN—Does that happen often?

Mr Fraser—It has actually happened in a case we dealt with recently. The hotline located in Denmark has brought to our attention a site that is hosted in the United States but there is nonetheless an Australian person connected with it. We have referred that material to the state police force for them to investigate and our understanding is that they are pursuing the matter.

CHAIR—Thank you for appearing before the committee. We will be sending you copies of the transcript for you to review before it is published. We appreciate your coming today, your forthright answers and the scope in which you addressed the issue today. We look forward to working with you, perhaps, in some of these areas. This is an important and rapidly changing area. Ten years ago these issues did not really confront us. But they are there now and they provide a challenge to us, so we appreciate your input.

Prof. Flint—May I say how much we welcome the initiative of the parliament to establish this committee. It is obviously very importantly bipartisan that the parliament be ahead of these problems and these emerging technologies.

CHAIR—Thank you for coming.

Proceedings suspended from 10.49 a.m. to 11.05 a.m.

SCOTT, Mr Brendan, (Private capacity)

CHAIR—The Joint Statutory Committee on the Australian Crime Commission to is examining recent trends and methods in cybercrime, with particular reference to child pornography; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime. I welcome Mr Brendan Scott. The committee prefers all evidence to be given in public, but if at some stage you wish to go in camera then please let us know. I invite you to make some opening remarks, and then we will proceed to questions.

Mr Scott—I have to say at the outset that my submission is not specifically about the areas that the committee is investigating, such as child pornography, and that is because I do not really have much knowledge in those areas. However, I have an interest in the cybercrime legislation because I have worked in the area as a lawyer—not as a criminal lawyer but as a transaction or contracts lawyer. I analysed the cybercrime legislation when it was before the New South Wales parliament and when it was last before the Commonwealth parliament in 2001.

My general feeling about the legislation was that it did not treat information crimes in an analogous way to how crimes involving physical property were treated. The committee I was part of felt—and I felt—that the approach taken was not an appropriate one, because it focused more on access to data and modification of data rather than the consequences of that access and that modification. I felt that the practical consequence of that would be the creation of a property right in information. If that is the case, or if I am correct in that assumption, then the legislation effectively acts as an industrial policy for IT without, I feel, the policy discussion of the consequences of that.

For example, the act has the concept of authorisation. Actually, there are two key concepts in the act that I think are problematic. One of those is the concept of authorisation. If you have a look at the legislation, it keeps coming back to unauthorised access to data, unauthorised this and unauthorised that. The word ‘authorised’ begs the question: authorised by whom? Who has the ability to authorise something? Let us say that I am an employee working at an office somewhere and that office has some software installed. There are possibly three people who might be able to give authorisation in relation to data for that software. They are that employee, the employer and, potentially, the provider of the software. The legislation, to my mind, does not make it clear who is able to give the authorisation; perhaps all of them can.

The other concept is that of restricted data. Restricted data refers to data which is stored in a computer which is subject to an access control system. It is not hard for me to think of cases which are not restricted data, but most, if not all, information which is stored on a computer is restricted data within the meaning of that term. Generally when you boot up a computer it asks you for your username and your password. The moment that you have given those you have been involved in complying with the requirements of an access control system to get access to the data that is on the computer. The legislative provision does not require that the access control system be subverted. All it requires is that there is access to the data.

That is one of the problems with the concept of restricted data. The other problem is that the access control system is not something which is inherent to the data, so if there are two ways of accessing the data—one of which is subject to the access control system and one of which is not subject to the access control system—how do you determine whether accessing the data is a crime within the meaning of the offence which is created? For example, a program might have a front end which asks you for a password, but when you give that password it simply reads another data file which is in a plain text format. Someone might be able to simply use a word processor to read that data file. If they read the data file have they committed an offence, even though they have not subverted the access control system? They are the two main concerns I have with the act. That all gets down to the fact that the act focuses on access to data and modification of data, rather than the consequences of access and modification.

CHAIR—How would you recommend that we fix this?

Mr Scott—That is a hard question. I am not even sure it is possible for it to be fixed while still retaining the structure of the act, because those two concepts go directly to the heart of the act. It is all about restricting access to information, and my point is: is it right to allow someone, without any limitations, to nominate some information as being capable of being protected by the act? By that I mean that, if they put it behind an access control system, as a result they criminalise any access to that information.

It is probably not as important today as it will be in the future. One of the important developments in information technology is digital rights management. The whole purpose of digital rights management is to put information behind access control systems. So, in the world of the future, I expect that most, if not all, information will be restricted data within the meaning of the act. If that is the case then there will be broad prohibitions on the dissemination of information.

So, to go back to your question of how to fix it, perhaps the answer is to rethink the approach or alternatively to try to limit the application of the act. Some of the provisions of the act explicitly state that if you go in and modify data but that does not have any effect—you do not actually impair the data—you are still liable; you still caused an offence. The issue for me is: should it be a crime if there is no actual or practical consequence of the person's action?

This is not specifically on your question, but there is another issue which I did not talk about in my opening statement: the possession of data. The act creates crimes where you possess data with the intent to do something bad with that data. The idea of possession makes quite a lot of sense when have something physical. I can say that I possess something that is in my hand, but it is more difficult to make sense of it in the case of information. There are a couple of reasons for that. First of all, I can store data on a whole heap of things and still have access to that information quite readily. I can store information on the Internet and just go with my browser to get that information. Does that mean I possess that data, within the meaning of the act?

The other thing about data is that you may find it difficult to dispossess yourself of it. If you delete things on a computer, they are not necessarily deleted. There was a case—I think it was in the mid-nineties—which involved child pornography in the ACT. A person called the police and said: 'I've got this stuff on my computer. What should I do with it?' He deleted it, and they got a warrant to go in and have a look at his house. The computer does not erase the data; it simply

throws the filing card away. So, if you go in and analyse the computer, you can still find the data. So there is the question of what it means to possess data. You need some technical knowledge or the effluxion of quite a lot of time to delete the data because it needs to get written over on the hard disk.

The other aspect—and I cannot remember the specific wording in the legislation—is the data or the information that you have. If I know someone's password, it is not easy for me—short of getting concussion—to divest myself of that data. I guess there is another issue: the act makes use of the word 'possession' but it is not clear to me that the word 'possession' makes the same sense as it does when you talk about physical items.

Senator DENMAN—Then how do you define 'possession'?

Mr Scott—That is a good question and I think it identifies the difficulty with the concept. What if there are instructions on the Internet about how to break into a specific computer, for example, and the availability of that information on the Internet counts as possession? The problem is that if you regard the Internet as a means of possession then people, if they have knowledge of the act, will not possess it on a computer—they will possess it by putting it somewhere where they can access it. Do you understand what I am saying?

Senator DENMAN—Yes.

Mr Scott—The problem is that if availability of the information over the Internet is possession within the meaning of the act, it means that mere intention can become a crime. Because you form an intention to do something and because you theoretically have access, possession can be implied.

Senator DENMAN—To ask a hypothetical question, when would you actually take possession of an email?

Mr Scott—It is clear that when I receive the email and it is on my—

Senator FERRIS—Is it not when you open it?

Mr SERCOMBE—Is it when the computer receives it or when you receive it?

Senator DENMAN—Is it when the computer receives it or when you open it?

Mr Scott—I think I would possess the email prior to opening it.

Senator DENMAN—What if it had some illegal content? How long would you then have before you had to report it to the authorities?

Mr Scott—I do not know. But that is another problem. What if I am away on holidays?

Senator DENMAN—Exactly. That is why I wondered when you take possession of it. I would have thought it would be when you opened it, surely.

Mr SERCOMBE—It is not the issue, in terms of the practical effect of Australian criminal law. We are talking a lot of legal theory. Mens rea comes into it—the guilty mind. If there is an absence of intent it would be pretty difficult to get a conviction. It is an interesting theoretical discussion but, given the criticisms you make of the structure of the cybercrime legislation, is there an alternative model elsewhere in the world that we can look at, in terms of addressing some of the theoretical issues you raise? The discussion is principally theoretical, I would have thought.

Mr Scott—I am not aware of any. I do not know if you know of the pedigree of the cybercrime legislation, but it is based on a European model—either European or from the UK—and I think the legislative provisions come from draft UK legislation. So it is not as though Australia is stepping out on its own in taking this approach, but I still feel there are problems with the approach.

CHAIR—We are looking at some of the problems of the cybercrime legislation, so it is appropriate that we raise some of them. Looking at possible solutions and what other people are doing offshore is an issue for us. One of the questions I have is about your concern that discretions available under cybercrime legislation make illegal a broad range of activities which persons would not ordinarily consider criminal, with those discretions being the only things lying between reasonable acts and criminality. So how would you suggest that these offences be approached?

Mr SERCOMBE—Would you agree with the proposition that criminality requires a question of intent to be proven as well?

Mr Scott—Yes, but—

Mr SERCOMBE—So in terms of the points you are making—they are essentially theoretical points, aren't they—in the absence of an intent, a court is not going to convict on a criminal ground?

Mr Scott—That is true. I think part of the point I am making, though, is that in some cases intent alone can constitute the offence. This goes back to the discussion of possession I was having earlier. If you have this idea of constructive possession, where the information is available to you, then the mere formation of an intention can be the offence itself. You might say, 'Well, if I form that intent no-one will ever know about it'—

Mr SERCOMBE—But that is common in all sorts of areas of the law. Attempted murder is a criminal offence: you have not actually carried out a murder; you have just formed the intention to do it. It is not as if this is a unique proposition.

Mr Scott—I think it is different in the case of information because physical items have characteristics as a result of their physicality, which tends to mean that they only have application in certain circumstances. A crowbar, for example, can be used as a housebreaking implement or it can be used for other things. But information is much more fluid, in that a piece of information does not have those necessary characteristics. I can have some information: today it might be innocuous, but tomorrow I may be able to use it, because of changing circumstances,

to devastating effect. I am trying to think of insider trading as an analogy but I cannot work out the details of what an analogy would be. I am sorry—what was the original question?

CHAIR—It was really the question that we had regarding your claims about the criminal act and the discretions available under the cybercrime act, and about the discretions being the only thing lying between reasonable acts and criminality; and questions about how you would suggest these offences be approached.

Mr Scott—I guess the gain is trying to give some more meaning to the definition of restricted access—

CHAIR—Yes, as you mentioned in your opening claims.

Mr Scott—Yes, but also to refer the offences back to some consequence. I keep saying that, and it is not something I put in my submission, so I guess what I am saying is: the absence of a reference to consequences is a problem with the act in my view. And that is because I am taking a position which says that access and modification in themselves should not be crimes.

Senator HUTCHINS—I am very computer illiterate but when we talk about these trojans—you talked about the absence of reference to consequences. Earlier, in Canberra, reference was made to people setting what are essentially time bombs in computer systems. I recall that it was said that there is no penalty for people who set those time bombs. So we know that they can wipe out a computer system in five minutes on 14 July 2005. Is that what you are referring to? How would you respond if, say, there were some sort of mechanism to punish people who do things like that?

Mr Scott—Referring it back to consequences, I would need input from someone with more criminal law expertise than I have. But I am not saying that the consequences would have to have occurred; I think it would be sufficient to say that the consequences were intended or were a likely outcome of whatever they were doing. The issue of recklessness as to consequences is a difficult one, often because it is very difficult to know what the consequences of your actions might be when you change data, and perhaps that is a reason why the report came up with legislation which says that access alone or modification alone is an offence. But if you create a situation where mere modification of data is an offence—and while you may think of it in terms of someone intentionally changing something, pretty much any time you use a computer you are modifying data—the scope of that provision is very broad.

CHAIR—Thank you for that. We appreciate your input and we appreciate your coming here today. We may get back to you with some questions, given your technical expertise in the area.

Mr Scott—I referred to a submission I made to another committee. I brought along a copy of that submission, if you would like it, because when I submitted this submission it did not occur to me that you might not have direct access to that other submission.

CHAIR—Yes, that would be great. We appreciate your coming. Thank you very much.

Mr Scott—Thank you.

Proceedings suspended from 11.32 a.m. to 11.46 a.m.

BURKE, Mr Tony, Director, Australian Bankers Association

GEURTS, Mr John, Executive General Manager, Group Security, Commonwealth Bank of Australia

CHAIR—Welcome. This public meeting of the parliamentary Joint Statutory Committee on the Australian Crime Commission is examining recent trends in practices and methods of cybercrime with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime. The committee prefers that all evidence be given in public but, should you at any stage wish to go in camera, if you advise the committee we will consider your request and then proceed in camera. I invite you to make some opening remarks about the committee's inquiry into cybercrime. At the conclusion of your remarks I will invite members of the committee to submit questions to you.

Mr Burke—I will speak first and then my colleague John Geurts will make some remarks from the perspective of a bank. I represent an industry association. Thank you for the opportunity to appear before the committee today and for the opportunity to make a submission on a crucial matter for us and a matter most important to the customers of our members. ABA does not wish to amend its submission and does not wish to give any evidence in camera today.

Firstly, I will offer a little bit about the ABA. We represent banks in Australia. Our membership is open to any entity which holds a domestic banking licence. We have some 23 members. They include the larger national banks and also regional banks and a number of international players. Our job is essentially about policy and public advocacy. A major policy area for us, driven very much by our recent research on the attitudes of customers and those of other stakeholders, is fraud and security matters, including those within the terms of reference of this inquiry. Within our submission we presented a deal of material. We took the opportunity to present a number of facts and some information in relation to cybercrime as well as what banks are doing to respond to the threat and what the ABA is doing at an industry level.

Within our submission—and I will confine my remarks to our submission—we spoke about a range of programs. We spoke about programs which banks individually take, the measures that banks have implemented to respond to this threat, and industry responses. Chief among those at an industry level is the education of customers, merchants and other parties to ensure that all are aware of the risks and are acquainted with measures for mitigating them. Industry risk management is essentially about identification and verification mechanisms to ensure that we know the true identity of those individuals who do business with the banks and that we conduct ongoing monitoring of account activity for those individuals and entities. As you would know, we have a very strong relationship with AUSTRAC, to whom we have obligations to report suspicious transactions. In more recent times there have been matters of suspicion arising from traditional crime and traditional money laundering. To that we have added a focus on the suppression of the financing of terrorists.

In the last six months we have instituted at the ABA level a fraud task force which has a very broad representation. It includes the heads of all the fraud squads of our members, the fraud chiefs of state and territory police services, the AFP, the High Tech Crime Centre, AUSTRAC, insurance industry representatives, credit union and building society representatives, and the New Zealand Bankers Association. I am sure I have missed a few, but the representation is very broad. The task force is very focused on specific new and emerging threats. Within its scope of interest, cybercrime certainly plays a significant role. Earlier this year we announced a number of projects that the task force is taking on. We were pleased to hear an announcement from Senator Ellison's office in recent days on the so-called identity verification gateway, which will dovetail very nicely with a couple of major projects that the fraud task force is taking on.

The key recommendations in our submission had to do with sharing the role of educating the public about their responsibilities and/or means of avoiding harm. We spoke also at some length about our desire to work collaboratively with government on critical infrastructure protection. I am pleased to say that since this submission was put forward there have been a number of developments. On our side there has been the development of a banking and finance infrastructure advisory group. We are looking forward to the first meeting of the Critical Infrastructure Advisory Council, to which our advisory group will report. Finally, we recommended that there be further consultation and research between government and industry on cybercrime developments and how to protect the interests of our customers.

CHAIR—Thank you very much for your opening statement. In your submission you say:

> The current regulatory framework covering cybercrime is satisfactory and no further legislation or regulation is required at the Commonwealth level.

That seems a little unusual in terms of not only some developments that have occurred but also the claim in your submission when you say:

> Customers have a vital role to play in protecting their own interests, and banks will continue to provide financial literacy programs including cybercrime self-protection.

A case involving the Commonwealth Bank was outlined to us yesterday by Mr Graeme Bond. It seemed that in terms of credit card fraud the banks were accepting very little risk themselves, as they passed it all back to the agents. In that case, despite the fact that Mr Bond had been through the process of talking to his bank manager about the case and whether it seemed appropriate, when the crunch came and it turned out that he was involved in a scam—which can happen to any retailer—there was no hint of any consideration by the bank at all. It took absolutely no risk and passed it all on to him. He ended up with a debt of $141,000 and went bankrupt as a result. I wondered what comments you might have on that, Mr Geurts, and on the broader base, Mr Burke, on this whole area of fraud, scams and so on, and what responsibilities the bank has in that. If you do not take any of the responsibility, it is not surprising that you do not think that any further regulatory changes are necessary.

Mr Geurts—May I point out from the outset that I am not aware of this particular case. I note from Mr Bond's submission that it may date back to 1996. I have been head of security for the Commonwealth Bank for less than three years, so I do not know this particular case.

CHAIR—You might like to write to our secretary with details as to why the bank believes it handled that case appropriately—or inappropriately, as the case may be.

Mr Geurts—Yes, I can do that.

CHAIR—Thank you.

Mr Geurts—Perhaps I could outline the situation as it is now for the committee, to give some comfort that, whilst I do not know about this particular case, certainly some of the matters it raised are not the practice now. There are two types of transactions with credit cards. The first is a card present transaction, where you swipe it through a terminal or a machine, and the second is a card not present transaction, where you might make an order over the telephone or Internet. In that situation it is more difficult to validate the card.

On credit card fraud generally, the bank and the schemes have invested millions of dollars in credit card fraud prevention and detection mechanisms. By way of example, both MasterCard and Visa have recently launched online verification schemes, called 3-D Secure and Verified by Visa, to validate online banking transactions with credit cards. This is where the bank takes the charge back risk in the case of fraud. So that issue has been addressed by the industry and certainly by the Commonwealth Bank. We take the risk of fraud in Internet transactions where they were processed through the Verified by Visa or the MasterCard 3-D Secure framework.

In cases where an Internet or mail order transaction is charged back to the merchant, there are two issues. Firstly, the merchant is told in the agreement that there is a 90-day charge back period where, if the transaction was fraudulent, the bank reserves the right to charge the transaction back to the merchant. Secondly, we have found through working with many of our customers that internal processes and procedures within the organisation accepting the transaction may also contribute to the risk of fraud.

Generally, if we consider that in a mail order business you provide the goods or value for the goods instantaneously without giving yourself or the bank the opportunity to validate the transaction, you are actually handing over value for goods prior to the cheque clearing in the physical world. So business processes, as well as close attention to fraud prevention by the banks, would solve those issues. For both our credit card customers and our credit card merchants, every day online we do full prevention and detection techniques. By early morning every working day we are aware if there is a scam or a fraud targeting one of our merchants and we take immediate steps to inform the merchant.

CHAIR—But would you necessarily know if, through a skimming device, they have picked up a legitimate cardholder's card? That would not appear for some time.

Senator FERRIS—Can you tell us how you would know? What signs of fraud do you look for?

Mr Geurts—We have invested many millions of dollars in rules based technologies that validate all transactions that go through either a credit card or a merchant. There is also some neural technology applied—we develop activity patterns for the normal business of a merchant so you can tell if suddenly there is a rush on a particular type of transaction. There are two

possibilities there: the merchant might be accepting transactions that he should not be accepting, or it could well be that there is a fraud being perpetrated on us.

CHAIR—What do you see as transactions that they should not accept?

Mr Geurts—In relation to our automated fraud routines, it really is a pattern of behaviour. Our analysts go in and talk to the merchant or customer to validate whether the transaction is theirs or not. For example, we make over 300 calls every day to our customers to validate credit card transactions. If there is a credit card transaction that is out of character, two transactions in different countries at the same time or an Internet transaction that is out of character for the customer, we ring the customer to ask them: did you make the transaction? Do you still have the card with you? That is often how we pick up credit card skimming, and we wear significant losses.

Senator FERRIS—Would it be possible for the committee to go and have a look at how you do this? Do you operate this from a centre somewhere that we could go and have a look at?

Mr Geurts—We can give you a briefing on how it operates. Because we are using live customer data, I would have to take in on notice as to what we can show you. But we do have those systems.

Senator FERRIS—It would be interesting to have a look at how you do it.

Mr Geurts—I will take that on notice and get back to you.

Mr Burke—I guess, John, there would be a demonstration capability to be able to say, 'Here are the exceptions and this is how they are generated.'

Senator FERRIS—It would be quite interesting to see it.

CHAIR—Take this case of your customer. Because the size of the initial transaction was $41,000, you would think that that would have happened immediately. In terms of these rules, you would think that you would have been calling the customer. Or did that not occur in 1996?

Mr Geurts—I was about to say that in 1996 this technology did not exist. The banks have invested quite heavily since the late nineties in this technology, so this technology has become available since 1998-99. This case may have actually predated it, but, as I said, I do not know this case.

CHAIR—I has happened to me. Credit card companies have rung me to verify transactions.

Mr Burke—The technology of which Mr Geurts speaks has a very high penetration in banks. They are all now using similar tools.

CHAIR—To what extent? In terms of the call back, how often, or in what percentage of cases, would you find or register a problem?

Mr Geurts—By the time we contact our customers, we have a false positive rate of about one in 20 calls. There are many thousands of transactions every day that go through the system. I do not have the exact figures.

CHAIR—It would be interesting to know.

Mr Geurts—We may be able to provide them to the committee in camera. I will take that away—

Mr SERCOMBE—But one in 20 you discover are—

Mr Geurts—potentially fraud. That is for one in 20 of the calls we make.

CHAIR—You have alert services for customers. What about the merchants? Do you also alert them?

Mr Geurts—Yes, we do. Because the credit card systems for the merchants are an overnight batch system, by early each morning—eight or 8.30—we have an idea of which merchants' activities the previous day may give cause for alarm. We either speak to the merchants or conduct further analysis to determine whether or not there is fraud there.

Senator FERRIS—Would that be based on size—amount of money—or regularity or types of purchases? What are the criteria that trip the system?

Mr Geurts—It is very complex. It is all of those. The size of the transaction, which may be too small or too large; the regularity; the frequency—all of those go into quite a sophisticated neural model that is global.

Senator HUTCHINS—I read somewhere, either in the ABA's submission or somewhere else—it may have been in a document from the New South Wales Police; I cannot recall—that merchants are involved themselves with credit card skimming. It was suggested that illegal migrants are stood over to do this. When you hand over your credit card, you lose sight of it for some time. They are skimming it, and then they bring it back. That sort of concern is there too. I think you also mentioned a situation where someone went on a spree through Kuala Lumpur and Taiwan—he even had a cup of coffee, I think, in Kuala Lumpur for 10 bucks—when the other person said, 'I was in France at the time.' That sticks out. But if you get my credit card in Sydney and go and dine down here or somewhere else, how does that register on the screen?

Mr Geurts—From a general point of view, we have been alerting our customers for some years now not to let the card out of their possession. Nevertheless, organised criminal groups have globally become quite sophisticated in credit card skimming, and the banks wear the loss of that skimming when it does occur. The issue there is that it can take some time to discover. Until the cards get used, you do not realise that they have been skimmed. It is a constant threat. We work very closely with law enforcement. We have a very successful task force in New South Wales, with the New South Wales Police, targeting skimming. It is an ongoing threat, and the banks, the schemes and law enforcement work very closely together on it.

Mr Burke—I imagine that whatever the means of compromise, including the one to which Senator Hutchins refers, the tools pick it up—whether the compromise was via a skimming device or via some other means.

Mr Geurts—Yes, but—

CHAIR—It is a shame you did not pick it up in 1996, when the merchant had to wear the lot.

Mr Burke—Although, interestingly, some of the discussion we have had touches on a particular point raised in the submission, namely the alert mechanisms for merchants and the claim that, as I understand it, there were not so many in existence. In addition to that which occurs at the acquiring bank level, the card schemes themselves—Visa, MasterCard and so on—have extensive alert programs in place. I cannot comment on what might have been in place in 1996.

Senator FERRIS—The interesting thing about this fellow though is that he went to the bank to check that there were enough funds in the account, and there were. So it was not that he took it at face value; he was very nervous about it. He went to his local branch and inquired whether or not the funds were available. I am not trying to provoke you at all. I realise you do not know the detail of it. But when you have an opportunity to look at the *Hansard*, you will see that he was always worried about it and he constantly went to the bank to try and do as much as he could back then to ensure that there was validity in the transaction.

CHAIR—We will send you a copy of the *Hansard* of his evidence as well so you can look at it before you respond. We do not wish to get bogged down on one case because, obviously, we have the whole issue of where we are today in 2003 and what mechanisms are there.

Mr Burke—Again, I cannot comment on the case simply because of a lack of knowledge, and it is not the ABA's place to comment on matters concerning an individual bank and a customer. But it raises a general point: while it is the case that banks, as Mr Geurts has been saying, have a wide variety of measures in place and have very large investments to prevent fraud and other forms of harm, banks cannot control the entire environment. Banks, and others, control the banking system so that the environment within the merchant's premises—whether virtual or physical—is not under the control of the banks.

CHAIR—I understand that.

Senator DENMAN—It has been reported that skimming is costing the Americans $110 million a year. Are they more sophisticated than we are? Why is it not costing us $110 million a year?

Mr Geurts—It that their losses?

Senator DENMAN—Yes.

Mr Geurts—I am not aware of those statistics.

Mr SERCOMBE—Are you able to assist the committee with any profiling or any observations based on the Commonwealth Bank's experience of the nature of the fraud that your customers, both merchants and retail consumers, experience? Are there any characteristics that are noteworthy in the generality?

Mr Geurts—For the purpose of this committee, the most noteworthy characteristic we have seen in the last two years is the increasing transnational nature of this type of crime.

Mr SERCOMBE—So it is being done offshore?

Mr Geurts—Offshore gangs may compromise the card overseas. They may actually compromise it here in Australia. The funds may be channelled offshore or withdrawn from ATMs overseas. So the biggest issue that concerns us is the level of vigilance of both the financial community—and the banks, in particular, who are at the front line in protecting our customers—and law enforcement to develop the skills, processes and understanding to deal with a problem that is not local. It is not just in New South Wales or just in Queensland; it crosses Australian borders and international borders. That is why it is particularly important that we collectively, as a community and as an industry, develop the relationships required, both within this country and overseas, to address the growing fraud problem.

Mr Burke—Mr Sercombe, have you seen the Australian Institute of Criminology's recent report on serious fraud in Australia?

Mr SERCOMBE—Yes, I have.

Mr Burke—That has some profiling.

CHAIR—So is it usually organised crime or does it vary?

Mr Geurts—It varies. I think organised crime, and I am probably not telling the committee anything, means a lot of things to a lot of people. They are organised groups so, given the official definition of 'organised crime', yes. As to if it is traditional organised crime as people would think, I do not know but there is a degree of sophistication to their work.

Senator FERRIS—Mr Burke, has the ABA a mechanism to share information when skimming becomes known? For example, if one of the members—say the Commonwealth Bank, as Mr Geurts is here—becomes aware—and I go back to that particular example where he subsequently discovered this—that small computer shops were being targeted by a particular gang, do they have access to a mechanism whereby they report it to you? Do you then send a note around your members? Is there an information-sharing thing or does the competitive nature of our banking system mean that that information is not shared?

Mr Burke—No to the latter. There is certainly information sharing. For some long time the ABA has had a fraud working group comprising the heads of fraud and that has been used as an informal information-sharing mechanism. I have to say, in relation to that working group and others in the ABA, that I have been pleased and surprised at the extent to which banks are willing to share information.

Senator FERRIS—Could you take us through a practical example of how that might work?

CHAIR—An episode of skimming.

Senator FERRIS—Yes, somebody who has been targeted by somebody in this way. Can you show us the practical way in which that would work as a case study?

Mr Burke—Yes, and I would also like to talk about the future because what I have just described has been a historical process. What we are moving to now within the fraud task force, a larger body, is to formalise that and to actually put in place a database, a restricted site to which the banks will submit information and be able to share that. Traditionally, the way it has worked is that sometimes it has been an individual instance of fraud simply because that particular instance perhaps represented something new. At the start of skimming becoming more recognisable, then there were individual instances reported. They were reported between the banks simply as we need to be aware that we have suddenly noticed that this particular mode of fraud is occurring. Otherwise it has been more general.

I will give you a specific case. You might recall the Internet cafe examples earlier this year up in Cairns where there was a compromise which relied on a piece of software being installed in a PC in an Internet cafe. That piece of software recorded the keystrokes of people using it, and by simply analysing the data one was able to isolate that which pertained to a banking transaction. While fairly small in scale, that was recognised as more of a systemic threat. That case was brought to the fraud working group, as it was at that stage, by the bank that first became aware of it—that is, before it hit the press—and there was analysis at a fraud working group meeting of what banks needed to do to respond to that particular category of threat.

Senator FERRIS—How quickly did all that happen?

Mr Burke—There was a teleconference within a day of the reporting bank becoming aware of it and then it was discussed again at a fraud working group meeting, as my recollection is, a couple of weeks afterwards. So there was initially a telephone conversation and then, more formally, we sat down and explored the details.

Senator FERRIS—I am reassured by what you say but, in testing that, I guess that within 24 hours there could be many thousands of dollars racked up on somebody's personal credit card details that might have been picked up in that way, whether in Cairns or by telephone or by Internet purchases around the world.

Mr Burke—Yes.

Senator FERRIS—If that were to be the case, whose responsibility would that debt then be?

Mr Burke—If I could just take a step back in my explanation, there was a piece I did not give, which is in advance of the ABA getting into the picture in terms of being a hub of information. There has always been a very strong informal network between the fraud investigators and other officials within the banks, who immediately tell each other what is happening, as well as the involvement of law enforcement and communication there. I would not want you to think that nobody was taking action proactively to disseminate information on an

incident. But as to the further question, yes, of course, even with that multistage response, further compromises could have occurred and hence further losses. The bank practice is that typically in those cases—and the customer does not wear the loss—

Senator FERRIS—Do the merchants?

Mr Burke—No, the bank does.

Senator FERRIS—The bank takes the loss?

Mr Burke—Yes.

Senator FERRIS—So none of the merchants who supply goods on the fraudulently obtained credit card details actually bears the loss?

Mr Burke—I cannot give you data on that specific incident and what exactly happened, but the general practice is—

Senator FERRIS—There is no set of principles on it, I suppose.

Mr Burke—Even in those instances—and I need to be careful: this is not a promise; this is a practice that banks have—where a customer has done something quite irresponsible banks would be prepared to take a fairly charitable view.

CHAIR—Banks—not the merchants?

Mr Burke—I am speaking of the bank practice.

Mr Geurts—Senator, I think I understand the question you are asking. Our current merchant agreement is that, if the card is present and it is a skimmed or fraudulent card, the bank will suffer the loss of that transaction. If the card is not present—that is, it is an Internet transaction—and the merchant has not availed themselves of services such as 3-D Secure or Verified by Visa where we take the risk, they will still have, in cases where the card is not present, the charge back risk if the card is skimmed or used unlawfully. That is why we have moved to these new mechanisms to take the risk back to the bank.

Senator FERRIS—How well understood is all this?

Mr Geurts—It is very clear in the merchant agreement. Also, even in my fraud group, we—as do most of the banks, I would imagine—send out advisories to our merchants to warn them about these sorts of frauds.

CHAIR—Could you be clear in terms of where you take the responsibility and where the merchant does?

Mr Geurts—In a card present transaction, where it is processed online and validated online, we take the risk.

CHAIR—That is where our merchant had the problem because it was over the phone.

Mr Geurts—Yes. Many of your secretaries would make travel arrangements for you by quoting your credit card number. You can imagine the catastrophic losses banks would suffer if a merchant chose not to use an alternative mechanism, which is now available. You should also understand that in many cases the merchant is actually unsecured by the bank. Therefore, if the merchant does fail there still is a risk for the bank as well, but that is a separate issue. If the card is not present and they are not using 3-D Secure or Verified by Visa—American Express have a particular scheme as well—to provide extra validation for the transaction then the merchant still wears the charge back risk.

Mr SERCOMBE—Why would a merchant not go through that process in the normal course of business? What circumstances would give rise to that, short of the merchant being involved in some scam? Is a lot of it just negligence or are there other circumstances where a merchant may choose to expose himself?

Mr Geurts—It can often depend on the nature of the industry and how you set up your business. If we talk about, as Tony did in his early comments, how business is about risk, sometimes merchants will take a risk too. They want to get out very quickly to the community and they want to offer this convenient phone booking service. That is a business risk they are accepting if they have not developed their own business processes satisfactorily to mitigate the charge back risk, which is brought to their attention in the merchant agreement.

CHAIR—When you establish credit card facilities with a merchant is there a briefing or are just written documents provided?

Mr Geurts—I cannot answer that, because I am not part of the process. I know that the written terms and conditions are in the information packs. In terms of each individual merchant I cannot answer that question.

Mr Burke—I would like to make a point of clarification, if I may, Senator Ferris. I began to talk about the case and how it was handled. The Internet cafe case was about Internet banking—that is, it was not a credit card transaction. There was no merchant involved.

Senator FERRIS—But there could have been?

Mr Burke—Yes.

CHAIR—What about the cases that have been brought to our attention—not least by my wife—of notices on the Internet saying that they are from the Commonwealth Bank and requesting information relating to account numbers and so on to ensure that it is accurate? How much of a scam is operating in that area—that is, people making out, through the Internet, that they are part of an established bank and that for verification you should provide your details et cetera? What losses are occurring and who picks up the cost of that?

Mr Burke—We have seen instances of that. At this stage, based on the information which comes to us, the volume of incidents is still fairly low. If it is the case that customers have

suffered a loss, because they have been duped in such circumstances, the practice to date—not the policy but the practice—has been that those customers have been recompensed.

CHAIR—I am encouraged by the fact that, having been brought to the committee's attention, it was then put up on our own web site or our own intranet. Are all banks acquainting their customers with the problem at the moment?

Mr Burke—Yes, indeed. There is material on this specific point on the major bank web sites that I have looked at. Also, and John might have a comment on this, there is a deal of investment in the IT departments, who are proactively looking for these sorts of things.

Mr Geurts—That is correct. Obviously one of the issues banks are now faced with is that our security perimeters, which we invest in very heavily to protect and secure, do not extend to the customer. As Mr Burke said, we have extensive awareness messages on our web sites and help desks. Part of my responsibility is as the chief security officer of the Commonwealth Bank. In our security model, we integrate IT system monitoring as well as account monitoring for this sort of activity so that we can respond very quickly, as these crimes can happen far more quickly than they would with the delays in paper based fraud. We are very active in addressing this issue. It is slightly out of our control in terms of directly influencing customers' computers and their responsibilities for keeping virus protection and so on up to date. I also have a fundamental view that many of these scams, such as emails and get-rich-quick schemes, are really variations on paper schemes that have been around for 20 to 50 years. It is just the medium that has changed.

Mr Burke—And the speed.

Mr Geurts—And the speed and our responses change. It is like the Nigerian fraud letters. They used to be very crudely typed letters; now they are crudely typed emails. But the fraud is still the same.

Senator FERRIS—There are a heck of a lot more of them.

Mr Geurts—Especially when they get your address!

Senator FERRIS—What about bogus sites? We are aware of an example where a bogus Commonwealth Bank site was set up. Somebody received an email which appeared to be from the Commonwealth Bank and which said: 'Dear valued customer, we are doing a check. Can you verify your account numbers? Can you verify these things?' How often does that occur and, when it has occurred, how has the bank responded to that?

Mr Geurts—It has occurred on several occasions in the last few months. We have always advised our customers that we will not ring them and ask them for their password. If they want to call in to us, they should call one of our recognised numbers. When we became aware of that, it was an event that we expected could happen at some stage and, when it did, we were ready to respond. We worked very closely with the Australian Federal Police in that case on the international aspects of that investigation. We worked very closely with the police here in New South Wales, and in one case the New South Wales Police were able to make an early arrest based on our information.

Senator FERRIS—How long did it take you to find out that it was happening? Was it days or weeks?

Mr Geurts—Hours. It was hours before a customer queried it. We try to educate our customers in the cyberworld, and they were very quick to alert our help desk. Our help desk has the procedures to alert us, and then the fraud response people and the IT security response people get to work very quickly.

Senator FERRIS—Were you able to find out how that was able to be created?

Mr Geurts—I cannot comment on some of these cases that are currently still before the court. But generally speaking—

Senator FERRIS—Can they download your logo and all that sort of thing very easily? Are there no firewalls on those things?

Mr Geurts—No.

Mr Burke—They do not actually have to download them. There are known factories out there in cyberspace for creating these things. Law enforcement agencies target these—that is what the response is. They do not need to actually take anything from the Commonwealth Bank.

Mr Geurts—They do not breach our systems to get the information.

Mr Burke—I think, as a general point, we are all sometimes lulled into a false sense of security behind our PCs and Macs. The Internet is a very scary place. There are the white knights out there who are chasing fraudsters of this type all the time.

Senator FERRIS—And the black pawns.

CHAIR—There was another issue brought to us—as you will remember, Senator Ferris. It was a case about offshore nationals contacting people of the same national background who had come to live in Australia to establish bank accounts which could then be milked. Have you had much evidence of that?

Mr Geurts—There is some evidence of that occurring. That is not to say that the people in this country who were duped into assisting are actually aware they are assisting a fraud. They may just think they are a commission agent helping to channel funds offshore. We are aware of that, and it is something that we are actively addressing. Again, whilst ever the funds are in the banking system there is actually a chance of interdicting those funds if fraud occurs, if you act very quickly.

CHAIR—Are you aware of other banking frauds that are taking place and that relate to the Internet?

Mr Geurts—Generally speaking, the only other fraud that we are aware of probably does not directly impact the bank, but it really concerns us because it impacts our customers. If you look at the top 10 Internet frauds, you will see that none of them actually involve banking. They

include the Nigerian scams, the auction schemes, the Spanish lottery schemes—all these other schemes and scams that ASIC do a tremendous amount of work in helping to educate people on. That actually concerns us a little more in terms of the impact on our customers than some of the online fraud, because we put a lot of effort into protecting our customers and our systems. It is the other types of fraud that are probably not necessary banking type frauds but that cost people money that do worry us. Some of the auction house scams are very serious.

Mr SERCOMBE—In the context of what we were saying before about the relative ease of forging identity documents and so on, do you have any observations on the operation of 100-point checks within the system? Are the banks regularly coming across examples of forged or false material being used to establish 100-point checks?

Mr Geurts—It is certainly the case that new technologies—scanners, colour printers and so on—have increased our exposure to this type of fraud. I think it has been publicly known that, if you can create several false documents of identity, then you can create some more and create a circular path. With respect to this issue, the bank's position is that we are looking at working closely with the work Senator Ellison is proposing in relation to identity fraud, because it is not just an issue for the banks, it is an issue for the customers. In fact, for example, we have published a guide on our Internet site for the customers about what to do if they are the victim of identity fraud—how to recover their identity, who to tell—because we think it is an emerging issue. So the bank, through to the ABA, will be working very closely to support that, because we think we need to look at validating documents at the point of issue rather than at the point of validation, which the bank currently does under the 100-point system.

Senator HUTCHINS—You say that there is no new uniform evidence regime in Australia, and that only New South Wales and the Commonwealth have adopted this uniform evidence act. Does that prevent you from prosecuting people who are involved in these scams? Secondly, I gather from your submission that you do not think that there should be more penalties for white-collar crime. Would you like to comment on both of those aspects?

Mr Burke—In terms of the ability to prosecute, I cannot think of a case where that has been a hindrance. As regards the difficulties presented to banks by lack of uniformity, in terms of their internal process management, quite a large proportion of our members operate nationally, in terms of the systems and processes they have in place. It would be better if there was uniform legislation in this area.

Senator HUTCHINS—So is it just a bureaucratic approach from the police services to the banks in the various states?

Mr Burke—Yes.

Senator HUTCHINS—Is that the problem?

Mr Burke—Yes. Secondly, yes it is our view—if this is the question—that the sanctions in place are adequate. That is not to say that we do not think that white-collar crime is a problem. Our recommendations have more to do with prevention and detection, I suppose. The crime having been detected, successfully investigated and brought to court, then we think the penalties are adequate.

Senator HUTCHINS—You say that we:

... need to review the sanctions for so-called 'White Collar Crimes' to ensure there is a sufficient element of deterrence.

Mr Burke—Yes.

Senator HUTCHINS—So one would assume that you do not think that they are adequate.

Mr Burke—We think they need to be reviewed from the point of view of consistency with other forms of crime, that is the point.

CHAIR—Do you think there should be further education programs so that customers are aware of their responsibilities, how to protect against credit card fraud, banking fraud and so on? Are you generally supportive?

Mr Burke—Yes, we are. We do support the need for further education. Banks are continuing to explore ways in which better education material can be provided more widely. We also work closely with the card schemes and we think that there are opportunities to explore ways in which we might work with government to develop more. We think education is absolutely crucial—that is our number-one response.

CHAIR—One of our witnesses yesterday praised your efforts in being cooperative with governments in trying to find solutions, so well done on that aspect of it. In your submission you talk about the problems of jurisdictional requirements across the country—the various jurisdictions. Is this an issue and, if it is an issue and a problem, how can we address it?

Mr Geurts—There was a recent report on cross-jurisdictional issues in legislation. Our view is that uniform legislation in these areas, and uniform structures for the administration of legislation, are important. I cannot point to specific cases. In fact, we are doing some work looking at that particular report and determining whether there are any specific recommendations that we can make.

CHAIR—I think we have covered the issues. Thank you for your submission and for coming today. We appreciate the efforts that you are making in this regard. It is an ongoing and rapidly moving field, so I am sure it is not easy. We congratulate you on the extent to which you have put in checks and alert systems. We ask you to come back to us on this particular case. Cases that seem to have a fair degree of unfairness, where all the responsibility is taken by the merchant, seem to us to be something that perhaps should be addressed. We may have further questions—particularly as one of the chunks of this inquiry relates specifically to your area—and, if you do not mind, we might come back to you before we finally bring down our recommendations. Thank you.

Proceedings suspended from 12.36 p.m. to 1.23 p.m.

BEZZINA, Mr Mark, Director, Business Standards, Standards Australia

THIYAGALINGHAM, Mr Brahman, Project Manager, Communications, IT and e-Commerce Standards, Standards Australia

CHAIR—Welcome. The parliamentary Joint Statutory Committee on the Australian Crime Commission is examining recent trends in practices and methods of cybercrime with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee when it reports wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime. The committee prefers that all evidence be given in public but, should you wish to go in camera at some stage, please let us know. Thank you for coming today. I invite you to make some opening comments, and we will follow those up with questions.

Mr Bezzina—I would like to start by thanking the committee for inviting Standards Australia to make a submission and to provide some information on some of the interesting and, we think, fairly exciting work that we have been engaged in with industry in this particular area. I would like to very briefly give you some background on Standards Australia and how we work. I would also like to go through some of the publications we have developed that would assist in the area that this committee is looking at.

Standards Australia is a not-for-profit organisation and we have been in operation for around 80 years. We have grown out of engineering standardisation activities but, over time, we have developed into the management field—high levels of standardisation are getting into management systems and things of that order. We are pretty much owned by society—we are a piece of national infrastructure. We are run by a number of members—around 97 members are associated with Standard Australia. Of those, we have developed a council of around 110 members. The reason that there are more members on the council than in the membership is that some members are major contributors to the development of standards and therefore get more representation.

That is our organisation. It is very much driven by industry associations. We have 1,500 associations involved with standardisation work and around 9,000 committee members sitting on 1,500 committees. Through those committees we produce around 500 documents a year. There is a huge scope of work. On the standards writing side of the business, we employ about 100 people. Those people have around 900 formal meetings a year and probably three times that number of informal meetings. We engage very heavily with industry.

My role requires that I meet with a whole range of people with different perspectives. That goes to the heart of how we develop standards. Under the formal governance structure that I mentioned, we set up those 1,500 or so committees. We constitute committees to ensure that anybody that has an interest in an area of standardisation gets a say in how a standard is developed. We consider the perspectives of product developers or suppliers, consumers, academics, government regulators—anybody who has an interest or a stake in that area of standardisation. We run a very structured process which we call a transparent process. It is

transparent in that we describe how we develop standards and make that generally available through our web site to allow standards to be developed with the greatest level of consultation possible.

The process is open and transparent and we also aim for consensus, so we get those interest groups together in the development of standards. Before any standard is published, it goes through two major stages. Firstly, it goes out to public comment and anybody in the community who has an interest in an area of standardisation is given the opportunity to comment on the document. Secondly, when the comments comes back in, the formally constituted committee, which we have gone to a lot of trouble to make sure that we get balance and representation on, ballots that document. We have to get 80 per cent of the people on that committee to agree to the document before it gets published as an Australian standard. Among the remaining 20 per cent that might possibly be unhappy with the document, there cannot be a major sectoral interest or collective major sectoral interest. In essence, everybody has to agree. When you consider that we produce about 500 documents a year, that is a significant effort. As you would know, since you do a lot of consultation, at the end of the day I guess you can say with a lot of things that you are just going to go ahead with them. But we have to make sure that everybody is happy with the outcome. That is a challenge for us. We have a formal process which assists us with that but, over the 80 years of doing this sort of work, we have developed approaches to facilitating consensus. That is about all I want to say on Standards Australia.

CHAIR—It is probably best if we proceed to questions now.

Senator McGAURAN—What are some examples of the documents or standards you have produced?

Mr Bezzina—I have some examples—

Senator McGAURAN—Are they for all different industries?

Mr Bezzina—That is right. We do everything from motorcycle helmets, building codes and wiring rules through to baby capsules, safety glass in cars and risk management. Corporate governance systems is a recent one. We have 7,500 standards in our range, so you can imagine the breadth that that covers.

Senator McGAURAN—Why are you non-profit, to begin with, and non-government? You would be doing most of your work for the government, wouldn't you?

Mr Bezzina—No, not really. Government is a stakeholder in the process and we ensure that government has a say on our committees, but in the same way industry and consumer groups are also very keen. We operate in a similar fashion to other national standards bodies throughout the world. Standards Australia is the national representative to international standards groups such as ISO, IEC, UN/CEFACT, EDEFACT, OASIS and a whole series of other ones. We try to operate in a not-for-profit way—which does not mean for a loss; we do try to cover the cost of our operations. We do that through the sale of these publications. That is how we fund our operations. We do get some money from the Commonwealth, and that is generally to support Australian representatives at ISO meetings, international standards meetings, so they can put forward the Australian position. I guess that is just the way we have evolved over time. There

was a time when we were much more subsidised by government, but we have been able to operate in pretty much a break-even manner. We get a little bit of cross-subsidisation from our certification activities, because we have got a commercial side to the business that verifies compliance to standards and also does some training that cross-subsidises the national interest component of the business.

Senator McGAURAN—I must admit that I did not know you existed. Did you know about them?

CHAIR—Yes, I did.

Senator McGAURAN—You are across it better than I am.

Senator DENMAN—I have one question. Because you go internationally, does that mean your standards are in line with other world bodies of a similar nature?

Mr Bezzina—That is exactly right.

Senator DENMAN—Are there any differences?

Mr Bezzina—In some areas there are differences, but where possible we try to eliminate non-tariff barriers to trade, and standards, obviously, are one of those sorts of barriers to trade. We are under world trade obligations to adopt international standards where possible.

Mr Thiyagalingham—We also take part in the actual standardisation of the international standards, so we sit on some of the international committees as well. We try to put Australia's input into those international standards so when we do actually adopt them they have taken into account Australia's interests and we can adopt them directly without modification.

CHAIR—I am interested in pursuing some questions. From your experience in establishing standards for information security, what do you consider to be the main areas in which information security is most at risk?

Mr Bezzina—I think—and I have a range of standards here that I brought in that I would like to submit to the committee for your later review—that it is hard to put your finger on any particular aspect. A lot of people try to do that and try to deal with security as a point issue—that is, with one particular aspect of security. Security must be considered as a continuum. A whole set of activities are required to protect information or whatever the asset is; we often refer to information as an asset nowadays in our standards. We look at all aspects. We look at the storage of information, the transmission of that information, authentication, identification of where that information is coming from or going to, and keeping that information in a format that will allow it to be, where required, submitted as evidence or to demonstrate that a transaction has taken place.

There is a whole range of technologies that I have touched on there. You have things like biometrics, you have public key infrastructure, you have encryption methodologies for transferring messages, you have storage requirements and then, around all that, you have risk management. You have to identify what your key assets are, you have to identify where your

threats, vulnerabilities and risks are, and then you have to take appropriate action and build systems around the bits and pieces of your system to make sure they all work together in harmony. There is a whole range of things and then at the end of the day you have to prepare just in case everything goes wrong and look at business continuity management. I have done a lot of research in this area—I actually produced one of these documents. I sat down and spoke to organisations like Telstra, other big companies and some international companies, and that is the message that came across loud and clear to me: it is not just one thing; it is a whole series of things.

Vendors often come to organisations with a solution trying to find a problem—rather than the vendors listening to what an organisation is trying to achieve in securing or protecting information and trying to address that—because they only look at part of the picture. If there is one thing to emphasise, I think it is that, and that is what we have tried to do with the development of standards in this area: to treat it as a process in its own right. I guess that is a long answer to a short question.

CHAIR—It is certainly an area that we are interested in. I suppose the second question is: how realistic is it to expect to create a secure critical infrastructure environment when there are areas of the world that will not comply with our standards? In terms of the Internet, we think of providers who may be based in the former east bloc or even in the United States, where you have problems with the Fifth Amendment and the other pressures that are in that society. How realistic is it when we are dealing with the Internet—which is such a global phenomenon and where we are a minority in terms of providers—to establish standards which clearly a lot of people are going to ignore?

Mr Bezzina—That is a very good question, and I think it comes down to fitness for purpose, deciding where you want to exert requirements for security and, really, having a cost-benefit basis for making that decision, because security is all about considering what you are trying to secure. There are trade-offs. The functionality is limited if you go for a higher rather than a lower level of security, and it is going to cost you more at the end of the day. I guess you are considering things like the availability of child pornography and trying to eliminate that—but in terms of security systems, you would not leave a system exposed to the Internet if that was a system that needed to be protected at a high level. But when you start to get into issues like—personally, I get a whole lot of emails sent to me that I would not want my kids to see. It is crazy, and everybody has the same issue. I do not know how you would prevent that. I think the tools that are available today are really unable to deal with the approaches. It is a system sort of thing: as soon as you come up with a tool to stop that, someone will come—for example, the old antispamming approach was to block an email address, but now every time they send you an email they send it from a different email address. The only way to block that is to have a list of the people that you want to receive email from, and then that reduces your functionality. As I said, it is always a trade-off, which depends on how important it is to you to have that security or protect information or prevent information from being exposed to you.

CHAIR—So what do you see as the principal issues to address in providing a national information infrastructure? How would you see that?

Mr Bezzina—I think standards are a key issue and I guess that is why I am involved in this work. For a start, standards provide a language that allows you to communicate how you manage

security. I will go through some documents now, if you do not mind, because it is a good time to mention them. A number of years ago when I got involved in this area, a whole lot of people were developing information security systems within their organisations. The challenge for them was to come up with an appropriate approach to managing security within their organisations, but every organisation would do it differently. So when you try to communicate what you do to improve security within your organisation, first you would have to understand their system and then you would have to understand the level of security that that provides.

But, if you have a standard system or a standard set of identifiable requirements for an information security system and you have a common set of terms to describe that, it makes it very easy to say, 'I comply within this level to that term.' That is what attracted me to this standard, ISO 17799. It is formally known as 4444 within Australia. I will just go through the content of what this standard covers, if you do not mind, Chair. There are only 10 elements so it will not take too long. It deals with having a security policy; organisational security; asset classification and control, so you identify what your key assets are and how you are going to protect them; personnel security; physical and environmental security; communications and operations management; access control; systems development and maintenance; business continuity; and, finally, compliance. Under those there are 103 other controls.

This standard—and there has been a certification system built around this standard—gives you, for the first time, a common approach to developing an information security management system within an organisation. You can compare levels of security across organisations. That is one of the major benefits; the beauty of that is having that consistency. It does not go into the detail and tell you at a nuts and bolts level what you have to do because, if you were to do that, if hackers or whoever knew what the protocols were they would be able to defeat them. But it says, in reasonably broad terms, that this is how you manage security in an organisation. That means that you can develop an industry to support that standard so people can be trained in how to implement that standard or how to develop a security system within a business. Otherwise, each security exporter would have their own system, and it is a nightmare when that occurs.

I have another document in the same range. This is the same document but it identifies what has to be done. This is a document that a certification system is built around. Somebody will come out and actually order an organisation to say that they have achieved this level of standardisation, which is an important thing to have because it is also an expensive activity. The nature of communications is such that people have to interact with one another and, in interacting, the weakest link in the chain is really how strong your security system is. If you do not have a standard and if you have a whole series of suppliers trying to develop an interoperable supply chain or something along those lines then each supplier has to audit the other supplier to make sure that their security requirements meet their requirements. But if there is a common standard defining what is a secure system and that element in the supply chain has been certified to that standard then that will give them a reasonable level of confidence that they are at a level that they can work with. So there is a reasonable benefit in having this. The infrastructure has developed so there can be a competitive market for that certification service and you can have comparability across the audit results. That is what this standard is for; I will submit this standard. Do you mind if I go through these other documents? It gives you a bit more background.

CHAIR—Sure.

Mr Bezzina—One of the difficult things in developing an information security management system is saying, 'These are the risks that I am exposed to.' We have a generic risk management standard, AS 4360, which is used widely within industry already. It is good, because people understand the approach to security. It is not rocket science, I have to say, but this is probably our most popular document within Standards Australia, and a lot of Australian standards have been being used internationally. I will take you through a methodology for risk management within an organisation. This standard here, HB 231, will take you through that risk assessment specifically for information security. When I say 'information security' I do not just mean the IT side of things; I mean any paper based information, for example. I submit that as well. That is just another document we have that outlines organisational experiences in managing information security. It has some background on how people have gone about doing that.

Senator McGAURAN—Is this the sort of thing that banks would rely on?

Mr Bezzina—Banks use it. ANZ have used that standard and have been certified to it. But we have another range of standards that we have developed. I have only brought a few standards here to give you an indication of our work, but we have a whole lot of standards that backup the operation of ATM machines, for example, and ensure that they maintain security. This has been seen as world leading work. Most recently it has been reapplied to national ticketing and tolling infrastructure to develop a means by which that can operate.

CHAIR—Do you have any information on how readily your standards are accepted by various sectors in industry?

Mr Bezzina—It is hard to get some clear indication on that. Probably the easiest way is to see how often it is referenced in documentation. Even ASCI 33, the government's approach to managing logical security, refers to 4360. The protective security manual, I believe, refers to 4360 and each government agency refers to it as well. I am seeing more and more that the standards are being called up. We are getting copyright requests to include the standards in training material and things along those lines. We know that we sell a lot of these standards but we do not know specifically which areas of industry are picking them up.

CHAIR—Certification is done by whom? Is it from within the organisation of people who are accredited to make the assessment?

Mr Bezzina—That is exactly right. It is a bit of a twisted set of terms. Australia has an accreditation body called JAS-ANZ—the Joint Accreditation System of Australia and New Zealand. They are the organisation that will accredit certifiers to then certify that organisations comply to a given standard. We have the infrastructure in place. The certification bodies will sometimes reveal who their clients are and other times they will not. Not all clients get a formal certification. Sometimes they do a self-assessment, particularly in the area of information security, because if they have an assessment that they deem not acceptable than they are obviously not going to want that revealed. Quite often they do not reveal that they have had an assessment until the very end, or they may never reveal that they have had an assessment.

CHAIR—Are the ISO standards predominantly taken up by small businesses or by larger businesses?

Mr Bezzina—They are developed with any size business in mind. Sometimes we do guides specifically for small business, because in some cases they have special needs, but generally we try to involve small business in the development of standards. We usually do that through the Australian Chamber of Commerce and Industry and having their involvement on committees.

CHAIR—What is the other organisation you were going to tell us about that you also sit on the board of?

Mr Bezzina—I would like to go through these first, because there are another couple of important areas. I have brought in some more detailed guidance on managing security, so I will just hand those to you, and this is a draft standard that Standards Australia has done work on with the Attorney-General's Department and the Australian Federal Police. It is to do with evidence collection, which is an essential component. Quite often people or organisations discover a breach of security or that someone has in some way broken the law, but the way they collect the evidence means it is deemed inadmissible in court. There is no assurance on how to manage that evidence. This document provides guidance on how to handle evidence so it is admissible in court. Finally—I know I am running out of time—

CHAIR—We have seven minutes left.

Mr Bezzina—there is a new range of standards that we have developed to do with corporate governance, which is another essential element of a security system—but this is more broadly about good governance within organisations. That is not so much a critical point. What is in here that is of most interest to you is the fraud and corruption control standard that we have recently developed. A lot of the issues around cybercrime happen internally, so you need to have very good controls.

CHAIR—Yes, that could be quite a useful document.

Mr Bezzina—There are a couple of others; I will not go through them. There is a whistleblower protection system so that, when somebody catches someone, they can provide evidence to the board or somebody else and not feel that they are going to get themselves into trouble by doing so. I have probably provided more information than I should have. I can talk in very broad terms about our work, but it is not until you see the outcomes of our work that you get an idea of what we are involved in. Do you want me to go into the Biometrics Institute now?

CHAIR—Yes.

Mr Bezzina—The Biometrics Institute has been around for a couple of years. It was set up with end users of biometrics in mind. We have around 20 members at the moment. A lot of them are vendors, but then there are a lot of users of biometric devices. The aim of the institute is to educate people about the use of biometrics and assist in building privacy codes and codes of ethics around the responsible use of biometrics. I do not think there is any need to go any further on that. I just wanted to make sure you were aware of its existence. If you require more information on the institute, I am happy to provide that.

CHAIR—That is fine.

Senator McGAURAN—I am quite overwhelmed by the sophistication and detail of your work. I guess there is no problem in the industries knowing and getting this information?

Mr Bezzina—No.

Senator McGAURAN—It is easily found. They know where to call you.

Mr Bezzina—That is right, yes. It is worth mentioning, too, that Henry Bosch—I do not know if you know him—was our chairman on that committee. As far as corporate governance goes, I do not think you could find a more prolific writer in Australia.

CHAIR—I had exposure to Standards Australia when I was at the tourism ministry. They were trying to develop standards there, meeting your criteria, and that began establishing appropriate standards for those who provide inbound travel and product. That proved to be very successful. Do you see that there is a greater need for public education and making people aware of standards, especially when you look at the areas that we are looking at—credit cards, Internet usage et cetera?

Mr Bezzina—Absolutely. I think that is a key component. For all the good work Standards Australia do, I do not think they have gone out and really promoted that work, and a lot of people, if they do know of Standards Australia, think of us very much as an engineering type organisation or as reasonably slow in the development of standards. We have put a significant effort into speeding things up, particularly in the areas that I manage, because technology does not wait. So we have come up with approaches to speed things up, but there is an increased need to make people more aware of what we do and who we are, and I guess that is part of the reason why I do these sorts of things and talk a lot at conferences—just to try to make people aware. Also, the quality of what we produce is to a large extent dependent on who is involved in the development process, so we are keen not only to get people to use our product but also to have people provide input into the very early stages or at least comment when things are out for public comment.

CHAIR—We appreciate your input. We may come back to you to test out some of our ideas when we are putting together the report. Thank you for your time today. We look forward to being in contact with you in the future.

Mr Bezzina—Can I just than the chair and the secretary again for asking us along to give you some background on Standards Australia and our work.

Proceedings suspended from 1.55 p.m. to 2.11 p.m.

[2.11 p.m.]

ATKINS, Ms Liz, Deputy Director, Money Laundering Deterrence, Australian Transaction Reports and Analysis Centre

JENSEN, Mr Neil, Director, Australian Transaction Reports and Analysis Centre

CHAIR—This is a meeting of the Parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime with particular reference to (1) child pornography and associated paedophile activity, (2) banking, including credit card fraud and money laundering and (3) threats to national critical infrastructure. When the committee reports, it wants to be able to provide a picture of emerging trends in cybercrime and offer guidance as to the role the newly established Australian Crime Commission might play in combating this crime.

I welcome Mr Neil Jensen and Ms Liz Atkins of AUSTRAC to the hearing. As you are aware, the committee prefers to receive all evidence in public but at any stage should you wish to go in camera please advise the committee. I invite you to make an opening statement and then we will follow with questions.

Mr Jensen—Thank you for the opportunity to put in a brief written submission, which we have very recently made to you and also for making time available for us to come before the committee today. I think the major issues that we would like to draw to your attention relate to the legislation with which we work—the Financial Transaction Reports Act—and the work of the organisation AUSTRAC. In our very brief written submission we touched on a range of issues that we thought may be relevant to the inquiry's consideration. Those issues came under four headings: proprietary financial systems and Internet payment systems; overseas based credit card tax evasion and fraud; proof of identity, including identity theft and false identity; and new banking products in the globalisation of financial services and capital markets.

I will not go into the detail of those issues which are in the brief submission, but I will provide some background that may assist in regard to a number of roles that we do have at AUSTRAC. Firstly, our primary role is to manage the processes relating to the Financial Transaction Reports Act. We receive financial information from a whole range of organisations referred to as cash dealers and that includes banks, building societies and a range of other organisations. That information comes into us and then we analyse the data and make the data available to the law enforcement agencies in the form of intelligence. The reason that is relevant to this inquiry into cybercrime is fairly obvious: we are providing information and cybercrime has the ability to evade the provisions of the FTR Act—that is, the Financial Transaction Reports Act.

One of the important areas that we have reports on in our work is the area of international funds transfer instructions or international telegraphic transfers. They are all electronic transmissions, and they are the first point of contact we have had with the cybersystem. We have had reports of those transactions since 1992 and they are a very valuable source of information. The reason why they are valuable is their quantity. We get some nine million per year. As for the use of the financial system—and it is part of the financial system—it is SWIFT transmissions

which have been on an electronic basis, probably for 20 years or 30 years I would suggest, and it is the main system that is used by the banks in getting information around the world about transactional activities. So as for sending money offshore, the banks do that through the SWIFT system. A large number of banks around the world are linked to the SWIFT system. We have seen over a period of time a lot of activity where criminals have used that system. Australia has a strong banking system. The criminals use the banking system to shift their money offshore and to shift the money onshore as well; it does work both ways.

About six years ago the organisation started to have a look at the potential for other methods of electronic transmission of funds. Stored value cards in particular were hinted at at that particular point in time. A couple of organisations did have systems in place. One of those was referred to as Mondex. It looked like it was going to start up and it would enable people to pass funds electronically between themselves, between individuals. So our first concern in this whole area is what happens outside of the regulated financial markets. Secondly, what is the potential for activity, the transfer of funds, to occur outside the regulated markets?

Around that time a group was set up under the auspices of the Heads of Commonwealth Operational Law Enforcement Agencies, referred to as HOCOLEA. That group, which meets regularly and comprises the CEOs of various Australian government law enforcement agencies, agreed that AUSTRAC should chair a group which would look at e-commerce type issues. One of the issues that we were looking at at the time was stored value cards. That group is still meeting, now under the title of the Action Group into the Law Enforcement Implications of Electronic Commerce, and it is engaged in a range of activities. It comprises representatives from the various law enforcement agencies looking at issues that are relevant to e-commerce and the law enforcement implications of that.

Harking back to the stored value cards, what appeared to be at that time something that was going to progress fairly quickly in the next couple of years has certainly not evolved as quickly as we had first anticipated. That is not to say it is not happening, that these stored value cards whereby you can transfer funds are not available; it just seems that it has not picked up here in Australia and in many other places around the world as quickly as we had anticipated that it would. The potential is there. The technology is there. In Australia the major banks bought out Mondex, and I think that is probably why it has not progressed as quickly. They are looking at those systems themselves and will see how they operate. The biggest concern, from our perspective and from the law enforcement perspective, was the potential to operate outside the regulated financial system. That potential is there. Technology allows that system to occur. Stepping back from that, one of the issues that we raise in our paper is credit cards and the use of credit cards offshore, and credit cards where people have obtained them offshore and use them onshore and also offshore for all their payments. That is an issue that is currently being looked at through the Action Group into the Law Enforcement Implications of Electronic Commerce. I will refer to that as AGEC. A number of other issues concerning payment systems are also being looked at at the moment in that group.

Proof of identity is also a significant issue in cybercrime. We have a proof of identity steering committee, which has undertaken quite a bit of work looking into issues of identity and identity fraud. That organisation comprises law enforcement agencies and state and federal government agencies and it is considering issues of ID fraud. It feeds into the whole-of-government approach on this issue and into the policy development areas, as AGEC does in its work.

These issues of cybercrime are not new to us. We have had a hook into them for some time in the regulated financial sector, through international telegraphic transfers. We are chairing groups comprising state and federal agencies and the private sector which are looking at a number of the aspects that have the potential to be involved in cybercrime—that is, the financial systems cards and, of course, identity, identity fraud and theft. That concludes my opening statement. I am happy to address you on any other issues that you may have.

CHAIR—I recall that the last time we met was when we were looking at legislation in the setting up of the ACC. Despite our best efforts to have you on the board, it was not to be. I think you are probably in a good position to judge whether you think that the whole area of cybercrime is being coordinated effectively on an Australia-wide basis. There seem to be various organisations that touch it to a certain extent, but do they need to be brought together effectively into one organisation whose prime responsibility is looking at cybercrime as such? Do you have any views on that?

Mr Jensen—It is an interesting question. We have the same issue with regard to financial transaction reporting and that side of it. It is important to make sure that all areas are covered. Sometimes, in one organisation, it is difficult to have all of the skill sets and knowledge in one place. What we have done with our AGEC group, for example, is draw in various skills. It is a non-funded group—it is funded by the agencies themselves to look at the various issues. We are not looking at it from a fixed point; rather, we are looking at all of the relevant issues of those involved in it. That is an important example, because in that group we have law enforcement agencies, revenue agencies and other regulatory agencies as well. It is not just looking at cybercrime from a law enforcement perspective but from an overarching law enforcement, regulatory and revenue type perspective.

If it is a single organisation, I think it would be very important that it has all of those skill sets within it. On top of that, you need information technology people and communications people who understand the underlying vehicles and how they all operate, because that is a very important part of it. You also need people who understand crime, legal people who understand the legal complexities of it all, policy people who can arrange the relevant legislation that may be necessary and, of course, the private sector and the government agencies that are dealing with these things all of the time. If it is one organisation, you need all of those skills. If it is not one organisation, you need to coordinate it so that all of those skills come together. I do not have any fixed views on the best way to do that, but, certainly from our perspective, bringing all of the relevant parties together has worked pretty well in what we have been doing. It is the same thing with the work of AUSTRAC generally. We are a single organisation, but communication and the coordination of all of the parties that we deal with is an important part of it.

Senator DENMAN—So you work cooperatively with agencies, banks, police and all of those things?

Mr Jensen—Yes, very much so. We provide our information to 27 organisations and there are perhaps a couple of thousand organisations that provide raw data and intelligence to us. We work with the casinos and the gambling sector and a whole range of wider financial services bodies.

Senator FERRIS—Mr Jensen, one of the things that has characterised work on these areas in the past is what I call ‘turfdom’ between federal and state agencies. Have you come across any

examples of where you think there could have been better information sharing in relation to the issues you come across, and do you believe that the largely state based jurisdictions are the best agencies to handle this sort of work or should there be one overarching federal reference, perhaps to the Australian Crime Commission?

Mr Jensen—It is more than a national issue; it is an international issue.

Senator FERRIS—Yes. So should it be handled by state jurisdictions?

Mr Jensen—I think that it would be difficult for it to be solely handled by state jurisdictions as such, because we would need each jurisdiction. But if, for example, it is a Commonwealth—or Australian—organisation or reference, it needs to involve those states as well. So I think it is a whole of Australia issue not just a whole of Commonwealth government—or Australian government—issue. The other side is very important, because it does need the links internationally and, generally speaking, the Australian government has those links, whereas some or each of the states may have links internationally but they are probably lesser links. My personal view would be that it should probably be the Commonwealth but involving each of the states in the process.

Senator FERRIS—What about the issue of turfdom? As a national body, do you see any areas where you think there could be more effective sharing of state-held information?

Mr Jensen—There is always the issue of sharing information. It is difficult in law enforcement for many reasons. Many of those are operational reasons, which make it very difficult to share at a particular time. I think that coordination is essential. The ACC, for example, is an organisation that has a coordinating role, so I would suggest that the ACC could be an appropriate organisation to do it.

Senator FERRIS—I think you are telling me that the answer is yes.

Mr Jensen—Yes.

CHAIR—What do you think is the impact on Australia of the use of non-financial Internet institutions, such as e-gold, on funds movement?

Ms Atkins—AGEC has a number of focus groups. Two of them have relevance in this area: one is about new technologies and the other is about the financial system. In that, we are looking at ways of avoiding the financial system as well. E-gold and other similar types of mechanisms have been of great interest, particularly to the Australian Taxation Office. People use them to avoid our reporting mechanisms, which Mr Jensen mentioned earlier, on international funds transactions. It is quite easy to use these mechanisms by buying e-gold and then having credit cards or debit cards on international accounts so that our reporting systems are completely avoided. There is quite a large amount of concern within the broader law enforcement agencies, including revenue and regulatory agencies, about those sorts of mechanisms.

CHAIR—You have been through these inquiries and so on many times before. What would you like to see us zero in on in making recommendations in this area? Is there a need for greater controls, legislative requirements and changes, and police monitoring of emails and the Internet?

Mr Jensen—I think the first thing is to fully understand the types of products and the potentialities that are and will be in the marketplace. So—before we put in place legislation or regulations—what really are these products and potentials, and what criminal conduct relating to these sorts of products are they finding overseas? When we find that out, we then know that we need potentially to do one of two things. One is to regulate in respect of those products or types of conduct, the other is perhaps to put in place some form of self-regulatory mechanism that can regulate and ensure that criminal activity is not in place. Certainly the word you used—monitoring—is very important to understand and to see. It would not, to my mind, be beneficial to regulate to a large degree something that we are not really fully certain about at the moment. If we were fully aware of the situation and the extent to which it is being used or abused overseas and in Australia, then I think we would look at the regulatory role and, equally, listen to the financial sector in terms of some form of self-regulatory role as well, provided that it was adequate for the purposes of controlling whatever criminal activity did occur. So I would certainly want to see a recommendation along the lines of ensuring that we have enough information. You may have that through this committee—through the process of the committee—I do not know that at this point in time.

CHAIR—The answer is that I do not know that we do. So what you are saying—in terms of knowing what the product is—is that you do not know what it is at the moment?

Mr Jensen—We have some information and through our AGEC group we are reviewing or analysing what is happening. So yes, in that sense, at this stage we do not have all the information, but we are bringing that information together through a group of appropriately skilled people who do have knowledge.

Ms Atkins—Relevant to that, of course, is cooperation between government and the private sector. That is a very important thing in this area. The only way we can know about current products and how they are being used and the changes in the way they are being used, as well as new products and what the potentials are, is to work closely with the private sector. Also in terms of the sorts of things you are talking about—monitoring and keeping records—one of the big problems for law enforcement, if somebody is, say, using the Internet to conduct transactions, is: how long are the records kept and how can they get at them? We have been doing quite a lot of work with people like the Internet Industry Association, who have developed a code into which, through AGEC, we have given detailed input about how long they are prepared voluntarily to keep information. In addition to that they are setting up a law enforcement industry forum to discuss exactly these sorts of issues. I think the big issue there is getting cooperation from people like the Internet service providers, who perhaps traditionally have not had the contacts with law enforcement, but we are starting to build those up and I think that is a very important area for us to continue to work.

Mr Jensen—On top of that, once we have got to that point—and that is very much advanced, as it has been very well worked on by both the government and the private sector—then we need to make sure that the appropriate tools are available for law enforcement. It is no good having, for example, a self-regulatory role if the tools are not there for the law enforcement to take advantage of when these crimes are occurring. So certainly we would be looking at something along those lines: that whatever is required by law enforcement, the appropriate tools are given to them to do the job.

Senator FERRIS—I want to take you to the issue of the banks. We had evidence from the Australian Bankers Association this morning that, by and large, they are happy with the way the regulations applying to them are now operating. However, they also told us that they have formed a fraud task force. We have also had evidence of a very sophisticated, and very damaging to the individual involved, scam in which a bank was somewhat compliant in the sense that it subsequently discovered the scam but six months later the man's account had been debited to over $100,000 as a result of the successful scam. Have you any comments to make on the way in which banks are dealing with credit card fraud, whether it be skimming or targeted? In this case it was international and it was well over the $10,000 trigger, but it was done through credit card so it did not attract your attention. Do you feel confident that, in principle, banks are doing as much as they can to protect their customers?

Mr Jensen—I would not like to comment on the broader question. Bringing it back to the work of AUSTRAC, we have an excellent working relationship with most, if not all, banks—in particular, with the big four banks. We work very closely with them in terms of their requirements under our legislation, which includes the reporting of suspicious transactions, and other transactions such as international telegraphic transfers and cash transactions. I think it would be fair to say that our working relationship is at a very high level. We inspect their procedures, and they have all the procedures in place.

In this particular case I do not know what the situation was or whether they did put a suspicious transaction notification in to us, which they can do, even if it is a credit card matter. I think probably one of the major issues with credit cards is the volume of transactions and the difficulty in being able to pick out of specific transactions conduct that is suspicious. In our document we refer to credit cards, and that is a real issue that we need to address in our legislation in the not too distant future.

To answer your question: from our perspective the banks are doing what they are required to do under the legislation. They have worked very closely with us since our inception in 1989.

Senator FERRIS—What about new technology that is being used overseas to double-check credit card transactions that might be suspicious? Are you aware of any technology that has been used overseas that could appropriately be applied here?

Mr Jensen—I think we have the ability to build technology that could be used. The problem is where you place that technology and how you use that technology. I think you will find that the banks are developing risk-management systems—because that is exactly what they are—for credit cards, general fraud or anything else. I know from personal experience that the banks are developing these systems and that they are developing systems that are very similar to those we use to find criminal transactional activity in the data we hold.

The real point is to find a choke point —if I can use the term—within the transactional activity, such that you are not causing disruption to the operation of the banks. We certainly do not want that. I mentioned earlier that we have a strong banking sector that is within world standards, and we certainly do not want to cause disruption to that. To give you an example of what can be done with international telegraphic transfers—and bearing in mind that credit cards are a lot more difficult—we have that information forwarded to us effectively overnight. So, in very crude terms, the transaction goes through the bank and it is duplicated and sent off to us.

Technology can do those sorts of things. It is then readily available on our database. The number of credit card transactions is much greater than the number of international telegraphic transfers—I mentioned nine million earlier—which are just in excess of seven million per year.

The Americans talk of trillions of transactions. I am not sure what they are here but they would be in the many hundreds of millions of transactions per annum, even on a daily basis for many of them. So the issue is not whether the technology is available—yes it is. How you use the technology and where you place it is the very important aspect of it, and then what you are looking for. A lot of it will be small values, but are you looking for small value crime that actually does build up to large scale crime.

Senator FERRIS—When you think about it, it is not new that people can get access to secure areas using a fingerprint or a thumbprint. Surely it must be reaching a situation now where somebody could opt to have a thumbprint ID on their credit card as a laser imprint, which could then be read against an automatic scanning device such as we have with the strip. Bearing in mind how long it has been since bank cards first came out, I have been surprised that very little has changed in a technological sense over those years.

Mr Jensen—You are very right. The ability is there, but how can the banks do this? The very important point that you did make is that people could opt to do something. I think that is important—people are not told to do something; they can opt to do it. The criminal element probably will not opt to do it, although they may opt to do it by somehow creating or fixing it in some way. I think the banks would say the equipment to read some of these things is still quite costly. Do you have it in every branch and can it be put into a small machine of some sort? Can the criminals defeat it? We have seen that they have been able to defeat a range of things. The smarter, organised criminals have the expertise—they have IT people, the lawyers, the accountants and everything else. The ability is there to do it, but the cost of it is the real issue.

Senator FERRIS—Think about how seldom a person looks at the signature on your card when you carry out a transaction. I often ask people if they want to look at my signature and they say no. It is extraordinary how quickly the transaction can now take place and they do not even turn the card over. In fact, often they give it back to you and you put it away in your wallet before you even sign. So a laissez-faire attitude towards the use of cards has developed in that sense. One of the things that come to my mind from the evidence over the last two days is how dangerous those cards can be in the wrong hands. But we do not think about it. We take it for granted as a simple transaction when it may not be.

Ms Atkins—To some extent I think technology has caused that. Now when your card is swiped and there is no signature on your slip of paper, if it has not been reported stolen and the technology does not to pick it up as lost, stolen or fake, they do not need a signature on it. The technology has caused a lot of this.

Mr Jensen—Equally, as we know from card skimming, the technology helps criminals to get the information that they need. A signature is just one issue. They can skim the material off the electronic strip on the back of the card.

Senator FERRIS—We saw that.

Mr Jensen—They can do that relatively easily and the technology can be purchased very cheaply. They are the sorts of issues that we are dealing with. Technology can help us to perform a lot quicker and a lot better. Equally, it can help criminals, and that is our area of difficulty.

CHAIR—To what extent are credit cards used in money laundering?

Mr Jensen—What we do not know is our biggest issue. I have absolutely no doubt whatsoever that in criminal activity and tax evasion, they would be used quite significantly. The best people to ask about those matters are the people who do the investigations. We do not have an area dealing with credit cards, as I said before, so we do not have a lot of information about it other than what we are trying to gather through our various groups. So I really cannot answer the question. We do not know the extent of credit card fraud. I remember saying those very words quite a long time ago. We still do not really know the extent of it all. It is like any crime: until you catch up with it, you do not really know how much money laundering is going on and all those sorts of issues.

Senator FERRIS—Are you satisfied with the $10,000 figure? Would you like to raise it or lower it?

Mr Jensen—In terms of our cash reporting?

Senator FERRIS—Yes.

Mr Jensen—No, I think it is an appropriate level. It is only one component of the information we get. That cash threshold is for both bringing currency into and out of the country and for cash transactions within the country. We do get all the customer based telegraphic transfers into and out of the country so there is no threshold limit there at all. Suspicious transactions may not have any monetary value at all.

Senator McGAURAN—That $10,000 limit was set in 1988, was it not?

Senator FERRIS—Yes. That is why I asked the question. That was a long time ago.

CHAIR—There probably are benefits in not having a CPI increase.

Mr Jensen—It has been raised and discussed, and in fact it would be an issue for the banks if it were to be CPI related because they would have to change all their systems and their procedures—everything—each time the CPI were changed. So there are good reasons for not increasing it. Is it still a relevant figure? Yes, it is very much still a relevant figure.

Senator McGAURAN—Is it $10,000 if suspicious or just $10,000?

Mr Jensen—It is just $10,000. If it is suspicious the transaction does not even have to occur.

Senator FERRIS—So effectively it is going down.

Mr Jensen—Yes, in real terms.

Senator FERRIS—So over the last 15 years in real terms it has gone down, probably by 50 per cent.

Mr Jensen—Equally, you would expect that the number of cash transactions that we receive would also diminish because people are using cards. There is still a gradual incline—gradual but still an incline—in the number of reports we are getting. So cash is still used and I would suggest that it is used by criminal elements to get it into the system to start off with and then it is shifted around the system electronically.

CHAIR—We understand from Attorney-General's submission that AUSTRAC are actually chairing a proof of identity committee.

Ms Atkins—I am the chair.

CHAIR—So how is progress going there? Is there anything that you see there that may be useful to this inquiry?

Ms Atkins—A big thing for us has been the recent announcement by the minister for justice about the feasibility studies looking at some online verification issues and things like that. That is very important to the financial sector. We have been saying for a long time that it is not the 100-points system that is the problem; it is the underlying integrity of the documents, so some sort of fast mechanism to check those documents would be of benefit. What has been announced by the government at the moment is looking within government, but it is a first step on the way.

Obviously there are some major issues to be looked at in terms of privacy and that sort of thing, which will need to be discussed and sorted out before we can go too much further, but at least everybody is very welcoming of that whole of government approach that is now going to be taken. For quite a long time there have been a number of committees looking at various aspects of identity, so everyone is very pleased to see some sort of centralised whole of government pulling together of that. Our committee will continue to exist, because one of the important things about our committee is that there are not just law enforcement and Commonwealth and state agencies on it; the four main banks and the ABA are all on the committee as well.

CHAIR—How many are on the committee?

Ms Atkins—It is quite large. We must be close to 20 people at the moment and resisting having any new people. We find a lot of people are interested in joining but we have had to start resisting that because it is just going to get too big to do any work.

Mr Jensen—Twenty organisations are represented.

Senator DENMAN—Who sets the number of organisations? Do you? Can you expand it or contract it if you choose to?

Ms Atkins—The committee does. The committee was created as a result of representations from one of the major banks and the Australian Taxation Office, who saw AUSTRAC as an appropriate area to look at these issues, so it was set up with the agreement of both government

agencies and the banks. So when somebody does ask to join, we go to the committee and the committee makes a decision.

CHAIR—Do you think it is possible that the whole changes that are happening in cybercrime may push us closer to national identity cards?

Ms Atkins—That is a matter of policy that I would not like to comment on.

CHAIR—I am not stating that on behalf the government. I just think that if you had one national identity card where all of these factors came together that would actually reduce significantly the extent of fraud, or does it go in different—

Senator FERRIS—Didn't we have a double dissolution election on that, Bruce?

CHAIR—Yes, you are right. It especially always makes me nervous when I see the press over there.

Ms Atkins—You only have to look at the US, where the social security number is a de facto identification, to see that in fact it does not necessarily help.

CHAIR—That is interesting.

Ms Atkins—The amount of identity fraud in the US is growing, just as we believe that it is growing here, and I think the social security number does not help. If we started an identity card system now, we would all have to produce our documentation, so you would still have that underlying document problem—

CHAIR—That is right.

Ms Atkins—leading to the one card.

Mr Jensen—We do have a good, robust identification system within the FTR act—that is, the 100-point system. The issue is the documentation behind it, which was not created necessarily for identification. Birth certificates, passports, drivers licences and even credit cards—all these sorts of things—can be used as part of the process. The system is okay; it is the integrity of the documents and the ability to verify them that creates the difficulty in the process.

CHAIR—So on this whole identity question—especially as our inquiry relates to the Internet—do you think that, as Senator Ferris was saying, rather than a password we may see more radical changes, such as eye and fingerprint identification?

Mr Jensen—I think the potential is there and eventually, yes, it will happen. It probably could have happened by now, but other advances have taken place. Who would have thought two years ago that we would have mobile phones that you can take a photograph with? These sorts of things can happen very quickly, but it comes back to pick-up by the Australian community, if you like. Stored value cards were not readily picked up by the Australian community but they were in some communities overseas. The mobile phone was picked up very quickly in Australia, but in other countries it was much slower. I think all the technology is for—in your terms—

'radical' ways of identification or use of these things, but it all comes down to pick-up by the Australian community, the cost of doing it and who is prepared to take that radical step of putting something in place. I used the word 'radical' because you used it, Chair. Many organisations have these things in place within their own organisation for the purposes of security for their own people. Overseas, numerous countries have iris and thumbprint scans and all these sorts of procedures at their front doors for staff to get in.

Senator FERRIS—Keyless entry.

Mr Jensen—Yes, keyless entry—stored value cards or cards with chips on them to get into the organisation. We use similar things for our own organisation's chips for entry. There is no reason why these things cannot be adapted. It comes back down to someone taking the step and it being accepted by the community at large because, if it is not accepted by the community at large, then the spread of the cost is much smaller.

CHAIR—That is right—absolutely. It is like the Australia Card. There was a huge debate about that.

Senator FERRIS—Until people realise how much credit card fraud, skimming and so on costs—I do not think it is widely understood—I do not imagine people will seek better recognition factors, because they do not realise how much at risk they are. It is almost a wheel that is turning. Until people better understand the cost to a small business, which might build credit card fraud into its price structure, they will not realise that those costs could be lower if they went to a different system.

CHAIR—Do you think that self-regulation achieves a realistic outcome?

Mr Jensen—In many circumstances, yes, I think it does. We need to look at self-regulation in the sense of how it is imposed—how it is self-regulated, I guess. If the impetus is there to make it work then, yes, it does work. But in certain circumstances self-regulation is not the answer and legislation needs to be put in place. It does come back to that issue of tools. We have spoken about cooperation. When cooperation breaks down in a self-regulatory component then you do not have the tools to do what needs to be done. It is a real balance between those two things.

CHAIR—This inquiry is an opportunity, if there are changes needed, to give input. So, if you feel that we are at the stage where we really need some regulatory or legislative changes, it would be useful to have that input. Certainly, your work has been praised by other organisations and in our informal discussions in Canberra before starting this inquiry. It is not your competence that is in any way in question; it is just a fast moving target. In terms of the source of funds being moved around and out of Australia, to what extent is it shifted through electronic transfer—is it now mainly electronic transfer?

Mr Jensen—For a long time now our financial system has enabled electronic transfer because we have a branch set-up. You can go to your Sydney branch and deposit money and you can collect it from the Perth branch. There has always been the ability to do that. In the United States, they have had a system of domestic wire transfers and they have had to transfer money, like we do internationally, around the United States because of the way they are set up. We have not had that; we have branch set-ups in Australia and the system is electronic, in any event. Sure,

there has been an increase in electronic use, there is an increase in electronic banking and there is an increase in the general electronic payment of bills and all that sort of thing—there is no doubt about that. Whether that is being used in a criminal sense is difficult to gauge at this stage and we certainly do not have a handle on that at this point in time.

Coming back to your earlier point, the work we are doing with AGEC can lead into a lot of these areas but it is not sufficiently advanced at the moment to be able to give you recommendations, although that could feed into that at some later stage, once all the work is done. That is the intention of it: to help policy by raising these issues, looking at them and then passing them on to the appropriate place for policy to be determined. So, yes, there is much wider use of Internet and electronic banking.

CHAIR—What percentage would you say?

Mr Jensen—I do not think we could say.

CHAIR—Can you give a ballpark figure?

Mr Jensen—The banks may have the answer to that.

CHAIR—We did not ask them, unfortunately.

Mr Jensen—From our perspective, we are still seeing an increase in cash, so it is difficult to gauge whether it is just an increase in financial transactions, an increase in population or that we are getting more organisations reporting to us—perhaps it is that that is causing the increase. But I would suggest that the use of electronic transactions in various forms is increasing by a much greater percentage than cash transactions.

CHAIR—I think we have covered questions of proprietary systems on the Internet. I am looking at a list of suggested issues that we might raise with you. Are you seeing any technological developments that might further circumvent what you are trying to monitor or achieve, or not?

Mr Jensen—What we have seen has been there for a period of time. Internet banking—the ability to sit at your home computer and transact overseas—certainly has happened in the last few years. Prior to that, what we saw were systems which the banks set up, but people generally still had to go through the bank here in Australia. It is now at the point where people are able to deal with their banks overseas directly. Certainly that is an issue.

CHAIR—But anything that is transacted with an Australian bank, you automatically pick up?

Ms Atkins—If they are moving money overseas.

Mr Jensen—If it is overseas, yes.

CHAIR—I guess because there are other ways of circumventing scrutiny?

Ms Atkins—The alternative payment systems that we have already talked about, like e-gold and that sort of thing, used in combination with an overseas credit card are the main ways. Really, that is not new; it is just that there are lots of different alternative payment systems—but they are all very similar.

Mr Jensen—It is using communications technology—instead of moving voice, as the phone has been used for a long period of time, the phone is now effectively a bank terminal. By using the digits on the phone, you are sending a digitised message across the line instead of a voice message and the bank at the other end can pick that up. It is all automated there. There are authentication processes—PIN numbers and things like that—which enable all this to happen. That can be outside our system. Dealing with the banks here it is fine—we are linked to them and obviously a whole lot of other organisations. But once it steps out of Australia our issue is are we after the criminal here in Australia who is creating the crime or conducting the crime overseas? The answer to that is obviously yes, because overseas they would like to get the criminal doing that here in Australia. How we control that is the most difficult part of it, and how quickly and how frequently it happens is a real issue as well. The speed of transactions, these days, is a significant issue.

CHAIR—That is true.

Senator DENMAN—The laws vary between Australia and overseas, so that makes it difficult as well.

Mr Jensen—Yes, but there are now various international groups which have standards. For example, the Financial Action Task Force on Money Laundering has 48 recommendations, and a whole range of countries are putting into place legislation, albeit slightly differently, but around the very issue that the recommendations refer to. There is a lot more of that happening. Globally, legislation is being put in place to assist each other. For example, in one of our roles we are referred to as a financial intelligence unit. Next week here in Sydney there will be a meeting of some 80 financial intelligence units, our sister organisations from all around the world, and we will be chairing that meeting.

Senator DENMAN—So you are consulting globally.

Mr Jensen—Yes. That brings those organisations together to talk about the issues they have, like those we are talking about here now, and how they can be resolved in their own countries and how we can exchange information. We have the ability to exchange information and that is another important part of this. It is global; it is not just Australian.

CHAIR—And you are going to similar conferences offshore.

Mr Jensen—That is correct.

CHAIR—I think that is important as well. Thank you very much for coming today. As normal professional input, you will be pleased to know that you are being praised by other organisations for your leadership in the field. I still believe that you should be on the board of the ACC.

Mr Jensen—I will leave that one with you!

CHAIR—We will work on that over time. Thank you for your input today. We may get back to you as we work through our recommendations.

Proceedings suspended from 3.02 p.m. to 3.23 p.m.

[3.23 p.m.]

BANES, Mr David M., Regional Manager, Security Response, Symantec Australia

DONOVAN, Mr John, Managing Director, Symantec Australia

CHAIR—I call the committee to order and resume this public meeting of the parliamentary Joint Statutory Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

I welcome Mr John Donovan and Mr David Banes of Symantec Australia. As you are aware, the committee prefers all evidence to be given in public. If you wish at some stage to go in camera, please advise us and we will consider it then. I invite you to make some opening remarks and then we will proceed to questions.

Mr Donovan—Thank you for the opportunity to appear before you. We are very pleased to be able to do so. We have reviewed a lot of the submissions that have been made to the parliamentary joint committee, and I am glad to say that the contributions that we have seen so far from the different entities are certainly in line with our expectations and what we would hope to achieve from this as well.

CHAIR—And you would know, by the way, that at the conclusion you will be able to get full copies of the *Hansard*.

Mr Donovan—Fantastic; thank you. Particularly of note were some of the submissions made by the Australian Banking Authority along the lines of education and also along the lines of early warning systems and threat management systems. That particularly is our area of expertise: educational services relating to the proliferation and development of malicious code and also the threat management systems and early warning systems. A lot of the work that we have been doing with federal and state government agencies is centred around those sorts of technologies.

I want to touch on a couple of things that were contained in Symantec's submission to the joint committee. Firstly, Symantec's capabilities are global capabilities in this area. We have built a very large organisation based on expertise in the areas of security response, security operations and threat management alerting services. We provide those services to a large number of corporate, education, defence and government organisations on a global basis.

Security response has the responsibility for technology along the lines of development of antivirus definitions, applications to reduce the effect of malicious code and swift response to threats of that nature. We have security operations centres based around the world that not only act as organisations that reduce or mitigate risk with malicious code but also act as collection

points. We collect information on the evolution of cyber threats on a global basis and these collection points feed into central resources, which allow us to develop a better understanding of how these threats are maturing, what we can see on the horizon and also the expertise in the area of threat management systems and alerting services. The alerting services once again pull in the information rolled into those security operation centres and from the security response groups and allow us to develop a very good idea of not only what is happening today but what we expect to be happening tomorrow. I want to focus today on the trends that we see in this area. Obviously, we are seeing more threats on a regular basis. We are also seeing more complex threats. We recently delivered a paper to the Australian Banking Authority.

CHAIR—You might like to describe threats for us.

Mr Donovan—Okay. When we talk about threats we are specifically focusing on IT threats: threats to critical infrastructure in the IT space and to systems ranging from individual consumer PCs all the way up to what we would term 'critical IT infrastructure', which are things like the Internet backbone and financial services. They can be anything from nuisance worms or mass-mailing email systems through to more critical style attacks that would be along the lines of things we saw with Nimda, Code Red and the SQL Slammer worm, which had the potential to bring down significant portions of the Internet backbone.

Senator HUTCHINS—What is a blended threat?

Mr Donovan—A blended threat is a threat that contains malicious code, something along the lines of a worm that is designed to cause malicious damage to a system but bypasses regular antivirus systems. It will go after specific vulnerabilities in applications or operating systems. In the case of Nimda, it actually attacked Microsoft ISS web server software. It looked for a specific vulnerability that was known about. It circumvented that vulnerability, deployed malicious payload and opened up new security holes. This is one of the evolutions that we have seen in malicious code or malicious threats over the last couple of years. Rather than single viral attacks, single worm attacks or single attacks on vulnerabilities, people are joining a number of attacks together and creating these multiheaded beasts that circumvent traditional security operations systems.

Senator HUTCHINS—Is there some financial gain for people to do that or is it just outright malice?

Mr Donovan—You are touching on why people write malicious code in the first place. Traditionally, it would be a nuisance. The Melissa mass-mailing email virus was really a nuisance more than anything else. It was designed to replicate. The effect of it was it clogged email systems. With the original Code Red virus the malicious content was to launch what we call a distributed denial of service attack on the White House in the US. Once again, it was a nuisance more than anything else but obviously we know from historical analysis that the effect was fairly profound. It actually brought down significant sections of the Internet backbone based on the number of infected systems and the clogging of those systems. The cost of cleansing systems from that particular infection and vulnerability approached something along the lines of $US2.6 billion in downtime costs to scrub servers, rebuild them and patch those vulnerabilities.

Senator HUTCHINS—Was someone tracked down and charged with that?

Mr Donovan—No. No arrests or prosecutions have been made with Nimda, Code Red, SQL Slammer or Klez. They are probably the top four attacks of the last two years. It is very rare—

Senator HUTCHINS—When you talk about Code Red and all those names, within the computer security industry do they represent significant attacks on the system?

Mr Donovan—They are very significant attacks.

Senator HUTCHINS—Is Bugbear one?

Mr Donovan—Bugbear is a really good one. We can talk about that for a second, if you wish.

Senator HUTCHINS—Yes.

Mr Donovan—Bugbear was picked up by Symantec's office in Sydney. The name 'Bugbear' came out of our security response labs in Sydney. They analysed the attack and determined the fix. One of our antivirus technicians came up with the name Bugbear. We very rarely call a virus by the name given to it by the virus author because we do not want them to achieve the notoriety that they would like to achieve. They might call it 'XYZ'. If we publish it as XYZ then they will go to the world and say, 'Look what I've done,' and will go a couple of levels up the pecking order of the hacker community. We do our best to reduce that kind of acknowledgment.

We tracked down the Bugbear virus, created the fix for it and named that particular virus. Bugbear was an interesting virus because it had specific malicious code hidden in the back of it. First, it was a mass mailing worm, attacking consumer systems; second, it had code which was designed to reduce the effectiveness of not only antivirus systems but personal firewall systems, which are a key component of reducing risk on consumer systems; and three—and this was of particular interest to the banking community—it attempted to deploy what is known as a keystroke logger, which means that if anyone was conducting any sort of online transaction to do with banking or a credit card or whatever, it would capture keystrokes. It would capture passwords, login names, sessions and that sort of stuff and would then attempt to push them out to an Internet address.

Mr Banes—Yes, to an email address.

Mr Donovan—A particular person was aiming to capture as much data about online sessions from as many users as possible. Theoretically, that would then give them the ability to go back in and conduct a perfectly legal banking session, using a known good password and user name, at any of the banks that it had captured information for. The list of banks that were targeted—I think through Bugbear, from the information we picked up from the threat management system—was quite extensive. It contained all the large US banks and links to all of the large Australian banks, including Westpac, National Australia Bank and others.

That is a good example of the evolution of the sorts of threats that we are talking about. They are becoming a lot more insidious, malicious and damaging, but they are also becoming a lot more complex and tricky to pick up. They are specifically targeting industries of this nature. Whereas before it was for notoriety: ' Look, I've hacked into a web site' or 'I've brought someone's server down,' now complex or malicious code is being written to operate with as little

knowledge as possible on the part of the user that that is occurring. It is designed to not let people know that it is operating but to steal information that it can use in the future.

Senator HUTCHINS—You mention electricity in your submission, don't you?

Mr Donovan—We do. Through the information that comes from the threat management systems, and from the information we pull from the security operation centres, we publish on a six-monthly basis a global threat report where we analyse on a global basis where we see these threats being targeted and what sorts of organisations they are targeting. From the information we pick up we generally analyse about 32 terabytes of data on a six-monthly basis, which is an extraordinarily large amount of data. We can determine the targets for these sorts of attacks—not only the consumer style attacks but the more complex blended threats at the higher echelon. Certainly, critical infrastructure organisations like power, energy and gas are high targets. Banking and finance are high targets. They are the sorts of organisations where we see almost bespoke sorts of attacks, written specifically, aimed at organisations in those sectors and designed, once again, to either bring down critical infrastructure or in some cases to pull information from them without people knowing—pulling credit card information from banking authorities et cetera.

Senator HUTCHINS—In the Bugbear and Code Red cases you have talked about, has anybody been charged or convicted?

Mr Donovan—With Bugbear, Klez, Code Red and Nimda, no.

Senator HUTCHINS—Do you know if the police or the authorities are any closer to a result? What about the one that cost $2.6 billion?

Mr Donovan—Code Red.

Senator HUTCHINS—Is that person or persons still out there?

Mr Donovan—No, that person is still out there. The issue is that in some cases it can be quite hard to track down where they are or why they did it, because they are not aiming to pull information back to them. Code Red was designed to exploit a known vulnerability and open up new security holes which would theoretically make these servers even more open to attacks from other hackers. One of the sideline things was the launching of the denial of a server attack on the White House, but that was designed to confuse people more than anything else. We would have to assume that the real objective was to open up more security holes in these servers. Because it was not pushing information back to a specific web address, IP address or anything of that nature, it is hard to determine what they expected to gain, which makes it harder to run forensics on where it came from.

Senator HUTCHINS—You say in your submission that 80 per cent of all attacks detected over the past six months were launched from only eight to nine countries.

Mr Donovan—Correct.

Senator HUTCHINS—Is there any reason why the attacks have come from those eight to nine countries and nowhere else? Is that because they are more technologically advanced?

Mr Donovan—The analysis that 80 per cent of attacks came from the top nine countries is simply because they were the last known source of an attack. It is interesting: most of the attacks on global organisations were launched from the US, because we know from experience that almost the greater percentage of attacks come from within organisations. Whether those attacks or threats to the network security of organisations are malicious or accidental, a lot of them are launched from within organisations themselves.

Second on the list you will find South Korea. That is not because South Korea is malicious in nature or its intention is to bring down the world's Internet backbone; it is simply because South Korea has a large number of broadband connections. There is great implementation of broadband technology in South Korea. However, it does not have very good security infrastructure relating to consumer usage of broadband and, therefore, because of the constantly on, high-speed nature of broadband connections, it is a convenient launching point for attacks. When we start to work back a couple of degrees behind the last known source of the attack, you see countries like China come up a bit further down the list.

The countries that are, from the US perspective, top of the list of cybercrime nations are countries like Cuba, Libya, Iraq et cetera, which are not terribly well known for their wonderful telecommunications infrastructure, so it is unlikely we would see huge numbers of attacks launched from those particular nations. If we are talking about cybercrime and particularly cyberthreats relating to terrorist attacks—cyberterrorism—it is unlikely that you would see a large number of attacks coming from a nation like Iraq or Cuba. It is more likely that they would come from a nation like Australia, the UK or South Korea, simply because that is where the best infrastructure is. And you really only have to have sympathies; it does not have to come from a specific country.

Senator HUTCHINS—I know you said that they have not caught anybody for Code Red, but have they caught anybody in any of these malicious attacks?

Mr Donovan—Certainly, there was the case of the virus that came out of the Philippines about three years ago, where they traced it back to a specific individual. Unfortunately, in the Philippines they did not have the legislation required to make that a criminal offence, and I believe that person is still running free today. Fortunately, in Australia we have made some good gains with legislation making malicious attacks a criminal offence, so I think that has potentially reduced the desire to launch those sorts of attacks in Australia. Knowingly launching malicious code by way of a virus or a worm in Australia attracts a maximum penalty of 10 years imprisonment. That is a fairly good way of dissuading people from doing that sort of stuff.

Senator HUTCHINS—Is there a police profile of the type of person who launches a malicious attack? Are they a 35-year-old dishevelled male who sucks a chuppa chup, has his cap turned backwards and his computer is his life?

Mr Donovan—And drinks diet cola and that sort of stuff. Traditionally—

Senator HUTCHINS—Is that what they are like? Maybe the National Party members are like that!

Mr Donovan—Actually, no. We do a bit of analysis on that sort of stuff, obviously, and we come into close-ish contact with the hacker community. We have a very clearly stated intention of not employing ex high-profile hackers, which is what some of our competitors do in the marketplace. We think that is sailing a little too close to the wind from our perspective. You can probably class hackers into three main groups. The first group are what we class as script kiddies. These are young kids, 15 to 21 years old, who download the latest hacking tools straight off a web site. If you launch Windows Explorer, go into Google or any search engine, type in 'hacking tools' and hit return, a plethora of sites come up that will give you the ability to generate your own malicious codes, worms, viruses, hack attacks or whatever—it is quite simple to do this sort of stuff. Most of that is filtered out as noise by the technology that companies like Symantec produce today. They are known vulnerabilities and they are known attacks, so they are fairly easy to block.

The second group would be politically motivated organisations that are attempting to hack into specific countries, for example, organisations that are anti global trade and that sort of thing. You see attacks on high-profile commercial organisations launched by special interest groups of that nature on occasions. The final group is those that are a little more insidious, those that are a little more talented in what they do. They are the ones that are specifically after personal gain. They are the ones that tend to launch the attacks that are not as high profile because you tend not to hear about them. They are the ones that are trying to steal credit card information or deploy keystroke loggers without people knowing about it. These things are not designed to bring down infrastructure or web sites or hack into web sites or display messages on web sites; they are trying to specifically pick up their own information without people knowing. So they are the three groups that we see—predominantly male, predominantly 15 to 35 years of age.

Mr Banes—Younger now.

Mr Donovan—You would not see many run out of aged people's homes, not that that is necessarily the case.

Senator FERRIS—I would like to ask you a question about chat rooms. We have been hearing in our evidence from previous witnesses about the difficulty of building any sort of infrastructure in a technological sense that would retain information that is put into chat rooms so that it could be used as evidence if people using chat rooms for sexual predatory reasons were tracked down. Everybody that I have raised this with tells that me this is a growing problem but that the difficulty is that there is no technology around that preserves the chat interface. I am just wondering, given your technological skills and knowledge, if you would know of any emerging trends that might provide the technology to either act as a filter on chat rooms like that or retain the information so that it could be used as evidence.

Mr Donovan—Yes, specifically logging at the ISP level. That is a good one for you, David.

Mr Banes—I am the Regional Manager of Security Response for Asia-Pacific and I am also the vice-president of AVAR, which is a malicious code research group.

Senator FERRIS—It sounds like you are the perfect person for that question.

Mr Banes—My hobby is instant messaging and real-time messaging and that sort of thing. I think there are technology solutions. If you look at the whole instant messaging or chat room space, however you want to look at it, there are a lot of third party solutions out there which you can bolt on to existing instant messaging and chat room technologies to record the conversations. It is just a matter of going out and finding the right bits that fit together and knowing how they work. I do not see that there are any real technology barriers there. It is just an extension of e-mail, which we are all used to and is logged and recorded.

Senator FERRIS—So if we as a committee were to make a recommendation in relation to that, it would be possible to find a technological solution?

Mr Banes—Yes, I believe it would be. The only exception that I would make is that, as more and more organisations become security conscious, they start to use methods like encryption to lock down conversations.

Senator FERRIS—Yes, but these people are not those people.

Mr Banes—But a lot of the systems that are coming out now, because of the pressure from large commercial organisations, are starting to put this sort of thing in by default, so there are already chat room and instant messaging and email solutions out there that, by default, come with encryption turned on, and at that point it does make it difficult. You can track the conversation and you can see the volume of data and who is sending what but it is a very difficult job to actually then decrypt it and find out what they were talking about. It is at that point that law enforcement would need significant resources to handle that level of encryption.

Senator FERRIS—I suppose I was thinking of something like the situation that was reported in the newspapers this morning of the 12-year-old girl in the UK who was effectively kidnapped by a guy she met in a chat room. She was clearly duped into believing he was something that he had painted himself to be when in fact he was not. I am just thinking about how her parents could have been made aware of this. If any function key could be eventually built into a computer system, parents could actually record the chat room conversations that their children might be having when they are not around so that they could audit what was actually taking place.

Mr Donovan—You could deploy the Bugbear virus, because it has a good keystroke logger in it.

Mr Banes—There are already lots of products out there with parental controls on them.

Senator FERRIS—Yes. I know Net Nanny and so on but, as I understand it, they are no good for things like chat rooms.

Mr Banes—I would not know on that particular product, but again I would imagine that it is just a technology issue and would not be that difficult to solve. There is a good analogy in the corporate workplace, where we talk about education, training of staff, monitoring usage and that

sort of thing. It falls into that category and the same sorts of technology solutions would be used. It is just a matter of providing something for the consumer space rather than—

Mr Donovan—In the consumer space, all you are looking at doing is deploying a way of capturing the log files—that is, what you actually type in a session—which is not a difficult thing to do from a technical perspective. You then start to encroach upon the area of privacy, which is always a balancing act with security. People want to lock down systems but, at a higher level, want to have knowledge of exactly what goes on. You then start contravening the privacy laws, which are a little open to interpretation in some areas at the moment. This is something we find with our own corporate clients in both the private sector and the public sector—determining the right balance between access to information, locking information down and privacy concerns.

Senator FERRIS—It is an interesting question, because people increasingly appear to be happy, or more relaxed anyway, about the ways in which the Net is regulated and, in particular, about the ABA's role in taking down sites on the basis of complaints and so on. Yet there is very little regulation on chat rooms—there is just about none. People can go into a chat room and appear to be anything or anyone. In the regulatory sense, not a lot is currently being done about it.

Mr Banes—Again, it is just a technology issue. It is the same as phones—anyone can phone anybody and pretend to be anybody. It is a very difficult thing to control.

Senator FERRIS—At least there is the voice there. You cannot, as a 60-year-old man, get on the phone and say that you are a 12-year-old girl, but you can in a chat room and people do.

Mr Banes—It is about technology solutions, education in the home and how parents look after what their kids are doing.

Senator FERRIS—But a lot of parents do not even know how to turn a computer on, let alone get into these sorts of systems.

Mr Donovan—David has raised a very good point. If you are looking for 100 per cent regulation of content through web site browsing, chat room use or whatever, where a parent is concerned about their child's usage, the tools that are available today—the semantic tools, Net Nanny or whatever is available through the ABA for usage by Australian ISPs—go a reasonable way towards reducing the risk. But unfortunately the key to security is that you will never get 100 per cent risk reduction—you will never make systems 100 per cent secure, you will never be able to filter out all the pornography, the bomb-making recipes, the nasty pictures or anything that is used in chat rooms. If parents are concerned about their child's usage, it should be monitored and managed in the same way that they manage watching television late at night—if there is something inappropriate, they switch the television off or take the children out of the room. The same needs to be done with computer usage at this stage. The tools are not strong enough to be able to manage heuristics or artificial intelligence to the level that people would like to see.

Senator FERRIS—In section 2 of your submission, on page 5, you talk about an 81 per cent increase, in a year, in vulnerabilities. Can you take us through a typical case of one of those

vulnerabilities—how you come to know about it, how quickly you can deal with it and what you would do with it—as a real time thing?

Mr Donovan—We discover about 70 new vulnerabilities on a weekly basis. That can relate to any number of applications that we track on a regular basis—an application being a specific software package, email package, database system or whatever.

Senator FERRIS—Or a virus?

Mr Donovan—No. When we look at vulnerabilities, we are specifically looking at the infrastructure—the Internet, the people who use the Internet and the applications that are running on it. On a weekly basis, on average, we pick up 70 new vulnerabilities. We have around 19,000 sensors deployed around the world that feed information back to us about vulnerabilities that are picked up. We actually scan people's systems and they have the ability to send vulnerabilities in to us. We create a database which we then send out through our alerting system. A vulnerability can be something along the lines of what we would term a 'buffer overflow' in a web server, a specific security hole in a particular application, or a backdoor that allows people to log into your computer without you actually realising it. These are all examples of vulnerabilities in operating systems or in applications. In the last period that we examined this data—the six months from July 2002 to December 2002—

Senator FERRIS—So that 81 per cent was over six months?

Mr Donovan—That was over a six-month period, comparing that six months with the previous six months.

Senator FERRIS—Goodness me!

Mr Banes—One thing you have to remember is that there has been really a big push in the whole software community to find these things, so that is one of the reasons.

Mr Donovan—A lot of it is due to disclosure. We have the media reporting new vulnerabilities on a daily basis, companies are more focused on security and therefore they tend to pick up more of this sort of stuff. If you equate it to your home environment, if someone breaks into your house then suddenly you get very interested in security and you walk around your house and notice you did not have a lock on that door, that particular fence was falling down and you did not have bars on that window. Suddenly you discover all these new vulnerabilities because security is a focus for you. That is what we are seeing in the general IT community as well. Security is pretty much top of mind with most private/public education and defence organisations, so we are picking up a lot more vulnerabilities. In a lot of cases they already existed but we are discovering them because more people are paying attention to them.

CHAIR—In your submission there are some concerning issues. It is a bit of an alarming picture in some ways, and obviously this is your marketplace too. One of the concerns we had in Victoria arose when the Victorian Bar expressed their concern over the possibilities under section 25A of the ASIO Act concerning the actions that can be taken over security threats. There were questions as to whether those who are using hacking procedures could fall under the aegis

of this. I wonder to what extent you think we could be see the provisions of section 25A used in this area of infrastructure threat.

Mr Donovan—I am not familiar with section 25A. Does it relate to seizure of equipment?

CHAIR—Yes. There are fairly draconian measures: people can be called in for questioning et cetera.

Mr Donovan—I am familiar with the particular approach that ASIO took towards limiting critical threats in the antiterrorist bill. It is difficult for us to comment because that becomes more of an opinion than anything else. Our responsibility as an organisation is to create a more robust security environment and to alert people to threats as soon as possible and to mitigate risks as much as possible. In terms of the responsibility of government organisations to take action, we stop at the area of education more than anything else. We believe it is in everyone's interests to be more educated about how to reduce security risks as much as possible, not just through technology but through best practices. In terms of the ability that ASIO has to pull people in for questioning over what period of time and seize goods, I am afraid it is really not our area to comment on.

CHAIR—Except that it would appear that most of these threats are actually offshore rather than within Australia.

Mr Donovan—There is a small percentage that is generated through Australia's telecommunications infrastructure, so through Australian users. It is a pretty small percentage though.

CHAIR—So you do not think the issue is significant?

Mr Donovan—No, that would be wrong. I made the point before that it does not matter as you cannot really determine from the last known point of attack—the last known country—where the threats are coming from. You can be 0.001 per cent of the total attacks on critical infrastructure in the world but you could be that 0.001 per cent that has the ability to actually bring the infrastructure down. It is possible that the next Code Red or Nimda or flash threat, which is a more complex and more damaging style of threat that we see coming up in the future, could very well come from an Australian hacking community. There is nothing that prevents Australian hacking communities from having access to the same tools or deploying the same sorts of complex threats as ones that come from anywhere else in the world. So I think it is appropriate that we are given the same sorts of legislative tools and ability to attack criminal activities as other organisations around the world have. We should not presume that, because we are in Australia, in the Southern Hemisphere, a long way geographically from where a lot of these attacks are occurring, we are safe. A hacking community is a hacking community. It does not matter where in the world it is placed.

CHAIR—Senator Ferris has talked quite a bit about the issues of paedophilia, chat rooms, access to pornography and so on. What about the other areas of interest to this inquiry that relate to banking fraud, credit card fraud and so on? Do you think we are up to world's best practice in the prevention of fraud in banking areas?

Senator FERRIS—And in skimming?

CHAIR—Yes. To what extent do you think the banking system is responsive?

Mr Donovan—I think the banking system has traditionally led the way—and it certainly does today—in its approach towards the reduction of risk in its own environment and the reduction of risk to consumers. The issue they face—and this was demonstrated quite visibly with the Bugbear virus—is that, theoretically, their technological expertise is limited at their own gateway; it stops at their own gateway. If you look at the banks' networks or the banks' infrastructures, they provide a service to the consumer community in the case of Bugbear that stops at the banks' own computer systems.

When you have consumers logging in to the bank through their own systems, they bring in their own vulnerabilities. They are blocked at the gateway of the banks; however, if Bugbear had infected their system, if they had a keystroke logger that captured passwords, user names et cetera, and someone was able to get that information—not through the banking infrastructure but directly through a virus like Bugbear—they did not even have to hack into or break into this user's account but were able to access this user's account—because as I said before they had a valid user name and a valid password—to steal money, where does the responsibility actually lie? The bank has done everything it needs to do to secure the infrastructure, but someone else has effectively used login information from a user. Is that the responsibility of the end users, the consumers, themselves, because they did not have security protection on their own system?

I think that area needs some sort of clarification in Australia. I know it is thorny issue, because banks suffer from PR as much as any other organisation of that nature. If there were issues and the banks came out quite strongly and said: 'That is the end user's responsibility. It is not our fault that someone stole their information off their system and stole money from their account, admittedly an account that we manage,' theoretically that should be a reasonable stance for the bank. At the moment, they have no protection against that sort of stuff. The banks have done a great job in focusing on their own infrastructure. They are probably among the top five per cent of secure organisations in the Australian environment. The issue they face is that they have no way of messaging the importance of security or policy to the end users; all they can do is advise. If the government were to join with the banking community and other organisations to raise the profile of general security awareness, it would go a long way to reducing the risk.

CHAIR—So would you suggest something like a general education program?

Mr Donovan—I think a general education program would be great. There has been a lot of talk recently about general security risks—talking about physical infrastructure and talking about being aware but not alarmed.

CHAIR—It is 'alert but not alarmed'.

Mr Donovan—Excuse me, 'Alert but not alarmed'—I did not read my fridge magnet before I came in.

CHAIR—I am glad to hear that you have one.

Mr Donovan—I kept my fridge magnet for posterity. I think that, along the lines of national security awareness relating to IT infrastructure, that would go a long way. Once again, it is not about tools and it is not about technology; it is about best practices. What are you doing to ensure that your own home computer has adequate security on it so that people will not steal your passwords? People tend to think of their home computer as something that does not have anything highly desirable in the way of information. They think, 'I've got a few games on there, I've got a cooking recipe and I access the Net. Why would someone want to hack into my home computer?'

They forget that they do their online banking and they purchase goods over the Net and all those sorts of things where, once again, if a keystroke logger is deployed, people can capture information that can cause tremendous damage to this person. So I think raising the level of awareness about security through best practices, communicated by government organisations and the banking community and through education programs through education institutions, would go a long way towards reducing the general risk. There are a few best practices that you can deploy as a consumer, as a private institution or as a public institution to significantly reduce the risk.

Senator FERRIS—Mr Banes, I will ask you this question, because I suspect it falls into your area: I made a comment earlier to AUSTRAC witnesses that it has been a long time since we got Bankcard—I think it was in the 1980s. When Bankcard came out it had the black strip on the back for swiping and everyone thought it was pretty fantastic technology. But we are still using that now. Credit card fraud, skimming and all the things we have talked about this afternoon, and that other witnesses have talked about, have grown exponentially over that time. But we are still using what must now be considered pretty ancient technology. Are there other ways—for example, an opportunity to choose to have your thumbprint instead of your signature put onto your card or maybe to have eye recognition put onto your card? Are the banks not doing it because it is not worth it? Is that smart-strip technology as old as I think it is?

Mr Banes—I cannot comment from an expert perspective on this, but I can make some comments on the basis of being in the IT security industry for a long time. There have been other ways of looking at this. I think Citibank do a credit card with photo ID on it. Some European countries have tried cards with built-in chips. For example, the UK have an EFTPOS equivalent that does not even require a PIN, so you just swipe it. So Australia is already one step ahead of the UK in that respect. There are a lot of technology things that you can do but when you look at the history of some of these things, the implementation and the user acceptance of them are the biggest hurdles. Often the technology is there but the issues are the cost of the technology and getting people to use it. Again, as John mentioned earlier, you have to make this cost-benefit analysis and if the financial institutions in a particular country have decided that there is an acceptable level of risk with a technology they are using, they are going to continue with that technology.

Senator DENMAN—Are there any disciplines in Australia—I do not expect you to name them—that in your opinion are not as secure as they ought to be? Just a yes or a no will do.

Mr Donovan—I can comment because we see it in the field on a regular basis. It is interesting because it replicates what we saw when they went through the Y2K process—the year 2000 millennium bug. Leading up to it, banking institutions, defence institutions, et cetera—those that

had security, computer or IT usage as the core competency of their organisation—were well prepared well in advance. As it got closer and closer, you saw the traditional non IT based sectors of the industry that use IT systems but did not have usage or management as a core competency lagging well behind. We are in a similar space from a security perspective at the moment. The traditional areas that you would expect to have high security awareness—banks, financial institutions et cetera—are well protected. It is a core competency of banks to have good security. That is why they exist. They have done that for hundreds of years. It is not a core competency of a manufacturing institution to have really solid IT security. They tend to be prone to attacks because they do not have good policy management. They do not have good utilisation or management structures for firewalls, anti-viral systems or intrusion detection systems, and they tend to be the ones that are hit on a fairly regular basis. They are not hot targets where people tend to gain the most. Theoretically, when you go after a bank you get credit card information and that is more usable than stealing the design for the next Nike running shoe or whatever. However, those organisations do tend to lag behind some of the other sectors.

Mr Banes—As well, you have to look at some of the organisations that do not necessarily have enough funding to be able to implement the right level of security. A lot of the dark side of the hacker community will then target those as soft targets to enable launches for different sorts of malicious code networks, which allow them to take over resources in those organisations and use them as launch points for denial of service attacks which could bring down different sorts of networks or launch different sorts of attacks. You will find there are these two sides to it. There is the side that John was talking about—whether these organisations are hardened to the correct level where they have a certain amount of defence—and then there are what you might call the soft organisations—whether they are funded enough so that they are not as soft and they cannot be used as a launch point because this is one of the big things.

If you look at the whole IT security field, one thing that might link all the different aspects of it together is malicious code. It is not just viruses and worms, it is trojans and all these sorts of things. They are often used to deliver what we call payloads—like key logging—but often they are used to set up backdoors to join collections of computers together to end up with a shared and distributed computing resource, which can then be used to transfer data from point to point. The data could be credit card information, images or it could be all sorts of things. If you are looking at it from a national infrastructure point of view then you need to make sure that these soft organisations are well protected in that they have funds to make sure that they can properly protect themselves. Some of those organisations are the areas where you might see hacking and virus writing activity kicking off and you need to stop it at that particular point.

Senator DENMAN—It is vital probably that those sorts of organisations have good educational programs.

Mr Banes—Yes, that is right.

Senator FERRIS—You made the point that the banks are not too bad at this and that if there were enough credit card skimming and other scams then they would probably upgrade their technology. But the reality is that, while banks can pass the responsibility back to the merchant and reverse up to six months later a credit that they have given the merchant, why would they? Yesterday we had some really distressing evidence from an individual who had a terrible experience to the tune of over $100,000 and some of the transactions were reversed months after

they were credited by the bank. I suppose the issue is that, while the banks can do that and get away with it and the little merchants are picking up the costs, the pressure is not going to be on them to the same extent to upgrade their technology.

Mr Banes—I do not think that you can necessarily fix it with technology. I see, as an example, that in Hong Kong the government is issuing digital IDs to everybody and these IDs, like digital certificates, are supposed to be used by people when they are doing online transactions to verify that they are the correct person, so that is one technology solution that you can use. But then you have to look at this: if the average person in the street or any of you here were given a digital certificate, would you know how to store it safely, when to use it and when not to use it, how to configure it and all these sorts of things? I do not think, from an IT security perspective, that you can necessarily rely on IT security to lock everything down.

CHAIR—Thank you for that particularly interesting evidence.

Senator FERRIS—That was very interesting evidence. It was scary.

CHAIR—Obviously you guys are at the sharp end of all of this. We thank you for your evidence today. We may come back to you at some stage, as we lead up to our recommendations, to perhaps test some of them. We appreciate your input today. Thank you very much for the comprehensiveness and professionalism of your input.

Senator FERRIS—Thank you, your comment on chat rooms was terrific.

[4.12 p.m.]

O'MALLEY, Ms Gillian, Manager (adviser to Executive), New South Wales Police

VAN DER GRAAF, Detective Inspector William Bruce, Coordinator, Computer Crime Unit and Fraud Crime Team, New South Wales Police

CHAIR—I call the Parliamentary Joint Committee on the Australian Crime Commission to order. The committee is examining recent trends in practices and methods of cybercrime, with particular reference to, firstly, child pornography and associated paedophile activity; secondly, banking, including credit card fraud and money laundering; and, thirdly, threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime. I welcome Detective Inspector van der Graaf and Ms O'Malley. The committee prefers all evidence to be given in public, but if at any stage you wish to go in camera let us know and we will proceed to go in camera. I invite you to make some opening comments, and then we will proceed to questions. Thanks very much.

Det. Insp. van der Graaf—As stated in the submission forwarded by the New South Wales Police, which I was consulted on, we think that the future of e-crime in terms of banking fraud—that is where I am basically coming from—lies in the use of spyware.

Senator FERRIS—The use of?

Det. Insp. van der Graaf—Spyware. It is a Trojan type program that people can pick up quite innocently on the Internet to capture things like password and log-on details for banks. It is an incredibly easy thing to pick up. We see some opportunity for what is called 'domain server poisoning'. The advice that I have is that it is possible to do—it is not something that every hacker can do but it is something that a few people are capable of doing—that is, compromising the actual domain name server, thereby being able to re-route traffic, say from an Internet banking site. That could be quite a dangerous thing. It has not happened in Australia and I am not aware that it has happened overseas. I have had some discussions with people who claim that they know what is happening, including members of AusCERT who say that it is possible. I would not like to see that happen in Australia.

In relation to credit card tampering, there has been a real problem with that type of compromise and skimming activity. One of the things that happens overseas—and we are not sure whether it happens here or not—is actual physical interception of telephone lines to pick up data. That is okay, provided that the data is encrypted. If, at any point along those communication lines, the data is not encrypted, that could expose millions of users to that type of compromise as well.

My main interest is in the future of Internet security in homes. If people have their systems compromised, banks have got some fairly effective means in place to prevent losses or reduce them, such as your daily limit of $1,000 or $500, but there are some accounts that do not have

any limits. If those accounts were compromised, someone could have their business account cleaned out fairly easily. If the moneys are transferred to a nonfriendly jurisdiction, it really makes the trail difficult to follow. One of the things we have to bear in mind is something that I saw on a chat line by a fraudster the other day, where he said 'We have to make the law enforcement path longer than they are willing to travel'. It was a very insightful comment. These guys are quite effective; they know what they are doing. They have skills available to them that are quite impressive. That is where I see a future threat to our financial institutions.

CHAIR—Thank you. I suppose we can look at the three areas we are interested in and then ask some broader questions. There were some suggestions in our discussions interstate about the need for some centralised body that is responsible purely for cybercrime. Do you share that perception of the need for a centralised body? It seems that everybody shares in it to a certain degree, but no peak body is solely responsible.

Det. Insp. van der Graaf—What the police service has done is to support the Australian High Tech Crime Centre. I am a representative on that body. What we would like to do is to make law enforcement more of a one-stop shop so that any customer anywhere in Australia can come to one body to report a crime and then whoever deals with it can deal with it. We still need people in every jurisdiction because it is the level of cooperation that really counts rather than the number of bodies.

CHAIR—Let us move on to the question of the area that we are responsible for, which is paedophilia activity, chat rooms and access to the Internet. How could that area be improved in terms of the easy access that minors have to chat rooms without knowing the identity of the person they are talking to online? Perhaps firstly we could talk about chat rooms. I am sure Senator Ferris has some questions on that area for you.

Senator FERRIS—This is an area that I have a particular interest in. It seems to me that while there are greater opportunities now to introduce forms of regulation to the Internet, chat rooms are largely unregulated and it is possible for people to appear to be many people that they are not. I notice that on page 2 of your submission you talk about enticing children through online luring and grooming, which is clearly where chat rooms are most effective. I am wondering whether you have thought about any form of regulation that could be technologically implanted into systems to monitor chat rooms. This morning I asked Professor Flint, from the Australian Broadcasting Authority, how he felt about the possibility of law enforcement agencies such as yours being given an opportunity to regularly audit chat rooms on a random basis to make sure that people using them know that they could be monitored. Could you respond generally to the question of the challenges posed by chat rooms, particularly in relation to luring and grooming, which, as we saw in the paper this morning, is happening in the UK?

Det. Insp. van der Graaf—A few issues there are of concern. The FBI do engage covertly in chat rooms.

Senator FERRIS—Successfully?

Det. Insp. van der Graaf—Certainly. They are able to engage paedophiles. Those guys are trained to identify who the likely people are, and the questions come out fairly quickly if you speak to those guys. They can be identified. The problem they have is that there is so much of it.

It takes no time at all to get a dozen targets on a chat room. The decision is: 'Which of these guys is the most dangerous and which am I going to take out first?'

Senator FERRIS—Do you think that would apply here?

Det. Insp. van der Graaf—I would be very surprised if it did not.

Senator FERRIS—Have you ever done any audits of chat rooms? Do not answer if it is difficult for you.

Det. Insp. van der Graaf—Some of us look at chat rooms periodically, but we do not at the moment have a particular program within our unit.

Senator FERRIS—Do you think it would be useful?

Det. Insp. van der Graaf—I would love to see some sort of program. I have had discussions with the High Tech Crime Centre about this.

Senator FERRIS—Fantastic.

Det. Insp. van der Graaf—Alastair MacGibbon is also interested in it.

Senator FERRIS—We have had a meeting with Alastair.

Det. Insp. van der Graaf—Ideally, rather than replicate an identical program, I would like to see a body which does it and forwards the targets to the states.

Senator FERRIS—So you think the High Tech Crime Centre might be the overarching body to do that?

Det. Insp. van der Graaf—I think that is a good place to do it. The actual technology is not so difficult—it just requires some covert access—but it does require some dedication of resources.

Senator FERRIS—Then you would see that being filtered out to the states, maybe on the basis of the postcodes that the tracing goes back to?

Det. Insp. van der Graaf—The tracing is not done by postcodes; it is more or less done by identifying servers through the public source of information, through the IP addresses.

CHAIR—I notice that in your submission you talk about the deficiencies in New South Wales legislation. We are not about trying to criticise any particular state legislation, because this is a rapidly evolving area. You mention section 578B(2) of the Crimes Act 1900 and the question of publishing child pornography. You note that these are summary offences rather than indictable ones.

Det. Insp. van der Graaf—Yes.

CHAIR—You also suggest that a new offence should be established 'for enticing children by online luring and grooming to engage in a sexual act'. Has this been brought to the attention of the New South Wales Police and New South Wales Attorney General's Department? Have you had a response on that?

Det. Insp. van der Graaf—I can tell you that an agency within New South Wales has brought that to the attention of the minister. I am not sure where we are at with that. However, I am not in a position to comment further than that on New South Wales legislation.

CHAIR—Having been involved in New South Wales politics, I understand. We also can look at that in terms of federal legislation. It is part of looking at how we can move forward collectively.

Senator FERRIS—Would you agree that chat rooms represent a new frontier for this sort of operation and these sorts of people?

Det. Insp. van der Graaf—Yes. It is a very dangerous place for children to play in.

Senator FERRIS—Do you think parents realise that?

Det. Insp. van der Graaf—Generally, no.

CHAIR—Senator Ferris has talked about the regular audits of what is happening in the chat rooms and the recommendations regarding the legislation and how we define the offence. What else would you see as important for effective management of this area? Obviously there are the screening devices, such as Net Nanny, some of which are effective and some are moderately effective. Do you have any specific recommendations in that area?

Det. Insp. van der Graaf—I think the best weapon is parental vigilance. Without that, the kids are going to get around it.

Senator FERRIS—A lot of parents cannot turn a computer on. If you are over 35, the chances are you are not computer literate unless you work in that area. It is not a criticism. It is a bit like driving a car. No matter how good the education campaign is, I think it is very risky to expect that parents will be eternally vigilant on this because they are uncomfortable with the technology.

Senator DENMAN—Kids are, and will continue to be, more sophisticated than unaware parents.

Det. Insp. van der Graaf—They certainly are. In terms of technological solutions—

CHAIR—Nevertheless, if you look at it logically, even though parents might not be terribly computer literate, they can still look at the screen and ask appropriate questions.

Senator FERRIS—Yes, but one press of one key and it is gone.

CHAIR—I understand. Anyway, public education is obviously part of that requirement.

Det. Insp. van der Graaf—There is a lot more scope for public education when you consider that many people do not even have firewalls on their personal computers and what they are picking up is quite scary. In some cases, it will only result in financial loss.

CHAIR—How effective have the New South Wales Police been in prosecuting those who have been placing pornographic child sex imagery on the Net?

Det. Insp. van der Graaf—There have been a lot of prosecutions. That is not my area; it is the Child Protection Enforcement Agency. They are swamped with those types of prosecutions and they now refer them out to local area commands.

CHAIR—Are you directly involved in the fraud and banking area?

Det. Insp. van der Graaf—In fraud and computer crime, yes.

CHAIR—It has been a self-regulatory area to a certain extent. How effective do you think that has been?

Det. Insp. van der Graaf—It is difficult for us to comment in the absence of widespread reporting of problems by the banks. If I assume they are reporting serious problems when they get them, I would have to say the problem is small at the moment. We had an incident early this year involving scam email from the Commonwealth Bank. The losses overall were fairly small in terms of general fraud losses, as far as we can tell. The thing that it illustrated was the ease with which you could set up a rogue site or a mirror site in another jurisdiction and then transfer the money overseas. Transferring money overseas and overseas evidence, as you may have read, are other areas which can impact us in terms of cost efficiency and pursuing investigations.

CHAIR—Does your area get involved significantly in credit card fraud?

Det. Insp. van der Graaf—The fraud squad has just completed a task force on credit card fraud, identifying points of common purchase.

CHAIR—Is that public knowledge?

Det. Insp. van der Graaf—Yes, it has been in the papers. There were quite a few arrests.

CHAIR—What is 'common purchase'?

Det. Insp. van der Graaf—A common purchase point is an area, usually a service station, where someone skims a user's card. The information is then passed on to criminal syndicates who reproduce the cards en masse and on-sell them again.

CHAIR—So it is casual workers in service stations who are doing it, is it?

Det. Insp. van der Graaf—Service stations are about 75 per cent of the common purchase points.

CHAIR—Really?

Det. Insp. van der Graaf—Yes.

CHAIR—What are the others?

Det. Insp. van der Graaf—The others are spread over other types of business. Service stations, for some reason, are the most likely places to lose your credit card data.

CHAIR—Is that right? That is very interesting. So what additional measures do you think the community should be taking and we should be recommending—what regulatory controls are needed in that area?

Det. Insp. van der Graaf—I do not have any recommendations for regulatory controls. The offences are fairly serious; they carry serious penalties. There may be room at some point to look at legislation with regard to identity fraud. We have not legislated along those models at this point; some other jurisdictions have. But I believe that the offences are serious and carry serious penalties. Regulation in itself is not going to be the solution. It is about enforcement—and, hopefully, one day a technological solution will arrive. Whether that will be in the form of biometric links to your credit data or some other solution is really a matter for what the community will tolerate.

CHAIR—Yes, it is a trade-off, isn't it, with biometric solutions?

Det. Insp. van der Graaf—Yes.

CHAIR—Is there a prevalence of this type of fraud in the restaurant industry as well? There was some suggestion of skimmer boxes and so on.

Det. Insp. van der Graaf—There have been some widely reported restaurant issues, particularly in Chinatown at some point, but it does not appear to be the current trend.

CHAIR—Do you think it is also a question of education about care in how you use your card?

Det. Insp. van der Graaf—I think so. I think people are aware and do not let their credit card out of their sight. But I have to say that the people who are involved in card fraud are fairly good and there are ways of compromising the card which do not involve anything obvious, such as a chip inside the machine. A lot of the equipment suppliers now make the machines tamper proof, which is good, so that you cannot open the machine. For example, American Express has tamper-proof EFTPOS terminals. If a terminal breaks down, you just replace it. There are no screws to open it. It is a single plastic-moulded unit. That is because on some occasions criminals have inserted their own electronic device to capture the information on the inside and then they come back some time later and remove it.

CHAIR—Because you have obviously been involved in some of the follow-up on credit card abuse, do you know of many instances where merchants were involved and suddenly had to bear the responsibility of the purchase? We heard from one merchant in Melbourne yesterday who outlined an area of fraud which eventually sent his business into bankruptcy.

Det. Insp. van der Graaf—There have been a lot of instances of merchants having to wear the losses.

CHAIR—Really?

Det. Insp. van der Graaf—Yes. And there have been quite a few instances of merchants being collusive. You can tell because they sweep the funds out of the account from which it could be recovered fairly quickly.

CHAIR—In instances where the merchant is responsible, is it because they took down the card number over the phone? We had a presentation by the Australian Bankers Association this morning and they said that if you have run the card through their machine they will take the responsibility, but if the number is taken down over the phone it becomes the merchant's responsibility. Is that what you have found?

Det. Insp. van der Graaf—That is one of the instances. It depends on the individual merchant agreement with the bank, but usually phone inquiries are excluded and the merchants wear those risks.

CHAIR—Right. But have you found some instances where the merchant has had the responsibility for the debt where they have actually run the card through the machine?

Det. Insp. van der Graaf—Occasionally, yes, because some of the agreements allow the customer to deny the purchase. The merchant will wear it then and it is up to the merchant to prove it. We know what the procedures are then.

CHAIR—Yes, that is right. We have heard about the impact. Does the committee have further questions? From our point of view there are obviously a number of potential areas for fraud in this area. Have you seen a rapid escalation in the areas you are pursuing with cybercrime?

Det. Insp. van der Graaf—At the moment, no.

CHAIR—Is that right?

Det. Insp. van der Graaf—Yes. Of course, we have a bit of a horizon. I have some views on what might happen in five years time—of where we might be at.

CHAIR—And what are they?

Det. Insp. van der Graaf—I think the spyware compromise issue is going to hurt some people down the track.

CHAIR—Could you outline what spyware is?

Det. Insp. van der Graaf—Spyware is malicious code or a malicious program which is covertly copied onto your computer, such as Gator eWallet. If you look at the Gator eWallet site there are programs which can be used for legitimate purposes but which can also capture passwords. There were some instances last year of Gator eWallet being downloaded onto

Internet cafe computers. Somebody downloaded this program. It runs fairly secretly; you cannot see it when you look at your task manager in Windows, for example. It captures people's passwords who come in to do Internet banking. A couple of weeks later someone just comes in and collects them.

CHAIR—Right.

Senator DENMAN—I asked this question this morning but no-one seemed to be quite sure. Can you tell me when someone takes possession of an email? Is it when the email comes to their computer and is unopened, or when they open it?

Det. Insp. van der Graaf—Are you asking when they take possession of it at law?

Senator DENMAN—Yes. When literally is it that they take possession? People get charged with various crimes by opening an email which probably is not really their email—but they open it and they are culpable. So when do they actually take possession?

Det. Insp. van der Graaf—When is it in their custody, for example?

Senator DENMAN—Yes.

Det. Insp. van der Graaf—Physically it stays on the Internet service provider's server until they log on. When they log on it is usually downloaded automatically.

Senator DENMAN—So that is when they own it. If it just sits there unopened—

Det. Insp. van der Graaf—On the server?

Senator DENMAN—Yes.

Det. Insp. van der Graaf—Then they have never gained access to it.

Senator DENMAN—Thank you.

CHAIR—In terms of child pornographic imagery, are you pursuing people who use the Internet to look at or browse these sites, or are you only taking action when they download and keep this imagery for themselves? How much of that is occurring and how many prosecutions are occurring?

Det. Insp. van der Graaf—I cannot really speak for that unit; I do not have the data from their unit. There are two people in the child protection agency whose sole work is to engage in that. They are certainly keen to expand into that type of monitoring. At the moment it is impossible to do it in terms of technical monitoring for that purpose because the offences do not justify it.

CHAIR—It was of interest to one of the other jurisdictions we have spoken to. We appreciate your input today. I regret that we have lost some of the people, it being the weekend and because of commitments et cetera, but of course this all goes in the *Hansard* and we have our key people

from the secretariat of the committee here. Thank you for your input. We probably should have put you on first today. In terms of that last question, can I put you on notice in terms of that? Can we have some response back? Is that possible?

Det. Insp. van der Graaf—Sure.

CHAIR—That would be great. It would be helpful in terms of our response on that issue. We appreciate your input. We will be sending you a copy of the *Hansard*. If there are any issues, you can raise them with us directly and then it will be published. Everything was on the public record, so that was fine. Thank you.

Committee adjourned at 4.40 p.m.