COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

Reference: Cybercrime

THURSDAY, 17 JULY 2003

MELBOURNE

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

Thursday, 17 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 and McGauran and Mr Baird, Mr Kerr, Mr Sercombe and Mr Cameron Thompson

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 11.07 a.m.

ORLOWSKI, Mr Steve (Private capacity)

CHAIR—I declare open this public 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. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and to offer guidance as to the role that the newly established Australian Crime Commission might play in combating such crime.

I welcome our first witness. As you would be aware, we prefer that all evidence be given in public, but if at some stage you wish to go in camera please let us know. We are very pleased that you are here today. We know that you have quite an impressive track record. We understand that you are also involved with federal parliament's legislation on cybercrime, and so we look forward to your evidence. We have read your paper with interest; it is quite technical. We understand that you are going to Thailand next week, and so we thank you for your attendance here today; it is really appreciated. I invite you to make an opening statement to the committee.

Mr Orlowski—Basically, I will give the committee an overview of the sorts of cybercrime activities that are occurring in the region so that you can get an idea of how your activities might fit in with what is happening in the region. While I am here in a private capacity, I am also the chair of APEC's eSecurity Task Group, which has now been addressing these issues for some seven years. I will just go through some of those activities so that you can see what we are doing and how it comes together. We were established in 1997 and, since then, we have been gradually expanding our role from what started off as one particular area of electronic authentication.

CHAIR—Are you talking about your consulting group or do you mean the APEC group?

Mr Orlowski—The APEC group. We expanded from just looking at a particular aspect of electronic authentication as it related to electronic commerce, to looking at a whole range of security issues, such as cybercrime and critical infrastructure protection, within the APEC economies. The group is not a legal group; we do not specifically address legal issues. We tend to leave those to established groups such as the United Nations Commission on International Trade Law. Nor are we a standards-making body; we leave that to the international standards-making bodies. We tend to look more at the policy aspects and then we feed requirements either up to the legal groups or down to the standards groups to support the sorts of policy aspects we need. We know from one of our early experiences that you have to address all three levels and integrate them rather than just addressing one without looking at the others.

In terms of specific activities, we have prepared a report on electronic authentication issues which was written over a period of six years, as various papers grew and as the technology grew. I have provided a copy of that to the committee. We have also been working on the interoperability of a thing called public key technology, which is a very strong security tool based on cryptography and which is seen as the cornerstone for electronic commerce in providing secure and authenticated electronic transactions. We have been working on interoperability in respect of how the different laws and the different economies can be

harmonised so that transactions from one economy will be recognised in other economies. Within APEC we have 'economies' rather than 'countries'; that is why I use the term 'economies'. We have been working with the Europeans to try to ensure that we are not working out a solution for our region which is not going to be compatible with the other regions. Between us and the European Community, we cover 90 per cent of the use of the technology, so any approaches we develop together will be de facto world standards.

We developed a cybersecurity strategy which was presented to ministers and leaders at their meeting in 2002 and has been adopted by ministers and leaders. The leaders then made three commitments, which we have been addressing in the last six months. The first is to endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including the United Nations General Assembly resolution No. 55/63 (2000) and the Convention on Cybercrime 2001. They committed to doing that by October 2003. The second commitment is to identify national cybercrime units and international high technology assistance points of contact and create such capabilities where they do not already exist—again, by October 2003. The final commitment is to establish institutions that exchange threatened vulnerability assessments, such as computer emergency response teams, by October 2003. They also called for closer cooperation between law enforcement officials and business in the field of information security and fighting computer crime.

In response to that, we have done a report on what economies are doing to implement the United Nations General Assembly resolution. We are following that up. At the moment—and this is the reason I will be in Bangkok next week—we are running a workshop to assist developing economies, in particular, to develop cybercrime legislation. At the last count, we had 120 representatives nominated for that workshop, which is quite a large number by APEC standards. That will be followed up by in-country training provided by the United States Department of Justice. They will go to the different economies and work with them to try to get that legislation at least underway by October 2003.

Similarly, we have a project to build computer emergency response team capacity which is cosponsored by AusAID, the Australian aid authority. We will be running workshops, again mainly in-country in this case, to assist developing economies in developing computer emergency response team capabilities. On the third point of the networks for contacts, as part of the workshop we are running on the cybercrime legislation we will also be trying to determine contact points and have those established by October this year.

In more general work, we have produced a compendium of IT security standards which documents the main standards that are available and gives a short summary of each. We are in the middle of building a search engine which will allow people to search that database in terms of the specific requirements of their operating systems and type of business. They will be able to retrieve any standards that may be relevant to their requirements. We have been looking at IT skill formal recognition and are in the process of trying to develop a pamphlet which will explain to potential employers what particular qualifications mean. There is a considerable cross-border element in computer skills these days, and people quite often present with qualifications from another economy rather than the economy where they are being employed, and the idea is that employers will be able to understand what that qualification means.

We have also been looking at encryption policies, in that encryption is seen as being one of the cornerstones of secure electronic commerce. The way we are approaching that is to try to ensure that all economies permit in their encryption policies the use of the most commonly used algorithms and key lengths to allow cross-border transactions.

Finally, we have been looking at the issue of child pornography within the context of the cybercrime legislation workshop. There is a specific question in there on what is being done on child pornography. We also had specific questions on fraud and forgery. We are not so much addressing money laundering within our group. We look at the national information infrastructure as opposed to the broader critical infrastructure. There is a counter-terrorism group within APEC which is looking at the broader picture. We are focused on the information infrastructure.

CHAIR—That is pretty comprehensive. We have been chosen for this committee not because of our IT skills, so we do not necessarily want to debate the finer intricacies of what you have been discussing, but more the general principles. The objective of this committee is to look at the three areas of banking fraud, paedophilia crimes related to the Internet, and credit card fraud. Given your experience, what types of recommendations would you be making to the committee on, firstly, the need to coordinate with our APEC colleagues and have an overall consistency of approach, legislation and dialogue and, secondly, what you would like us to follow in terms of the objectives of this inquiry?

Mr Orlowski—In terms of the APEC group, Australia is one of the leading economies in the implementation of measures in respect of cybercrime and cybersecurity. The survey has revealed a couple of areas where there may be some differences between our approach and those of some of the other economies, but by and large they are not considered to be major impediments. We have had representatives of the Attorney-General's Department attending our meetings to ensure that the information exchanges are occurring.

CHAIR—Representatives of the Australian Attorney-General are at your APEC working group?

Mr Orlowski—Yes. We have also had representatives from the Computer Emergency Response Team here in Australia, who will be doing some of the training for us. So there is an interchange at the moment between the APEC group and the Australian government, but it is not filtering down to the state governments. We rely on the Australian government to filter down to the state governments what it brings back. We have also been working with Australian industry groups like the Internet Industry Association to ensure that what they are doing is consistent with what we are doing.

In terms of the specific activities and how they might relate to the committee's work, the electronic authentication work is fairly critical to combating forgery and fraud. We are working with the National Office for the Information Economy, which has been working on authentication techniques for government transactions, techniques which will probably spread to becoming a national approach to electronic identity. Electronic identity is one of the most important issues that has to be addressed. There has been a lot of promise with public key technology as the approach to that, but to be blunt it has stalled. It has turned out to be more difficult to implement than most people thought 10 years ago when we were first starting to

address this issue. Ideally, it could result in people having virtually an electronic drivers licence and a single identity which would be difficult to forge. In terms of fraud and money laundering, if transactions are tied to electronic identities it is going to be difficult to circumvent them—not impossible but difficult.

In terms of critical infrastructure, probably the most important work we are doing is, one, making sure there is a capability within each economy for the computer emergency response teams to address incidents when they occur and, two, the compendium of security standards. By and large, governments set their own standards but the extent of standards use within the private sector is very patchy between different organisations. A lot of our critical infrastructure is in fact operated by the private sector, so there is a need to ensure that they have guidance on the way they should be protecting this infrastructure on which we rely.

CHAIR—Are we likely to see a general agreement amongst APEC countries on areas of concern, the issues of identity and the question of the computer emergency response team?

Mr Orlowski—I think so. We do not have formal agreements within APEC; it is not a treaty organisation. The sorts of commitments given by the leaders in Mexico indicate that the economies will be working together to approach these things. The electronic authentication stuff is what we were originally established to do, and we are well down the track on that. We have at least a general agreement on consistent standards from economy to economy.

All the economies are committed to the CERT workshop. With regard to the cybercrime legislation area, there are only four economies that will not be sending representatives. They are Peru, Chile, Papua New Guinea and Vietnam. Most of the economies will at least be represented at that meeting. There will be discussion on trying to ensure consistency with the cybercrime legislation amongst all the economies and similarly with the CERTs. Most of the economies that do not have CERTs at the moment will be subject to in-country training to ensure that they do develop that capability. Another part of that project is an information-sharing network which will allow threats, vulnerabilities and incident information to be shared among all the APEC economies.

Mr KERR—What about reporting legislation? Many companies do not report to CERTs or anywhere; they cover it up.

Mr Orlowski—That is a problem that I do not think anyone has found a solution to yet. We can encourage it, but I do not know that we could legislate. I do not think it would be effective to legislate a requirement for everyone to report a computer incident any more than it would help to legislate a requirement to report a burglary.

Mr KERR—It is certainly an area that could potentially affect critical infrastructure. If we go down the privatisation track as we have, then huge chunks of basic infrastructure will be managed by the private sector. If their security is penetrated, then there are national consequences.

Mr Orlowski—In terms of critical infrastructure, I agree—that may be a potential area for it. In general, we probably could not legislate for them to report, but for critical infrastructure there may be a case to examine the pros and cons of mandatory reporting.

Mr KERR—We now have provisions that require auditors to report fraud and various other things. If penetration of the security system of AMP or one of those companies caused a crash or something of the kind, many people could lose. Is there any reason why we should not mandate some kind of reporting as we do in certain areas? I concede that normally we do not require people to report crime, but there are some areas where we do, such as where there is a public interest—doctors have to report suspicions of child sexual abuse or violence against children, for example. I do not know the degree of risk. What is out there? I have gone to some of these CERTs and talked to them and they say, 'We only touch a tiny piece of what is actually happening.' Most of this is never disclosed at all. Is that a problem? Have we got big spooky shadows out there that we are worried about that really we could ignore?

Mr Orlowski—It is a significant problem. As to how we should address it, I am not sure that blanket regulation would be the answer, although industry-specific regulation may be an option. For example, banking regulations may incorporate an element to say that incidents that affect the sector must be reported. Health and transport sectors are different critical areas. However, rather than trying to adopt a blanket approach, it would be more useful to examine that at the sector level, where there are already regulations and it is just a matter of making amendments to allow for that.

We have some differences on this within APEC. A lot of economies are trying to put everything into cybercrime legislation. My personal view is that, where possible, it should go into existing legislation. The existing crime should be extended to the computer world; otherwise, eventually, as computers become more pervasive, you are going to end up with two sets of laws which are exactly the same—one for the paper world and one for the electronic world. I do not think that is a good approach. Forgery is forgery, whether it is committed electronically or in the paper world, and should be approached as forgery, rather than having a computer crime forgery provision and having a paper forgery provision.

Mr KERR—You may have to look at the evidential issues. That is really where the cybercrime legislation is important.

Mr Orlowski—And there are a number of offences that are unique to the cyber-environment which need to be addressed in cybercrime legislation. In some economies, the cybercrime legislation is becoming quite bulky because they keep adding new offences which already exist in the paper world. They are creating these new offences in the cyberworld if they are done via computer.

CHAIR—Isn't there a problem in terms of the difference between the public sector and the private sector in relation to levels, standards—the differences are quite significant—and questions of economic security? In terms of APEC, do you see that that is a big distinction between the private and the public sector?

Mr Orlowski—Definitely. There are always problems within the private sector in each economy. We are all experiencing the same problem. The governments are starting to put their requirements in place but the responses from the private sector are, at best, patchy.

Mr KERR—One of the issues that is likely to cause a great deal of difficulty is verification of de-encryption. It seems to me that we have not really seen this emerge yet as a significant

problem. It used to be commonplace, before we videotaped police interrogation, for people to claim that they had been verballed. In an evidential sense, if someone says, 'I've got a PalmPilot or some information-holding device, we have given it to the police and this is what it contains,' you will need a verification process to check any claim of there being a set-up. Is that a practical difficulty? Are there techniques that are replicable and are able to be forged within the evidential chain so that the subsequent addition of data can be identified? Are such claims being made? How are they being dealt with?

Mr Orlowski—I have never heard of such claims being made as yet, but that issue has been raised in theory. There are a number of different elements to it. If you assume that you have got a copy of the original data and the suspect or person involved does not challenge that that is the original copy, then it is relatively simple, without revealing how you managed to get the key, to reproduce in court the process of de-encryption, to take it from the encrypted form. The question of how you got the key is a very sensitive issue. If you start to get to the stage where evidence is challenged, the potential solution, if everyone has an electronic identity, is to get the suspect to electronically sign the data you take, which will then reveal whether it has been altered at all.

Mr KERR—But we do not have that at the moment?

Mr Orlowski—No, but we have not been challenged as yet. Hopefully by the time it becomes an issue we will have it. We may be able to get a notary or someone who has that electronic capability, if each individual has not, to be present with the police and to sign the computer record.

Mr KERR—I have not followed the end of the debate, but I remember there was a huge debate about providing unbreakable encryptions for the general public to use, particularly in the United States where the government wanted to have the public keys. Where does that stand at the moment? Are there private encryption systems in use now that are effectively unbreakable?

Mr Orlowski—Yes, they are commonly available. The net result of that particular debate was not to support the government holding the private keys of all individuals. There are some problems. If you are holding a private signing key, you could then actually forge something. That is almost the situation you were outlining before, of taking electronic evidence and falsifying it.

Mr KERR—Then there was an argument that there should be a trusted third party. Is that where we are at the moment?

Mr Orlowski—No, that has not really developed either. One of the main concerns was that a lot of this stuff is available and you can bypass any trusted third party just by generating a new key. You can generate a new key for each transaction, if you like, and there is no way you can keep track of that. What is happening technically is that encryption packages are being developed which have a voluntary data recovery capability and people are being encouraged to keep a spare key, almost as you do for your house. You have a spare key and then there is more chance that you would be able to get a spare key from someone else if you cannot get it from the person you want to get it from. But the general debate ended up—

Mr KERR—Basically it is over, and law enforcement lost.

Mr Orlowski—Yes.

Mr CAMERON THOMPSON—I was going through the various submissions that we received. The banking association seems to think that the systems to protect people in their use of and access to their bank accounts and those sorts of things are perfectly adequate. There have been a couple of recent examples—there was a warning out the other day about an ANZ web site—where the security of people's access to their own account, and protection from anybody else breaking into that, was placed at risk. I wonder what you think about the standard of the Internet banking security as it currently operates. Is it adequate or does it need radical change?

Mr Orlowski—Adequate—just.

Mr CAMERON THOMPSON—Adequate—just?

Mr Orlowski—In the current situation it is. The banks are moving towards stronger protection, using encryption and using the identity. We think the roll-out of the electronic identity will be more common once the banks implement a thing called Project Angus, which is an electronic authentication technique based on the same standard used by the Australian government in its transactions. In fact, it will be recognised as a thing called the Australian Business Number Digital Signature Certificate, which will provide a much stronger access control technique for users.

However, most of the problems that are occurring at the moment are due to inadequacy within the banks in terms of some of their protective antihacking measures. The Internet itself is not the problem; it is what is happening at the end point where the data is being held. For example, when I use Internet banking I use a password. That password is encrypted as it travels across the network. Unless I am mistaken, I have not had an update for about six months, but up to six months ago no-one had ever heard of a password being stolen in transit; they were always stolen from the bank or the organisation end.

Mr CAMERON THOMPSON—But if people can be duped into providing their password—

Mr Orlowski—If they can be duped, yes; social engineering can do it.

Mr CAMERON THOMPSON—It would just take a thing that looks like their bank communicating with them, and they would communicate with that and in fact hand over their password.

Mr Orlowski—That is a possibility. Again, that is—

Mr CAMERON THOMPSON—Have you heard of that?

Mr Orlowski—I have heard of that sort of thing being attempted; I am not sure how successful it has been. I have also heard of viruses that have been available, which can get into your home computer, grab the password while you are typing it in and transmit it to someone else.

Mr CAMERON THOMPSON—Do you still think that the way it stands is adequate?

Mr Orlowski—In terms of current technology, it is as adequate as we can make it. Once we get to the stronger electronic authentication, it is going to be more difficult. Ultimately, the technology will involve the use of a smart card, which means that the person will actually have to get the card to be able to become you. It is computationally infeasible to break that information.

Mr CAMERON THOMPSON—How far away is the completion of Project Angus? Will that then become the standard way in which people access Internet banking? Would it be secure, in your view?

Mr Orlowski—That would be secure, in my view. How far away it is is probably a matter for the banks; I am not involved in any discussions with them on what their timetables are.

Mr CAMERON THOMPSON—I turn to ISP providers. Does it concern you that there are absolutely no checks on them—no process of licensing or scrutinising them—to make sure that they are not exploiting the material that passes through their networks, which they would have complete access to, for criminal or other inappropriate activity?

Mr Orlowski—There are laws already in place that limit what they can do in terms of communications interceptions, which is how they would access the material. Most of the information, like PINs and passwords, is encrypted when it is passed over the Internet, so the service providers cannot read it. It is just gibberish. That is why we have no history of it being stolen. In terms of communications, it is probably no more vulnerable than the current telecommunications network. By and large, the ISPs are in fact carriage service providers under the Telecommunications Act.

Mr CAMERON THOMPSON—In closing, Symantec—the Norton AntiVirus people—in their submission to us say that there should be an international cybersecurity day on which everyone would be encouraged to drive all the bugs out of their computers. Is that the kind of strategy we should be thinking about?

Mr Orlowski—I do not think one day would do it; no.

Mr CAMERON THOMPSON—I think that they mean an annual event.

Mr Orlowski—Yes, but it is something that people have to be educated into the habit of doing much more regularly. For example, my computer is programmed to go out and check for the latest virus definitions as soon as I switch it on, and you will find that most organisations that have proper security do things like that. They do regular virus scans; I do regular virus scans once a week, just in case one has got past the definition I have—I have a firewall. I think that people need to be educated.

One of the things that I did not mention in this is that APEC, with Idaho State University in the United States, has developed a whole collection of training and awareness-raising materials for cybersecurity. That is available free of charge to any university. Part of our philosophy is that all university courses, not just computing courses, should contain an element of cybersecurity. These days most professional graduates use computers, and we feel that they need to be educated in how to protect their professional, if not their personal, information. We are also looking at the

development of a computer ethics package which would be taught at school. This would start with the basics at school level of teaching kids how they should be protecting their data. That is something that is going to have to happen. It is going to have to be part of basic education that you understand what the vulnerabilities are and what you need to do. It is just like learning to cross the road, as with all of the other basics that you learn. With our society becoming more dependent on computers, the young have to learn that as part of their growing process. The older ones like us are going to have to catch up. I think that the only way that we are going to achieve it is to train from the start.

Senator DENMAN—Several times in your submission you speak of extradition being one of the problems. Why is this such a problem? How can we overcome it?

Mr Orlowski—It is not a problem unique to cybercrime. As with most of these things, there is not the basic framework in place between a number of the economies. It becomes more of a problem with cybercrime because of the global nature of the crime. That is why we have specifically addressed it and why we are particularly raising it in the workshop next week—to see if we can improve the relationships at least for extradition for cybercrime if nothing else. We will try to get recognition of that.

Senator DENMAN—So you are looking at ways of how you will overcome this if that is possible?

Mr Orlowski—Yes, if it is possible. There will be areas of economies in which we will probably always run into problems, but by and large we are trying to educate people that this is a global problem, that the perpetrator of the problem is more likely than not to be outside the economy in which the offence has occurred and that without extradition we are going to be facing major obstacles.

Senator DENMAN—Do you know of any countries that are outside this and are perpetrating these crimes more than other countries are?

Mr Orlowski—Anecdotally, there have been a few countries mentioned. Some of them are APEC economies. Where we can we pay particular attention to them to get them to try to improve both their legal approach and their security arrangements. Quite often it is happening through lapsed security as much as lack of laws.

Senator DENMAN—You speak about October 2003 as the deadline for lots of this stuff happening with the government. Is that likely to be met?

Mr Orlowski—Not completely; I think that trying to achieve all of that in 12 months was—

Senator DENMAN—unrealistic.

Mr Orlowski—Well, in a couple of cases they say ‘attempt’. We have certainly initiated responses to all of those programs. We hope to at least have done cybercrime legislation training, which should facilitate putting the laws themselves in place. We will have done the CERT capacity-building training, but whether the CERTs get up and operational can take several years after we have passed on the expertise, certainly for them to become fully functional. As for the

24/7 contact points, I think we are going to have them pretty well in place in every economy so far as we have already nominated the point.

Senator FERRIS—I would like to pick up the issue that my colleague Cameron Thompson raised in relation to the banks. We have from the witness who is coming later this afternoon a submission which appears to give a fairly graphic description of the way in which credit card fraud can be carried out. He outlines the assurances given by banks to ensure that credit cards are protected and gives an example of how obviously they are not. How difficult is it ever going to be to actually ensure that credit cards are totally safe? Would it perhaps be a better idea for people to better understand that credit cards are not safe? People tend to think that credit cards are fairly safe because the bank tells them they are. This witness will indicate this afternoon that they are not. You say that they are adequate—only just. I wonder if people really have a false sense of security with credit cards, as they are actually a lot more vulnerable than we might imagine.

Mr Orlowski—I cannot speak for the banks regarding figures on—

Senator FERRIS—No, but you know the technology better than we do.

Mr Orlowski—I was thinking more in terms of whether in fact the fraudulent use of credit cards is any higher now, in the electronic environment, than it ever was in the paper environment. It was fairly high in the paper environment.

Senator FERRIS—Do you think it is any higher?

Mr Orlowski—No, I do not.

Senator FERRIS—Goodness me, that surprises me.

Mr Orlowski—One of the issues is that it is higher in certain areas and not in others. In areas where goods are delivered electronically, it is high. But, if you are buying something that has to be delivered, you have to give an address for it to be delivered to, and I do not think it is any higher in that area than it was in the paper world. It is only higher in that electronic area, including paying for downloading music or actually signing up for and running an ISP account.

Senator FERRIS—We were given a briefing by the Australian Federal Police that showed just how easy it is to actually steal an identity, and Mr Thompson has touched on that. It is so easy that it is frightening, and the gadgetry available to assist the process is now small enough to hold in the palm of your hand. I just wonder whether people really need to better understand that credit cards are extremely vulnerable.

Mr Orlowski—I think they need to be aware of what they should be doing to look after them. We get to the balancing act of whether we throw the baby out with the bath water if we suddenly frighten everyone off.

Senator FERRIS—Yes—hence my question. I was going to ask you next whether you have any idea of the actual costs of what you call PKT. As you say, where do you start and where do

you stop? In the end this is going to be an enormously expensive process, I suspect. Have you ever put a costing on what it is likely to be?

Mr Orlowski—No. One of my colleagues is trying to get a project going to do that at the moment.

Senator FERRIS—I imagine it would be very difficult to define.

Mr Orlowski—Yes. In terms of equipping everyone with an electronic identify, the cost of a public key certificate is about $25 per year at the moment and the cost of the storage medium is around $100. It is coming down at the moment, but it is around $100 for a smart card and a smart card reader. The problem is that, if you get the smart cards, most computers do not have readers at the moment. Some new ones are being developed that fit into a thing called a USB port, which most computers that have been bought in the last couple of years have. So at the moment you are looking at around $100 up-front and $25 per year to maintain the certificate. People are not taking it up at that cost. That gives you an idea of the importance they place on their own security, yet they will spend $25 on a new lock for their front door. So that is the problem we are up against at the moment. It is possible that, if the banks were to issue those sorts of technologies for free, people would use them. Once you have it from the bank you can also use it for other activities. Some liability issues are involved, in that the banks may not accept liability if you use it outside transactions with them. But the technology itself would allow you to use it for other electronic transactions which are not just with the banks. The thing is that people are not prepared to spend that sort of money.

Senator FERRIS—Which makes me go back to my original question: is it because they do not understand just how vulnerable they are?

Mr Orlowski—Yes. That is why I mentioned the need to raise awareness.

Senator FERRIS—My final question relates to the report in your document on the economy implications of the UN General Assembly resolution. Have you any information on where the offences occur? The first dot point you give in that summary is the elimination of safe havens and the coordination of law enforcement cooperation. I am just thinking of the countries involved in the UN. I think we all get the Nigeria offer of the $8 million transfer once or twice a day. Are you able to tell us whether the UN has a definition of the location where the offence would occur? Would it be, for example, where material might be sent from or where it might be received that the crime would be committed? In the case of the electronic email from Nigeria or wherever else it comes from, such as some of the more primitive technological African countries, how would it determine where the crime occurred? Would it occur here in Australia if someone was silly enough to transmit some money or in the place of the transmission of the original document? It seems to me that it would be very difficult to eliminate all the safe havens.

Mr Orlowski—I have not got the exact proportion of the APEC economies concerned, but of those that responded the majority have extraterritorial jurisdiction. They have written it into their computer crime legislation so that they can prosecute either for the offence being committed in their country or the offender being in their country, and again prosecute outside the country and request extradition. They are trying to eliminate the safe havens by saying, 'Wherever you are, we will get you as long as there is an extradition treaty.' That is why that extradition issue is an

issue; we need to be able to do it with most economies. We are encouraging the approach that it is an offence either if the person conducts the offences in your jurisdiction or if the damage is done within your jurisdiction.

Senator McGAURAN—Following on from Senator Ferris's comments: who takes liability in regard to credit card fraud—for example, if goods were not delivered? I had a similar experience myself recently. I questioned what was on my credit card. If it is found that I did not undertake that transaction, the banks take the liability. Am I right or wrong?

Mr Orlowski—No. In general terms it is the merchant. I think one of the banks had their web site hacked into and some information was taken, and the bank admitted liability in that case. By and large, the bank charges back from the merchant.

Senator McGAURAN—It is only when it is a bogus merchant that the liability comes back to the card holder?

Mr Orlowski—Even then I am not sure. I am not a lawyer. I am not sure exactly how much liability falls on card holders. It depends on your contract with the card issuer.

Senator McGAURAN—Which may explain Jeannie Ferris's concern that the public are a little more relaxed than they should be with their credit card being spread all over the Internet. What is the law on that? Is there any law in regard to who picks up the liability at any one point, or is it 'consumer beware'?

Mr Orlowski—As far as I am aware, it is governed by contract—the terms and conditions of use that you signed and which the merchant signed with the bank. That can vary from economy to economy, from bank to bank.

Senator McGAURAN—Are the banks liability free?

Mr Orlowski—They may in the terms and conditions say: 'If you have protected your pin then it is at $50, we will pick up the difference.' I am not sure. It would vary.

Senator McGAURAN—Wasn't there an example perhaps earlier this year of credit card fraud involving someone skimming small amounts? Perhaps it is not the big amounts that we need to be concerned about. Most people do not notice the small amounts. It was to do with bogus Qantas charges or something like that. Do you recall that incident?

Mr Orlowski—I am afraid I do not. That technique has been used since computers have been around.

Senator McGAURAN—It was $20 here and $20 there.

Mr Orlowski—Even a cent here and a cent there over enough accounts can be quite significant.

CHAIR—At our briefing by the AFP, they talked about the great majority of computer owners not having virus scanners. If they universally worked then we could consider a

compulsory requirement for virus scanners. How reliable are they, and is there the need for a greater requirement for those who produce the computers and software to provide virus scanners?

Mr Orlowski—The effectiveness of virus scanners varies from product to product. Whether you have the software or not, the main thing is whether you are updating that software. As I said, as soon as I switch on it goes out every morning and updates the software. I have friends who have had a computer for two years with an antivirus package who say, 'Yes, we have an antivirus package,' but they have never updated it. They have not got the latest virus definitions. Even if manufacturers were to provide the product, there is still that educational aspect—making people aware that they need to update that regularly and they need to go and get the definitions.

CHAIR—So it is an education issue rather than anything that we could require?

Mr Orlowski—Yes.

Senator DENMAN—I believe that mobile phones are becoming so sophisticated that some of this cybercrime stuff will be able to happen over them. Is that right?

Mr Orlowski—I can access the Internet and get my email on my phone.

Senator DENMAN—So that is going to add another dimension to all this.

Mr Orlowski—Yes. The whole question of wireless communications is a major issue that we are addressing. We have actually put in a specific item in our terms of reference to start looking at wireless aspects. I have a war story, if you like. We had a meeting in Kuala Lumpur where a wireless network was put in for the convenience of delegates. One of the delegates, who had a bit of a hacking bent, managed to get into everyone else's computer that was connected to that wireless network, without even needing their passwords.

CHAIR—Is that right?

Mr Orlowski—Yes. There is a whole range of educational issues with regard to new technologies, which are being rolled out without all the security aspects necessarily being considered at the time the products are put on the market. It would not happen with mobile phones because they are encrypted as part of the service, but this particular service did not require encryption between the different elements. Once you logged on, you were open to anyone else who was logged on.

Mr KERR—Have you had any discussions with AusAID? In these types of havens there is often no real economic reason why they would bother with this. I can remember going to Vanuatu and making the absurd case that it was in their interest that they should assist us in anti money laundering. It was in our interest that they assist us with anti money laundering, and ultimately the political and economic pressure that the United States and Australia brought to bear led them to do that. These countries have no real interest in spending huge amounts of money putting in the infrastructure that we would wish them to put in place. Is there an aid strategy developing out of APEC to help with some of these smaller countries? Presumably, the bad guys will simply relocate to more friendly territory when they can.

Mr Orlowski—AusAID is certainly working on the CERT project. They are funding six of the 10 economies through the CERT capacity-building project because they are in the immediate region. There are two aspects by which this could be done: firstly, raising their awareness to start with—the problems it could cause for them—and, secondly, as you say, funding some technology that may be needed to secure their networks to prevent problems for us from their networks.

CHAIR—Unless there is an absolutely burning question—it would have to be good—

Mr CAMERON THOMPSON—Is there something international that agrees that organisations that are providing antivirus software are in themselves unable to be corrupted in some way?

Mr Orlowski—No, most of the major virus protection software providers are members of professional organisations—usually professional security bodies—and are bound by codes of ethics. But, in terms of them having regulations to ensure that they do not employ rogues who might put loopholes in antivirus software, and things like that, no, I am not aware of any.

CHAIR—That was a fair question. Mr Orlowski, we may come back to you, in terms of your experience of working with APEC, as we work our way through and consider some of the recommendations that we might want to make in our inquiry, if that is okay with you.

Senator FERRIS—Perhaps about things that come out of your conference.

Mr Orlowski—Yes, I was going to raise that. I raised with the secretary this morning that I have a draft document, which I am still working on, which goes into some more detail on some of the issues that have come out of the survey. That will probably be finished on Monday, and I could arrange to get a copy to you as soon as I get back from the conference.

CHAIR—We are blessed with a very competent secretary, so, if you wish to discuss it with her, that would be great. Thanks for coming. We appreciate you taking the time and wish you well with the conference in Bangkok. Does it start on Sunday?

Mr Orlowski—It starts on Monday morning.

CHAIR—Thanks very much.

Proceedings suspended from 12.07 p.m. to 1.10 p.m.

LORKIN, Mr Edwin James, Barrister, Victorian Bar; and Secretary, Criminal Bar Association

CHAIR—I call the committee to order and welcome Mr Edwin Lorkin, representing the Victorian Bar.

Mr Lorkin—I am also Secretary of the Criminal Bar Association, which is a division of, but separate to, the Victorian Bar. To that extent, I was consulted, as were the other executive members of the Criminal Bar Association, by the Victorian Bar in connection with the request from this committee for input.

CHAIR—Thank you. As you are aware, Mr Lorkin, the committee is examining recent trends in practices and methods of cybercrime, with particular reference to, one, child pornography and associated paedophile activity; two, banking, including credit card fraud and money laundering; and, three, 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 would like to thank you for appearing today. As you appeared before us in our previous guise as the Joint Committee on the National Crime Authority and your input was quite valued at that point, we thank you for your input once again. We look forward to your opening comments, and we will follow them with questions.

Mr Lorkin—Thank you. First of all, and traditionally enough, could I thank the committee for asking the Victorian Bar to consider the terms of reference. More particularly in that context, as I recall the way in which it developed, the terms of reference appeared extraordinarily broad, and that is perhaps understandable. But, in making a sensible response, the Victorian Bar felt it lacked sufficient particularity to grapple with the issues. The bar would like to thank the committee, particularly its secretary, for acknowledging the difficulty the bar was under and for acquiescing in the suggestion that, when the ACC's submission was lodged, it be made available to the bar so that it could see a bit of the flesh on the bones of the terms. That has been of great assistance.

In looking then at the almost 60 pages of submission from the Australian Crime Commission, the bar concluded that there was very little in that that it felt required comment from a body of its type, in part because a whole lot of the issues seemed to the bar to be setting the scene—and that is understandable; it is almost a benchmarking of the position so far as the ACC sees it at present—and some attempt to prognosticate where it may go, emerging trends and what part of the armoury of law enforcement that it would see itself bringing to bear on those issues. The bar believes it is better educated as a result of reading that material but probably cannot make any sensible comment upon it.

That said, however, there were a couple of elements towards the end of the document which the bar did feel it should comment upon, principally because on one view of the executive opening it might be said that those portions of the submission that dealt with cyberwarrants, and in particular the portion dealing with section 25A of the ASIO Act, might be articulating a case for the addition of a section 25A equivalent into either the ACC toolbox to pick up that term or

the powers of one or a number of the associated law enforcement agencies that the ACC deals with on a regular and consultative basis.

The bar's view, and it is set out very briefly in the eight paragraphs or thereabouts, is that there is no articulated case in favour of that and, moreover, section 25A should be seen as a specific power reserved for matters of national security. It has to be understood that the power is only triggered in accordance with the provisions of 25(2) and only when the Attorney-General is personally satisfied that the triggering requirements are met. It is a very high level set of problems that 25A is concerned to address and it is a very high level trigger before the power of up to six months—I think—of constant monitoring of computer services can be permitted.

The bar's position is that that should not be seen as a blueprint or a footprint or in any other way a power which ought to be uplifted and dropped into normal law enforcement regimes. When I say normal I would include in that the ACC, although, of course, the ACC is already seen to be, in a fulcrum sense, a very important national body, and neither I nor the bar are seeking to debate that. Nonetheless, the bar's position is that the power would not be appropriately uplifted and dropped into the ACC and that nothing, frankly, in the documentation that has been put before the committee, at least from the ACC's submission, can properly be seen as justifying that. It was lest we did not say that and that later on it was said, 'There it is; that is what the submission was contending,' that we made what might be seen as a defensive submission, and it remains that. It is not getting any better for repetition, so I will stop repeating it. That is the extent of the interest that we have.

CHAIR—I am sure Duncan Kerr will lead the charge once more, but before he does I have a question. In representing the bar, to what extent are the normal ways of detection, prosecution and conviction in the legal process relevant to cybercrimes, and what paradigms do we need to shift in Australia in 2003?

Mr Lorkin—I agree with that. The bar does not wish to say, 'Here we are in 2003 but let's pretend it's 100 years ago.' Far from it. Modern criminal techniques do embrace cybercrime and do ignore borders that are national or international, and they have to be dealt with and resisted by appropriate techniques. There is no doubt about that. It is always tempting though. The committee might remember that I was the Commonwealth Associate Director of Public Prosecutions for five years. I have been on that side of the fence and indeed I prosecute regularly enough, so I have an interest in, as does the bar, proper levels of balance existing in law enforcement. The contention I still make is that, tempting as it is to look over the fence and have a look at 25A from a law enforcement perspective and say, 'That looks really interesting; let's have one of them,' it is not enough to simply put it that way. With respect, that is how this submission is couched.

I think one would have to look at the case, if it is articulated, and be very responsible in dealing with it by meeting whatever contentions of shortcomings or failures or omissions or inabilities to progress investigations, and deal with those sequentially. But they need to be the subject of a proper analytical response, after being properly laid out, and that is not where we are at all. I do not disagree, Mr Chairman, that we need to have a set of responses that meet the threat, because otherwise law enforcement is simply running down a track which the criminals will skirt.

Mr KERR—I have a few general questions. First, you would recall Steve Orlowski—a witness before us this morning—who was previously from the Attorney-General's Department. He now provides advice to APEC countries. He was making the general point that he thought that we should develop our criminal law by adjusting, if necessary, elements of the ordinary framework of the law—so that fraud would, if necessary, be broadened to incorporate elements that might be connived by new technologies—but that we should not rewrite a whole separate criminal code for actions in cyberspace. He was saying that we should adapt existing criminal law and that there is a debate going on within the APEC countries as to whether or not you need a separate codification of a whole set of offences. Could you give your reflection on that.

Mr Lorkin—Only in a general sense. I am not aware of the debate that you refer to. One can make perfectly defensible arguments in favour of either an engraftment—by referring to the present state of the criminal law and simply adding on or amending the provisions to make sure that they catch the impugned behaviour if there is a gap—or, alternatively, the creation of a cyberspace criminal code. I must say, as a traditionalist, I would be more inclined to agree with the submission that was made before you this morning than to keep creating slabs of associated and side-by-side legislation. That is only, I suppose, a drafting preference.

One imagines that the provisions, wherever they are found, after due consideration ought to be pretty much the same. I guess we should not worry too much about practitioners but, through the practitioner to the client, if there is only one tome that one has to go to and master and so on, it is far easier. Indeed, the Cybercrime Act itself is an example. In the Western Australian bar, for whom I am not appearing, it may well be that X per cent are aware of the Cybercrime Act. They are all aware of the Criminal Code, but they are instinctively not aware of the Cybercrime Act. Even running the risk of having a code which necessarily expands physically is a better risk, to my mind, so that the people who are charged with advising clients, governments or whoever are more likely to be across the developments. That is only one aspect. I do not know how helpful that is to you.

Mr KERR—There are two other issues that interest me: one is the practicalities of evidence, and you are working in that field—

Mr Lorkin—Yes.

Mr KERR—Do you have any comments to make about the procedural side of the law, rather than the substantive side, that we need to take on board and address?

Mr Lorkin—That is an interesting issue, because this is a federal committee. When we get down to the hurly-burly of prosecuting for Commonwealth criminal offences, we do so pursuant to the evidence acts of each of the states and territories—although a movement towards adopting a uniform evidence act is already gaining momentum. It applies in New South Wales, and Victoria is certainly looking at it. I do not want to suggest that that is a perfect model either, but it is very difficult if the model changes depending upon where you are, if the rules of evidence materially change depending upon what side of the border you are on. I do think that is a significant issue.

I do not know that it is the function of this committee, but it seems to me that during the first half of this century we should be aiming towards a far more uniform system of criminal law in

Australia from top to bottom—from investigative measures through to sentence, through to incarceration, through to release. It is a very odd thing that our 18 million citizens are exposed to such an extraordinary range of techniques across all of those strata—each one vigorously defended by the persons who live in that state, or not necessarily—such as rights to committals. They are very fundamental issues and matters of great practical moment.

The concept of fraud and cybercrime is an interesting link. If you leave pornography to one side, cybercrime is probably all about defrauding in one sense or another—shifting money, shifting the proceeds of crime, emptying someone else's coffers, intellectual property—and classically depriving the due owner, maybe the Australian Taxation Office, of their entitlement.

Mr KERR—By a trick.

Mr Lorkin—Not necessarily by a trick, but in any event doing it to the potential detriment of the other person. White-collar crime is hard enough to prove when there is a victim—not necessarily a victim that always attracts sympathy, but usually a victim. Cybercrime is such an ethereal issue—unless it is within the realm of normal victim analysis. Pornography is a good example of where I think the prospects of putting forward the case, everything else being equal, and achieving a conviction would be predictable, but I am not so sure in other areas where it is dollar driven—against a major bank or maybe against an international bank—how easy that is. I think that is yet to be the subject of a real test, but I would not be surprised to find that the cases become longer, slower and more bogged down. The introduction of evidence from overseas is still full of difficulty. The major impediment is often not at the court end but at the investigative end. It is just understandably difficult and slow. Cases that occur in 2003 might be trialled in 2010. It just gets harder.

So, full circle, does that mean that you knock down all the walls to make sure you can investigate without any difficulty or impediment? The answer to that, in our submission, is clearly no. Again, it is a question of finding the right balance. But in finding the right balance, if I can return to that theme, it is our submission that it is incumbent upon the person who seeks these powers to articulate a very well-reasoned, well-researched and well-defined case to those of us who otherwise might say that the sky is falling. It seldom does fall, but you have a concern that the pillars are being pulled out left, right and centre. Those pillars are hard to replace once they are gone, and we therefore say hasten slowly. It is just like prosecuting: if you want to prove the case, you have to prove it. It is no good saying, 'We think we would be better off with a guilty verdict.' It is not like that. That is not very helpful, I suppose; but the analogy is not imperfect either.

Mr KERR—Currently we can access data servers seized by warrant.

Mr Lorkin—Absolutely.

Mr KERR—There is interception capacity under the Telecommunications (Interception) Act, so warrants can be issued judicially.

Mr Lorkin—And are.

Mr KERR—Yes. Are there any gaps in that? There is one thing, which I did not think about, that may be a gap. Steve Orlowski was talking this morning about open networks—the idea that you walk into a space; there are no lines. There is nothing that you can identify to intercept, except that you have a receiving device and everybody in that space is capable of instantaneous communication with you. I am talking about wireless communication, Blue Tooth systems.

Mr Lorkin—I see.

Mr KERR—I forgot the technical jargon. Through the work you did as a prosecutor and now as a defence advocate, are you aware of any areas that ought to be tightened up? You are warning us against one specific tightening up—I accept that—but you say there may be some areas which emerge that should be specifically addressed in the existing regime. Is there anything that you are aware of or have heard of?

Mr Lorkin—There is not. I am not aware of investigators saying, 'We know of this form of criminal conduct that is occurring but our present ability to intercept or to persuade a judge to issue a warrant on this, that or the other is inadequate.' I would expect to know that. I am not saying it does not exist, but I do not know if it does. This seems to me to be saying that there are limitations in time. Of course, from a law enforcement officer's perspective, that is a matter of considerable annoyance. How does one really forecast that the interception of the suspected conversation, data or whatever it might be will occur in the next six days? I can follow that that is difficult. On the other hand, presumably the draftsperson and the parliament thought that, on the material then available, that is what an investigator ought to be able to pinpoint and that was a reasonable balance between the rights of people to have their communications freely and the need for law enforcement to intercept.

I do not know whether the changes in criminal conduct are such as to make that sort of time frame now not adequate but that is not really what is being put here. They are not saying that they have reason to believe that, were they permitted to listen, intercept, for six weeks, two months, three months or four months, their catch would be greater. They do use the word listening in to the `offender.' There is a bit of assumption in all of this.

Mr KERR—There are two practical reality changes. One is that people who are the subject of these warrants can now have non-intercepted communication. Again, we heard this morning that the battle to prevent encryption of a standard that is unbreakable has been lost. Law enforcement has lost that argument.

On the one hand, it does not matter how long your warrant is for an interception; if it is encrypted both ends, you are just hearing noise. On the other hand, if there is not high-level encryption, then new law enforcement tools mean that what used to be an extremely resource-intensive activity—it could take six days—is less resource intensive. The biggest constraint in the past on interception was resource limitation. You would have to have someone sitting there—and you cannot afford to have someone sitting there—listening for six months to people talking about their grocery bills. So there were resource limitations there, but now with technology, you can plug in and you do not need a human being to listen. You can have a whole series of triggers, and then electronically select out that piece of message and you only have to listen to a small piece. It is interesting that it is an all or nothing exercise now whereas before it was quite different.

Mr Lorkin—With the risk of the skies falling emerging again, my real concern with that sort of analysis is that, fundamentally, you may as well have everyone being listened to at all times because there is no human resource involved. A computer can go 'Bing!' and we can listen and find out whether it was a humorous aside between two drunks or whether it was just people playing the fool or whatever. Of course, the answer to that is that you would not do that. It would have to be subject to judicial sanction and there would need to be proper evidence of the offender mentality and so on. It does not appeal to me. We all know that from jurisdiction to jurisdiction there are very different attitudes to what is a fair trigger for the issue of warrant, and so it would be in this case. It is very hard to control it in a proper way.

Mr KERR—Anyway, if it were a serious criminal they could scramble or encrypt their conversations so that you would get all the couriers and none of the big players.

Mr Lorkin—I think that is right. Then you may say you would be able to break the couriers down but there are—

Mr KERR—a whole set of balances, as I understand it.

Mr Lorkin—Exactly.

Mr KERR—I am sorry I have wasted everyone's time.

CHAIR—No, I think it was valid.

Mr CAMERON THOMPSON—Is there a standard protection of data that all law firms and barristers offer their people? We hear about people hacking in when there may be serious personal data in there, and even with courtroom records it may be possible to hack in and change the transcript in a case.

Mr Lorkin—I would love to do that!

Mr CAMERON THOMPSON—What!

Senator FERRIS—Hansard better not record that!

Mr CAMERON THOMPSON—Is there any standard—

Mr Lorkin—I do not believe there is any standard at all. It is a very interesting question because you are quite right: the amount of intensely personal and privileged—in a legal sense—communication about clients or potential witnesses or whoever is extraordinary and probably does represent a hacker's paradise. There are no firewalls that I am aware of. For example, in the Victorian Bar there is an intranet for email—I think that is what it is called, or a wide area network or something. It would have a firewall at the point at which external communication attempts to get into it. Within it, I am not so sure. I am saying that I am not so sure—it is probably well protected; I do not know. But in a general sense, with the computers in my chambers, you are quite right: hackers could very simply get in. I am quite worried about it.

Mr CAMERON THOMPSON—Without personalising it to your particular case, in general do most law firms establish some kind of hacking monitoring, firewalls or virus scanning?

Mr Lorkin—Yes. According to my experience—and it is a bit dated now—all of the major governmental agencies and all of the major law firms that I am aware of have firewall protection and all the usual antivirus materials. Whether any of that is ultimately sufficiently sophisticated enough to prevent a genuinely skilled hacker from getting past it, I do not know.

Mr KERR—I do not think it is. That is why the United States, for example, has four levels of telephonic communication. The top one has only five phones in the system because it is for the President, the Secretary of State, the Secretary of Defense and what have you. Unless you have a closed system, anyone can get in.

Mr CAMERON THOMPSON—Has that issue been raised among members of the bar?

Mr Lorkin—Not to my knowledge. As I say, not all barristers are part of and elect into the email system. I think that would be fairly well protected. Again, as I understand it, that is a relative term. I am not aware of it being raised specifically from the bar to members of the bar.

Mr CAMERON THOMPSON—What about in communications? Do law firms and barristers use the Internet to exchange pieces of what could be personal data of clients relating to court cases?

Mr Lorkin—Of course. Yes. If I am involved in a multicounsel case, a lot of material is emailed. The amount of personal data is probably quite limited because most of that would be held tightly within—

Mr CAMERON THOMPSON—I am sure a lot of it would be sensitive, though.

Mr Lorkin—Absolutely.

Mr CAMERON THOMPSON—Are you fairly confident of the security of that system when you use it to exchange that data?

Mr Lorkin—I do not feel that it is likely to misfire, but the issue is whether or not someone can come in through it. Frankly, that is a technical area which I have got no ability to comment on, except to say that it is a relatively recently established network and that it was established by external consultants. One imagines that parts of their terms of reference were geared to security issues; but I do not know the particulars of that.

Mr CAMERON THOMPSON—Before all this wonderful gadgetry, did you use registered mail and that sort of thing to protect the data that you sent to a client?

Mr Lorkin—No.

Mr CAMERON THOMPSON—So it would just be a normal mail situation?

Mr Lorkin—I suppose it depends. If there was a particularly sensitive document, I suppose it would have gone either by courier by hand or by registered mail. Having said that, I do not think the vast majority of material would have fallen into that category.

CHAIR—In terms of your comments about the ACC and the role it would play, don't you see the potential for hackers getting into power and water supplies and banking et cetera as constituting a national security issue under section 25A of the ASIO bill?

Mr Lorkin—Absolutely. With great respect, that would then be dealt with within the confines of 25A and subject to the quite tight triggers that exist. I am not for a minute disputing that. If a threat to national security were to emanate through cybercrime techniques, that would satisfactorily fit within the definition of security within, I think, section 4 of that act—it is not a problem.

CHAIR—Someone has suggested changes in the cybercrime area. In terms of your comments on warrants, how would that fit with traditional warrants? Do you see any problems in bringing the two together?

Mr Lorkin—Not really. The suspicion, which is the trigger for the application, would still necessarily be grounded by reference to intelligence of some sort and the context in which it would be expressed in the information provided to the person considering whether or not to issue a warrant. It would presumably need to articulate with some precision what the systems were, in what way they were believed to be operating, why that constituted criminal conduct and so on. I do not think it is difficult to do that. There are plenty of areas that are necessarily factually complex which are understandably the subject of warrant issue. That is really just another example of that sort of thing, it seems to me.

CHAIR—I remember the input of the Victorian Bar in relation to the ACC legislation. Are there things that the bar feel strongly about that you would like to see recommended in this area, in terms of changes that might be necessary?

Mr Lorkin—That is not something on which I have received any instructions from the bar, except to say that the submission itself recalls the fact of the previous hearing and—

CHAIR—Yes, we remember it well.

Mr Lorkin—I think it repeats the concerns and the in-principle objections et cetera but decides it is not appropriate to renew those now. I do not think it would be appropriate for me to go beyond saying that. Certainly nothing has been mentioned to me that would be appropriate to pass on.

Mr CAMERON THOMPSON—That being the case, I would like to pursue some of the things I was talking about before. When we are talking about critical infrastructure, what proportion of court records and things like that are now kept in computer files as opposed to paper files—do you know?

Mr Lorkin—I would not know. It would be a pure guess, unfortunately.

Senator FERRIS—What about your own material?

Mr Lorkin—In my case? If I look at my chambers, I would like to think that 90 per cent of it must be in written form, but I know that is not right. There is an enormous amount of material on disks and hard drives and so on. In terms of a percentage, I would hate to think; I cannot make that guess for myself either. I think there would be more on computers than there would be in physical form.

Senator FERRIS—That sort of begs the question about the Privacy Act, doesn't it, in a way, because in the past it used to be that files were locked up every night. In our own situation we get a lot of private material—constituent problems—and we have one room that we are able to lock up, but there is a massive amount on our hard drives and it would be a matter of walking out with a laptop sometimes. It is an interesting question. I was thinking about it when Mr Thompson was asking you the questions before; you think about your own situation.

Mr Lorkin—I agree with you.

Mr CAMERON THOMPSON—When we are talking about attacks on critical infrastructure, we tend to think of people hacking in, getting hold of the valves in the sewage plant and turning them all around the wrong way, whereas I would think that if someone, for example, were to dump a virus that ate up all the court records it would be a horrendous impost on the legal system.

Mr Lorkin—It would be. There is no doubt at all about that. Again, I would think there would be fairly sophisticated firewalls at the point of entry.

Mr CAMERON THOMPSON—Backups?

Mr Lorkin—I am not sure about backups—perhaps. I think post September 11, at least in the court structures in Victoria that I am aware of, there has been quite a significant security shift. Points of entry and so on are much more carefully patrolled, monitored, scanned and so on. That will necessarily help on the cybercrime front, but—

Mr CAMERON THOMPSON—Seeing that you raised that issue—and your criticism of section 25A and that process—I raise the fact that there is the potential for a terrorism element in this. Doesn't that then warrant the ability to be able to use that?

Mr Lorkin—With respect, Mr Thompson, that ability presently exists. Provided the suspected behaviour fits the definition of 'security' in section 4 of that act, then the fact that the behaviour is being carried out by use of cybercrime techniques will not mean that government will not be able to deal with it provided it has the necessary impact on national security. In my submission—and I cannot remember the definition verbatim—it certainly involves infrastructure protection so that dams, power stations, nuclear facilities—

Mr CAMERON THOMPSON—Court records!

Mr Lorkin—I do not believe so. Frankly, I do not think criminals would see how to make a quid out of getting in and knocking over the court records. If they wanted to be highly sophisticated vandals then of course they could.

Senator FERRIS—Changing transcripts could be to their benefit.

Mr Lorkin—Not really. No-one relies on the transcripts. In the event of a dispute what happens is that everyone says, 'That wasn't what was said.' What was said? You then get 2½ versions out of four people and you negotiate what was said. That is a theoretical difficulty. When I said in answer that I would like to change a few transcripts, it was for what I said on a few transcripts.

Mr CAMERON THOMPSON—A lot of this, such as attacks on power stations, is just vandalism or people who are angry with the system who just want to cause an outrage or to attract attention to themselves or to their cause. They could do that by targeting the courts. That would be just as vicious.

Mr Lorkin—Yes. I am not saying that it will not or could not happen—it could—but courts have not traditionally been targeted, which is interesting.

Senator FERRIS—Other than Family Court judges.

Mr Lorkin—Very interestingly, yes—two major incidents involving Family Court judges that led to a revision of court style—

Senator FERRIS—And security.

Mr Lorkin—Security and court design. So, all of a sudden, instead of courts sitting like this, all on one level, we got back to judges being elevated. Which of those various changes made the difference is anyone's guess. The Family Court is a very emotional area, but it also has to be seen in the context that there have been only two incidents—tragic incidents but only two. In any event, I am not saying that these things cannot happen, Mr Thompson—they clearly can—but I think there are other targets that would be more prone to that sort of attack. I am happy to go back to the Chief Judge of the County Court, who was here last time with regard to the ACC bill, Chief Judge Rozenes, and tell him that these issues were discussed. He is fairly computer literate—much more than I am—and I am sure he will be interested to see how they could play out and to get some feedback in response.

Mr CAMERON THOMPSON—That would be handy.

CHAIR—Thank you very much, Mr Lorkin.

Mr Lorkin—My pleasure.

CHAIR—We appreciate your input once more. It was very professional and very worth while.

Mr Lorkin—On behalf of the bar, many thanks to the committee and to you, Chair, for allowing me to come along.

CHAIR—We are always glad to have you on board.

Mr Lorkin—Thank you.

[2.01 p.m.]

STANLEY, Dr Janet, Acting Research Fellow, Australian Institute of Family Studies: National Child Protection Clearinghouse

CHAIR—Welcome. The parliamentary Joint Committee on the Australian Crime Commission is examining recent trends in practices and methods of cybercrime, with particular reference to child pornography, associated paedophile activity, banking—including credit card fraud and money laundering—and threats to national and critical infrastructure. In its report the committee wishes to provide a picture of the emerging trends in cybercrime and to offer guidance on the role that the newly established Australian Crime Commission might play in combating this crime. We prefer evidence to be given in public but, if at any stage you wish to go in camera, please let us know and the committee will consider your request. I invite you to make an opening statement, and following that we will proceed to questions.

Dr Stanley—I would like to clarify a couple of things that I said in my submission and to give an overview of what my position is. You could call me a specialist researcher in child protection issues.

CHAIR—That is exactly what we want.

Dr Stanley—In Australia we have decided there is a need to protect children from certain behaviours—for instance, children are not allowed to buy cigarettes until they are 18 years of age. In relation to the Internet, I believe children are being exposed to behaviour that has already been considered not appropriate in other media and abusive to children in other circumstances—that is, children being exposed to inappropriate material on the Internet and being subject to sexual exploitation.

Unfortunately, there is so little research on this that we largely do not know its impact on children. We know from research from other areas that child abuse is very damaging to some children. Child sexual abuse especially can cause great problems for children and later on into their adulthood. We know that there is a link between viewing severe violence and severe sexual behaviour and the people who do this. There are problems in other contexts for children viewing such behaviours. For instance, it has been shown to cause in children an increase in violent behaviour, disturbances and a desensitisation to violence—those sorts of problems. Some research has shown links between exposure to pornography and subsequent sexual assaults. We know this.

I believe the greatest adverse impact of these events occurs in a group of children who are particularly vulnerable. This is a group that some research is suggesting is being targeted for sexual exploitation, is being used in the production of child pornography, is more likely to access unacceptable material on the Internet, and is least likely to know how to deal with it appropriately. These children are vulnerable because they have already been abused, they have some problems with their peers, they have some attachment problems at home, they are depressed or they are vulnerable through other circumstances. In my view, the solution is to have a scattered approach—attack it from all sides where you can.

Research is my area. We really need to know the facts about the impacts these events are having on children and how we can address the impacts. We do not know that at the moment. I think the Internet industry should be more accountable within this area. I think we should attack it from the policing side, put in more resources and enable the police to do more in this area. I think there should be more emphasis on a public awareness campaign. I do not think a lot of parents know the extent of problems that the Internet can provide for some of their children. That is what I wanted to say.

CHAIR—In your submission you said that self-regulation is not working and that we really need the government to establish some standards. Part of our committee's work is to look at the area, to see the extent of the problem and also to make recommendations where they are appropriate. Firstly, could you outline what you think we should be doing in this area. Obviously the parents can buy the equipment, in terms of their own computers, which can prevent their children from having access to pornographic sites, but it is not easy. Would you like to outline what recommendations you would like to see?

Dr Stanley—In relation to the filters and things that you just mentioned, a recent finding that I have seen reported that up to 50 per cent of material is not effectively being blocked by the filtering process. Net Nanny is the software that is recommended and, off the top of my head, I think that up to 50 per cent of the content is allowed through, so it is not very effective. The report also said that only about one per cent of people with computers actually purchase this filter stuff anyway, so it is not widely used. People do not avail themselves of the software. One way might be to put the research into the technology to try and make these filters more successful. Also, a public awareness campaign might encourage people to use them broadly, not only in the home, libraries and schools but right across the board where children get access to computers.

The Internet industry is a self-regulatory body with codes of conduct. My understanding is that the legislation allows something to be self-regulatory where there is not a serious concern about public interest. It is my belief that the Internet industry does not come under this category because there is a serious public interest in the welfare of children who are exposed to this material. To me, self-regulation does not seem to be working. Internet service providers do pass on this material to the home computer and, in my view, there should be a system of accreditation—whatever you like: taxation, some licensing—so that Internet service providers reach certain standards of behaviour and they have some sort of inspectorate. That sort of system would allow some sort of inspectorate, some sort of regulation and some sort of guidance to be funded, and it would allow codes to be set up, with some sort of requirement that there is not just wholesale passing on of any material through them—that there is some sort of regulation and monitoring of what material they pass on to their end point computer users.

CHAIR—With your research into what happens in various countries overseas, have you seen anything which is attractive and which we should emulate?

Dr Stanley—No, I have not. My interpretation is that unfortunately the Internet has caught us pretty well unawares. It is an explosion of technology and we are really playing catch-up worldwide on how to address the associated issues. European commissions and committees are being established to look at them and make recommendations, hotlines exist where offensive

sites can be reported and a network of international policing authority is being established. But at the moment all of these are just starting to take off.

Senator FERRIS—For some time now the ABA has been running a take-down action. Julian McGauran was a member of a committee that set up the opportunity for the Australian Broadcasting Authority to take down dirty sites within something like 24 hours, but arguments in total opposition to your position were put very forcefully during that hearing on the basis that the speed of the Net and the flow of information would be interfered with. The whole regulatory argument was run very forcefully by the Internet association and the librarians association; they oppose putting any kind of filtering mechanism on any computers in public libraries. I do not disagree with your position at all; I just find it fascinating that philosophically, in that regulatory sense, it is opposed very forcefully by the industry.

Dr Stanley—Yes. I understand why the industry might oppose it—because most industries do not want compulsory regulation. I recognise that the ABA is doing work in this area. I cannot remember the exact figure, but fewer than 1,000 actionable sites have been addressed. It is estimated that there are 14 million offensive sites on the Internet. The scale of the problem is just so big. I agree that it is important to do this and to continue it, and it is very important to expand it. But the scale of the problem is just so huge. Part of the problem is that many of the sites come from overseas and you cannot tell an overseas entity to pull its site; you have to do that through the police. You report it to the police and they then do it through their international connections. So it is a little bit removed and it is very difficult to do it.

Senator McGAURAN—Your submission is very lengthy and very good. In it you mention that the Federal Police child sexual unit has been closed down. Do you know why that was done? Was it because of individual state laws, bodies or jurisdictions?

Dr Stanley—I think it might have been started up again now.

CHAIR—Was that a Victorian Police unit?

Dr Stanley—No, I think it was a federal unit. That part of my research was published in 2001. I think the unit has subsequently been reopened but, I am sorry, I am a bit unsure about it.

Mr KERR—I think they have re-established it.

Senator McGAURAN—You also mention that the penalties for child pornography offenders—not for children's access to pornography—are not high enough: $60,000 or two years in jail. What is an appropriate penalty? I know there are degrees and degrees, but what would you consider to be an appropriate maximum?

Dr Stanley—I also believe that has been changed. Recent Victorian legislation has now increased it to 10 years. I am not in a position to judge this; I think it is law and criminology. All around the world it is changing and the jail terms are being extended. Recently, after about three years of international work, the Wonderland Club, a child-abusive Internet activity, was broken. At that stage one major offender in Britain was given a community service order. All countries are now upping the severity of the punishment for these offences. But again it is all catch-up; we are not taking the action before it happens, in a way.

Mr KERR—But aren't we really rolling up together two very distinct issues? One is people who film sexual activities with children and promote such films to their members—people who in jail are called 'rock spiders' and what have you. These folk generally encrypt their material, they operate as clandestinely as possible and they code their communications with each other. Broadly, law enforcement all across the system, whether it is efficient or inefficient, is trying its best to find these people and, if they are found, they are brought to court and increasingly dealt with pretty severely. That is one aspect and, in a way, it is a traditional law enforcement issue.

Dr Stanley—Yes.

Mr KERR—The other issue you have raised—and I think it is quite different—is that, essentially, the generation of material that our community says adults are entitled to see is not otherwise seen to be inappropriate; it might be confrontationist and many people would not wish to see it, but broadly we have made a social decision that adults can choose to see it. Such material comes from both within and outside of Australia and, yes, the receiving mechanism is one which is not like taking a kid to a cinema; it is one where most parents let their children use the computer. It is more like a radio station where you have basically unlimited broadcasters. So we have two very distinct issues and one, I think, is incapable of solution. Unless you pull down the Internet, you will have the second problem. The whole nature of the Internet creates that second problem, although it creates a lot of other benefits as well.

I understand why some parents want a filter, but all filters are hugely inefficient. They often take everything out. The English language is so imprecise. The word bottom, for example, could be a bottom going up and down as opposed to the bottom of a well. A filter can take everything out and leave you with nothing, and with Net Nanny filters the problem is that they cannot take everything out. In the end, although you say it should be institutional and systematic by its control, isn't it true that we cannot do that and therefore, in a sense, what we really have to do is harden parents and schools and be very effective in our communication? Every time your child switches on their computer and works away and you are absent, they can see material that you would not allow them to see in a cinema.

Dr Stanley—In my view multiple things can be done. Making the community much more aware of the dangers of what children can access on the Internet I think is very important—education programs for both children and parents. From research that has been done, a lot of parents simply are not aware of what their children are seeing on the Internet. In many cases children do not tell their parents that they have seen offensive stuff that has upset them; parents find out because their child has a nightmare or whatever.

There are barriers to communication at the moment. The community does not understand the extent of offensive material on the Net that their children might be seeing. There is a generation gap. A lot of adults are not computer literate. I agree that there is a lot more on the education side that we should be doing. In my view there is also a strong argument for a lot more resources to go to the police. It is like catch-up with the technology at the moment to allow them to understand, to keep up with, and to get ahead of, the technology—it is illegal activity on the Internet—to fight this illegal activity.

Mr KERR—Can I separate two things out. I have no problem with throwing the weight of the law against people who are filming sexual abuse of kids and consuming it as a product. I do not

think that gets on the Net in public display very often; occasionally it escapes. But most of this is consumed by fetishists who do not want it to be known that they are there; they hide it away. The sort of stuff, though, that you are talking about is the porn industry, I suppose. I am not being crude about it. In its many manifestations both here and overseas, some people offer a pay per view and put up pages for advertising and others are sorts of home offerings. In that area there is nothing the police can do, even if they knew about it.

Dr Stanley—I am not only saying that it should involve the police. There should be lots of ways in which we can take preventative measures against this.

CHAIR—Duncan has pointed out an important distinction for our inquiry. Our bottom line is to look at the problem and come up with a recommendation. There are these two distinct areas, which he rightly talks about. One is the filming of children for pornographic reasons, which is then consumed not by children per se—it can be, I presume—but in the main by paedophiles. The other one is access to the computer and the pornographic sites—which we have decided is legitimate for adults to access. The problem is that you cannot restrict children's access without also impacting on adults' access. Then it becomes a question of how does government get into that regulation, in what ways can it do that? The bottom line is that it is more a parental responsibility. This is somewhat of a dilemma that I am raising publicly.

Mr SERCOMBE—The third area is the chat room situation where predators can prey on children but which in itself is not pornographic.

Senator FERRIS—Cybersex.

Mr KERR—A very good example is the 12-year-old girl who met a man on a chat room. She was complicit. She described herself as a 19-year-old college girl in her communication back to him, as I understand it.

Mr CAMERON THOMPSON—That is the source of some dispute.

Mr KERR—That is what the news said.

Mr CAMERON THOMPSON—He claimed that, but it is being disputed. They say that he did know she was only 12.

Mr KERR—I do not know. The point is about the chat room.

Mr SERCOMBE—I understand the sort of thing we are trying to get some response on is that the one size does not necessarily fit all in terms of how you respond to it. It is not a uniform phenomenon; there are a variety of components and, therefore, one policy approach does not necessarily suit all situations.

Dr Stanley—I agree with that. The only way you can attack it is by addressing it in multiple ways and on multiple fronts. I would argue that it is not solely a parental responsibility; I think it is society's responsibility to protect children. When I first addressed the committee, I made the point that the group that concerns me greatly is that vulnerable group of children who appear to be targeted for sexual exploitation. It is these children who seem to be targeted for child

pornography and it is these children who seem to be accessing the unsuitable material. In those cases, in many situations there might not be a parent who is responsible for the protection of those children.

CHAIR—How do we stop their access but allow adults who want to access that?

Dr Stanley—In my view, you have to decide whether our society is about protecting children or allowing completely unfettered freedom to adults. We have to make that decision. I know what I would decide.

CHAIR—Don't you think we could have both?

Dr Stanley—No, I do not believe you can have both.

Mr SERCOMBE—Dr Stanley, could you be more specific about what you are saying to us about vulnerable children being targeted? Are you saying that these are children in a chat room situation that are being targeted by paedophiles?

Dr Stanley—Yes.

Mr SERCOMBE—Or are you talking more generically about targeting by promoting pornographic material to them? What, in specific terms, are you saying to us?

Dr Stanley—I am saying both of those things. There is almost no research, but there are some suggestions that these children are particularly vulnerable to being targeted for sexual exploitation. They are children who are needy children. They might have a lack of affection at home or might not have a suitable adult model. Perhaps they are depressed, or perhaps they do not get on with their peers too well and they sit on the Internet and establish friendships through a chat room. They are particularly vulnerable because a paedophile has watched the child and assessed their vulnerabilities and knows how to target that particular child, to feed into their needs and offer what they need. They deceive the child.

Mr SERCOMBE—Are you talking on the basis of empirical knowledge? You say there is not a lot of research on it. Are you talking on the basis of research, or is it a subjective view about what happens?

Dr Stanley—There is very limited research. Some evidence suggests that this is what is happening—that these are the children targeted. There is almost no Australian research, but there is a little American research on which I am basing a good bit of this.

Mr KERR—My problem is this. Let us go away from the computer. Let us assume that some parents are indifferent about the welfare of their kids and they buy, say, several X-rated and violent videos—which I think are much worse—and some of the R-rated stuff and they watch these videos with their kids, or they leave them around where the kids can watch them, or they go out and leave the kids unsupervised or mum is working in the sex industry and she brings home clients and has sex in front of the children. None of those things is criminal. All of them are ill-advised, if you are trying to bring up children in a rich and loving environment. The analogy is that this is something that comes in because the adults are lawfully entitled to see it,

and they regard it as their right. If some adults are irresponsible, they would act irresponsibly in a whole range of areas. I am trying to see the difference here. If I thought there were some way you could have a coding system where material is G-rated or what have you, I would accept that but, because this material comes from so many different places, it is almost infinite in its generation. Because there is no framework that I have ever heard of that realistically does this, in the end it comes down to mum and dad or—if there are not two of them—mum, dad or whoever is caring for the kids being either irresponsible and leaving the videos around or doing the bad things, such as letting the kids have access to computers without giving them any guidance about their use or any care about what they seek.

Dr Stanley—Just because a child is exposed in one area, we do not throw up our hands and say, 'Oh, it doesn't matter if you're exposed in another area.' Society has a responsibility to try to protect children. In other areas of child protection, where that parent is unwilling or unable to protect a child, we as a society step in and say we have a responsibility to protect the children.

Mr KERR—We do not if they are just doing things that I described to you. We do not. I do not like it, but—

Senator DENMAN—I just want to make a point on what Duncan was saying. I was teaching before I went into the Senate. About 15 years ago I taught grade 4—they would have been about 10-year-olds. A child got up one morning to tell what she had done over the weekend. What she had done—and she did not know that everyone else in the class probably did not have a clue about what she was talking about—was sit with her parents and watch pornographic videos. She was telling the class about this until I stopped her. It is happening. Because she was being shown these videos by her parents and with her parents, she did not have a clue that it was not a good idea for her to be seeing them. That must be happening on the Net as well.

Dr Stanley—It is worse than that because, although some children may be seeing it with their parents' knowledge, what is happening is that the parents are not realising the extent to which children are accessing the Internet in multiple ways.

Senator DENMAN—So they are using it as a babysitter?

Dr Stanley—Yes, it could be a babysitter, but children use the Internet far more frequently than adults.

Mr CAMERON THOMPSON—If you are a parent who buys an X-rated video, presumably the title says, 'X-rated video'—it has some pornographic title or whatever—whereas on the Internet you can type in just about anything, such as green trees, lovely views or something or other, and when you feed that into a search you actually wind up with pornographic sites.

Dr Stanley—Yes, you may.

Mr CAMERON THOMPSON—Is that particular differentiation a concern?

Dr Stanley—Yes, it is. Very recent research that came out this year shows that something like 85 per cent of boys have unwillingly accessed material that upset them and something like 60 per cent of girls have unwillingly accessed material from the Internet that they found disturbing.

Mr CAMERON THOMPSON—Where did that research come from?

Dr Stanley—Hamilton is the person who I got the information from. Flood and Hamilton—

Mr CAMERON THOMPSON—From the Australian Institute of Family Studies?

Dr Stanley—No, the Australian Institute in Canberra. The title is *Regulating youth access to pornography: discussion paper number 53*.

Mr CAMERON THOMPSON—I was interested in your discussion of ISPs and your proposal to do something about regulating ISPs. I wonder if you would have any comments about various elements in relation to ISPs. You seem to be concerned about the pornographic material that they then pass on to the users, and regulating that, but ISPs also have the capacity to watch what each of their participants are watching. Is that an area of concern? There is also a potential, I would think, for an ISP to manipulate what people within an area might watch or be able to regularly access. They also have the ability to, I suppose, look at the nature of the material that is flowing through—a proportion of which is pornographic or otherwise. Do you have any wider comments, apart from just looking at the issue of the material that they pass on and regulating that? Are there any wider implications? For example, I would think that, if an ISP operator had criminal intent—watching what all their people were watching and perhaps blackmailing them about what they were watching—that is something that they might do.

Dr Stanley—That would be another argument for some sort of regulation that is not entirely voluntary over the ISP providers. If you have a licensing system—accreditation—then presumably you would be able to cover all sorts of areas, including the problems that you have raised.

Mr SERCOMBE—Regulating ISP is not going to address of problem of predatory behaviour in a chat room, is it?

Dr Stanley—No. That is why I say you have to have lots of approaches with different fronts.

CHAIR—This is the first day of our inquiries, so we are thinking aloud to a certain extent. There is no doubt that we all agree with your basic premise that sexual abuse amongst minors leads to all types of problems later. We all accept that. The problem that I have is where you go in terms of trying to change it. I can understand the need for some control mechanisms with the chat rooms—but how we do that, I am not sure. We have talked to the Australian Federal Police about that.

As Duncan Kerr has said about the child pornography sites and closing them down, I too am not sure how you can limit the ability of young people to access the broader pornographic sites without closing them altogether. Is that what you are recommending? I can understand that some people would argue that way, but I am not quite sure how you could stop the access. If people do not purchase the Net Nanny or if parents do not ensure that it is followed, it seems to me the only way that you could logically stop access is by closing down all of those sites. In the broader community that of course would cause a reaction. Whether that is appropriate or not, we are not here to make that judgement. Do you have any comments on that? That issue is a difficulty for our inquiry.

Dr Stanley—I understand that it is difficult. All those questions are difficult. There is no easy answer. In my view it is not a matter of 'this one is good and that one is bad'. There is a continuum of pornography. Child pornography is illegal; adult pornography is not illegal. But there is a continuum from mild to very severe pornography. There are sites on the Internet that show nonconsensual sex—rape. There are sites that show death. There are sites that show how you can commit suicide—'let's do it together, let's do it now'. I think the extreme end should be taken off the Internet. I do not want my children watching extremely violent sex—rape. I do not want my children to see that. There is a continuum. They need to go.

Mr KERR—I can take my digital camera—and I do this—and send photos to my brother and others. But let us assume that I am going to do something more malign. I can take some digital photos, create a web page using one of the very simple web tools and, using one of the listening devices that you can buy for $5, send an email to half a million people with an invitation to subscribe. I can do that routinely. I cannot imagine how an ISP provider could look at every email and their attachments on them that go through to see whether it is a photo of my house in progress—which is what I am doing at the moment—or something that is a bit gross.

I do not know how many millions and billions of these things are being sent all the time. I now get friends emailing me with photos, weddings and God knows what else; it is just going through in such volume. I honestly think that unless you are going to shut the Internet down you are going to have to live with parents providing guidance to their children and with a law enforcement focusing on the things that are absolutely illegal and chasing the really bad guys.

Dr Stanley—Because you cannot address every aspect of it very easily does not mean you cannot try to address areas where you can. Maybe we need to put a lot more resources into the police for them to understand and keep up with the technical processes. The Free-Net is coming, so we will probably not even be going through ISPs in the future. At the moment, my understanding is that there are not the resources for them to get the technological knowledge to keep up with the people who are offending in this area. And, yes, we do need more community education—I agree.

CHAIR—You have raised a lot of questions for us and I am not sure we have come to any resolution today. If you have anything further that you would like to add, drop us a note, which we can circulate to the committee, or, alternatively, talk to Maureen, our secretary. That would be useful, especially in terms of the dimensions of the problems of the three separate categories that we have been talking about and how we address them without alienating some segments of the community.

Dr Stanley—I think you are going to have to alienate some sectors of the community.

CHAIR—I understand that, but that is the dilemma.

Senator McGAURAN—I just want to ask one question. I am not sure if it was covered in the cut and thrust of what we were just saying, but this is just for my information. You mentioned the high-profile catch from the Wonderland Club—and, by the way, there was an Australian branch here—but there have been some other high-profile catches, such as a couple of old rockers of whom some of you might have bought records.

Mr KERR—They were doing research, I understand.

Senator McGAURAN—Do you know how they particularly were caught? Have we made any such catches in Australia? I do not know of any. I do not necessarily mean high-profile people, but catching them downloading. How do you catch a downloader?

Dr Stanley—I think you would have to ask the police that. For instance, with the Wonderland Club it took three years and I think 30 countries were involved. There was a huge amount of cooperation between the international police forces.

Mr KERR—His name was on the electronic list that they found when they cracked one of the senders. He had accessed the site and paid a fee, so his name was on a list. That is how they followed it up, by working backwards.

Senator McGAURAN—They were working backwards. It is not as though they are sitting at the computer and waiting for a downloader.

Dr Stanley—In respect of international legislation, we do not have international courts. Where do you prosecute these people? All this needs to be resolved with the resources to be able to understand it.

CHAIR—Thanks very much. We really appreciate your input.

Dr Stanley—Thank you for the opportunity to come and address you.

CHAIR—No, thank you. We applaud what you are doing and now we have to work out how we address it.

Proceedings suspended from 2.43 p.m. to 2.53 p.m.

GRANT, Detective Acting Superintendent Richard, Acting Manager, Organised Crime Investigation Division, Victoria Police

MASTERS, Detective Superintendent Philip, Major Fraud Investigation Division, Victoria Police

O'CONNOR, Detective Acting Inspector Christopher John, Sexual Crimes Squad, Victoria Police

WHEELER, Detective Senior Sergeant Peter Francis, Officer in Charge, Computer Crime Squad, Victoria Police

CHAIR—Before we welcome the next witnesses, two outstanding issues need to be addressed.

Motion (by **Mr Cameron Thompson**) agreed to:

That the committee now take evidence from four instead of two representatives of the Victoria Police.

CHAIR—A request has been made by a journalist from the *Australian* to make an independent tape recording of proceedings. There being no objection, permission is granted to do so.

I welcome the present witnesses. It is great to have all of you here and we appreciate your input. I understand that you may wish to go in camera today. Please let us know when you wish to do so. Obviously, at that stage the representative from the *Australian* would need to leave the room. For now we will proceed in public. To start us off and set the mood, please speak first to your submission. We will then move to questions.

Det. Supt Masters—The verbal submission I am about to make can go into the public *Hansard*. Thank you for the invitation and opportunity to address the committee. I offer the apologies of the Assistant Commissioner of Crime, Simon Overland, who unfortunately was unable to attend on this occasion. First, I will introduce myself and the other members of my team, who are available for any questions relevant to this inquiry. I am the divisional head of the Major Fraud Investigation Division of the Victoria Police Crime Department. I have had 27 years of policing experience; predominantly that has been in the criminal investigation arena. My portfolio is the operational management of the six squads that make up my division. These squads include the Initial Action Squad, three major fraud investigation squads, the Asset Recovery Squad and the Computer Crime Squad. The Major Fraud Investigation Division is a multidiscipline group consisting of accountants, solicitors, administrative staff and detectives. In total I have 135 personnel within my division.

The Victoria Police Major Fraud Investigation Division is the largest fraud group in Australia. On my right is Detective Acting Superintendent Richard Grant, who is currently Acting Divisional Manager of the Organised Crime Investigation Division. He was formerly the detective inspector in charge of both the Asset Recovery Squad and the Computer Crime Squad.

He has in excess of 25 years of policing experience, which again is predominantly within the operational and criminal investigative areas or arenas. Detective Acting Superintendent Grant is also the current Victoria Police Liaison Officer to the Australian Crime Commission.

Detective Senior Sergeant Chris O'Connor on my left is currently attached to the Sexual Crime Squad and has a wealth of experience in the investigation of sexual abuse of children, paedophilia, child pornography and sex related crimes generally. He has over 25 years policing experience, and within Australian law enforcement circles he is one of the foremost investigators of child exploitation.

On my far left is Detective Senior Sergeant Peter Wheeler. He is currently the squad manager of the Computer Crime Squad and he has extensive knowledge of computer crime and its impact upon law enforcement. Like our other team members, Detective Senior Sergeant Wheeler has over 25 years of policing experience in various operational and investigative roles. Currently he is the Chair of the Australasian Computer Crime Managers Group.

Victoria Police has provided a written response to the committee that gives an important overview of the existing trends in cybercrime. The attachments contained within our submission were prepared by the Computer Crime Squad. However, I thought it important to ensure that the committee have the opportunity to ask questions of the experts in their respective fields; hence the attendance of my team today. This I hope will allow the expansion of the discussion to include issues surrounding child pornography and associated paedophile activity, banking and credit card fraud and threats to the national infrastructure, which are key factors of the committee's terms of reference.

Cybercrime has many manifestations and is of serious concern to all law enforcement agencies throughout the world. In support of the Victoria Police submission I will expand briefly upon those areas of concern. In relation to child pornography and associated paedophile activity, child molesters use Internet technology as a tool in the same manner as most other criminals. The essence of online child sexual assault criminality is related to the offender and the offence dynamics, not the technologies utilised. As a class of criminals, child molesters are the most computer literate and they actively network one another globally. Millions of child pornography images and movies are available on the Internet via news groups, peer-to-peer sites, chat channels, e-groups, email, web sites and bulletin boards. A number of commercial, organised rings have been identified and those sites have turned over many hundreds of thousands of dollars. There is a high commercial demand for this material. Online child sexual assault is a classic transnational crime, and there is a clear nexus between viewing child pornography and committing child sexual assault offences.

With fraud related to banking, including credit card fraud and money laundering, law enforcement has seen an exponential growth in credit card fraud through card cloning and skimming, mirroring trends overseas. Identity related crimes are evident in most fraud related offences, including loan applications, credit card fraud and online banking. This is demonstrated in the statistical data provided with our submission. Identity related crimes are currently one of law enforcement's greatest problems globally, but significant efforts to combat this criminal methodology are being made in a number of fora nationally. The Victorian state government has recently enacted legislation that greatly assists the Victorian Police to address a number of computer related offences, and this closely mirrors the Commonwealth's Cybercrime Act 2002.

I turn to incidents from Victoria's perspective involving the national critical infrastructure. Earlier this year the Victoria Police Tactical Response Squad sought the assistance of the Computer Crime Squad in the investigation of a Melbourne man who had forwarded threatening emails against Melbourne Water to the National Terrorist Hotline. This man made a series of threats that he would remotely detonate drums of cyanide submerged in water reservoirs. The offender was apprehended and has been charged with a number of serious offences.

Law enforcement nationally has made significant inroads in identifying cybercrime as a key policing priority and has undertaken a number of strategies to combat it. The recent establishment of the Australian Hi-tech Crime Centre within the Australian Federal Police will provide a coordinated and national approach to such threats. Further, it will ensure the timely dissemination of intelligence and investigation of incidents involving cybercrime in conjunction with its state counterparts. Also, jurisdictions have supported the establishment of this centre by ensuring that it is appropriately resourced and viable. The future looks bright and the commitment is intense.

In conclusion, rapid technological advances through faster connectivity and the global reach of the Internet make fertile ground for opportunistic criminals to commit old offences in new ways. It is important for law enforcement agencies nationally to continue to undertake a unified approach through coordination, investigation and intelligence on cybercrime. The members of the Victoria Police delegation are happy to answer any questions or explain any issues that may assist the committee in its inquiry.

CHAIR—Thank you for that very useful and comprehensive review. Before handing over to my deputy, who is a man experienced in the policing area, I direct your attention to your submission. You talk about some initiatives that Interpol has been taking in this area. We are particularly keen to learn about your knowledge of what other countries and Interpol may be doing. From discussion with our last witnesses, we are concerned with the different areas of paedophilia. There are the paedophilia sites, which you have outlined; the question of access of children to pornographic sites; and the chat rooms that are used by paedophiles. There are problems as to how we should address some of these areas. What initiatives have you seen that you think may be of interest to the committee?

Det. Supt Masters—Chris and Peter have had connections with Interpol; in the past they have attended a number of Interpol forums. But perhaps Chris could address you specifically on the paedophile side.

Det. Insp. O'Connor—In 1997 and 1998 I attended a number of meetings of law enforcement agencies overseas. At that time Victoria Police was perhaps the pre-eminent law enforcement agency in the world in the area of child sexual assault investigation via online services.

CHAIR—Does that imply that they are not now?

Det. Insp. O'Connor—I am leading up to that. A lot of water has passed under the bridge, particularly with the work that the European Union has performed in northern Europe, which has homogenised a lot of the efforts over there. From Australia's perspective—and specifically from my perspective in Victoria—coming from a time when our liaison and our expertise were

world's best practice, the main European countries' law enforcement agencies and certainly the United States have now raised the ante quite a lot. We are still performing as well as most, but we do not have the liaison perhaps that we had in those days. So the flow of intelligence now is not as strong as it was perhaps five or six years ago.

CHAIR—Is it five years since you have been with Interpol?

Det. Insp. O'Connor—My last time was in 1998, although I obviously keep in close contact with what is happening with my overseas colleagues. Perhaps the area where we have been superseded to some degree by those overseas is the ability, particularly in Europe, of law enforcement agencies to cooperate. Most large-scale paedophile rings operating on the Internet are investigated now by multijurisdictional teams.

CHAIR—When such an operation is occurring, are you advised of it here so that you can check to see whether those suspects have infiltrated here also?

Det. Insp. O'Connor—Generally at the end of the line. We are advised once all the intelligence is gathered in relation to the suspects and the activities. Obviously if there are Australians identified, then Australian law enforcement is advised. We are advised generally of most of the operations that are conducted.

Det. Supt Masters—I wonder whether at this point we could invoke the in camera provisions because certainly some things could be explored further in that forum.

CHAIR—Certainly.

Evidence was then taken in camera, but later resumed in public—

[4.05 p.m.]

BOND, Mr Graeme, (Private capacity)

CHAIR—I call the committee to order. We resume this public meeting of the parliamentary Joint Standing Committee on the Australian Crime Commission. Thank you very much for coming, Mr Bond. As you know, you can go in camera if you wish at some stage. If confidential information will be discussed or if individuals are brought into it, we should perhaps go in camera, but we will discuss that as we go along. A reporter from the *Australian*, who is outside, may come in. I am just letting you know that. We heard a little of your story. Please press on and tell us what happened.

Mr Bond—Have you read my submission?

CHAIR—Yes, it has been distributed around.

Mr Bond—If you have all read the submission, I really do not have anything specific to add. However, I would like to emphasise that the weakness I see is that banks have a tension between their marketing message to merchants and the legal message. The marketing message is that this is a safe, secure way of accepting payment, and the legal message is, if anything goes wrong, 'Sorry, Mr Merchant, you're liable.' I remember most vividly the marketing message that was expressed to me by a bank employee when our EFTPOS machine was installed. It was that this was a safe, secure way of accepting payment for goods, and it was much safer than a cheque because it could not bounce and cleared funds would be in our account the next day. When we became the target of an organised crime gang operating a credit card scam, we discovered that the true situation was that we had accepted a means of payment that was similar to accepting a cheque, with a clearance time of six months, because that is the period in which the bank can take money back out of your account.

The bank's marketing message to merchants is also that all you have to do to avoid chargebacks is follow their procedures—get proper authorisation for transactions according to the procedures provided by the bank and you will avoid chargebacks. I can provide the committee with a sample of the marketing material that the banks pass on to merchants that states this. The published message is reinforced by verbal messages from bank staff.

When I was initially signed up as a merchant, I looked at the merchant agreement and I queried a section that spoke about chargebacks in the event of a dispute between a cardholder and a merchant. The verbal assurance I got from the bank was, 'You don't have to worry about that. That is merely to protect the bank from dishonest merchants who would attempt to defraud the bank.' It has never been seriously alleged by the bank, nor could they seriously allege, that we participated in a fraud. We were simply the victims. The true situation, in my view, is that we were targeted by two crime syndicates—one being the organised crime syndicate recognised by the police and the other being the bank, which served as a facilitating mechanism to extract the money from us. That is the true position, no matter what the banks might say.

The Reserve Bank of Australia and the ACCC published a report a couple of years ago in which they spoke about a payment guarantee for credit card transactions. That payment guarantee was used to justify the high charges that the banks levy on credit card transactions. The report went on to indicate that there was a difference with card-not-present transactions—telephone and mail order transactions. My merchant agreements made no such distinction whatsoever, and nor do the majority of merchant agreements, I believe. So we have, on the one hand, organisations like the Reserve Bank and the ACCC putting in their report—and merchants believing—that once a credit card transaction is approved the bank has approved the transaction and accepts responsibility for the payment. On the other hand, the banks maintain that that is not the position if anything goes wrong—and they resort to the law. We were coerced into a settlement with the bank, where we had to pay them for the value of the transactions that were fraudulent.

CHAIR—Are you able to tell us how much that was worth?

Mr Bond—Yes. It came to a total of approximately $141,000, but my total losses would have greatly exceeded that as I incurred considerable legal expense, and also it brought about the collapse of my business. It also brought about the collapse of my wife's health, and that has entailed considerable hardship.

CHAIR—In terms of the role of the committee, which is looking at cybercrime and fraud in several areas, including banking and credit cards—which is right in the area that you are concerned with—how would you avoid the situation that happened to you? What recommendations would you be making?

Mr Bond—I made recommendations in my submission. The way I see it, the banks and credit card companies control the system. Card merchants do not. The security of the system relies solely on the banks and the credit card companies that operate it—Visa, MasterCard and the like. There is very little that merchants can do. For example, merchants are obliged in their merchant agreements to take payment by credit card in circumstances where they would accept payment by any other means. So the merchant is in the invidious situation of being obliged to accept payment by credit card from someone he would accept cash from, but he may not be entirely comfortable accepting payment by credit card.

There was evidence given in a county court case in Melbourne in 1998 by a former bank investigator, Mr Graham Burgoyne, that banks had been negligent and had repeatedly failed to implement security measures that they were advised to implement by overseas authorities. Mr Burgoyne put me in touch with other former bank investigators, and they confirmed what he had to say. The story was essentially that the banks receive advice from overseas about scams that are known to be operating and countermeasures that can be introduced. The banks consistently look at these countermeasures and say, 'No: if we implement that it will cost us money; if we do nothing it may never happen. If we do nothing and it does happen, there is no problem; we can simply shift the risk on to the merchant.' That is, in fact, what they rely upon. That is what they do; that is what they get away with.

I approached the ACCC—or initially my solicitor did—believing that the ACCC was the appropriate authority to take action, because we had a situation where banks were using their market power to coerce small merchants into coughing up when these scams occurred, due to the

banks' lax security. I could not interest the ACCC in this. The ACCC told me, incredibly, that I was the only person this had ever happened to who had complained to them. I do not believe it. We have Mr Fogg in the room here today. He is another victim of a credit card scam that was of a similar nature but was perpetrated more recently. He is in a different industry, and we know of about a dozen people in that industry in Melbourne who were similarly targeted. It is quite widespread. The ACCC seems to me to be the appropriate authority to do something about it by putting pressure on the banks to clean up their act, clean up their security and introduce proper measures to prevent these things from happening.

I suggest a couple of things that they could do. For instance, had I been a merchant in the US at the time of this credit card fraud, I would have been able to take advantage of the address verification service. I would have been able to ring up my bank and say, 'I have an order for some goods. Payment is by this credit card,' quote the credit card number, say, 'The delivery address of the goods is,' quote the address and say, 'Can you confirm that that is the address to which statements go for that credit card?' That could have been done in Australia, but it was not done.

There was a second measure: the card verification code. If you look at the back of your own credit card, on the signature panel you will see the number that is embossed on the front of your card and an extra three digits. That is the card verification code. That can only be seen by someone who has got the card, because it is not embossed on the card and it is not imprinted by imprinters. It does not appear anywhere. That is an additional security measure that is only now coming into effect in Australia. Some utilities are, I believe, asking for it when payment is made by credit card. It has been available overseas and it has been actually printed on cards here for quite a number of years now. The banks are simply not interested. They can get away with this absolute scam of passing on all the risk to the merchants.

Senator FERRIS—Can I ask you how you came to get involved in this scam? Did somebody come in with a stolen credit card or was it a telephone order? How did it come about? Did you have any suspicions at the time? Was it a person known to you? Can you just give us a little bit more information on how your actual case study evolved?

Mr Bond—Certainly. It commenced with a phone call one morning. A gentleman on the phone wanted to buy a computer product and he haggled about price, as people are inclined to do. Finally he said, 'Can you do better if I buy two?' I said, 'Okay.' So we went through that sort of cycle of haggling over the price, and finally we agreed. He said, 'Very well. I will fax you an order.' Then he said, 'I want the goods delivered overseas.'

CHAIR—What kind of goods were they?

Mr Bond—Computers. In the first instance it was two laser printers. Later on we moved on to other products such as RAM and hard disks. This seemed quite unusual, but I had been in the situation myself of importing goods from the US and paying by credit card and it was really just the reverse of that situation. Whilst unusual, it was not necessarily anything fraudulent. I asked him a series of further questions, such as why he would want to buy from Australia. He had the answer that they were actually cheaper here than in the UK, even after you allowed for the freight, because they were manufactured in this region of the world. I said, 'Why not the US? I am sure they would be even cheaper there.' He said, 'You're right. However, they use the wrong

voltage over there.' That was correct again. He was very well prepared, he knew his story, he was well rehearsed and he had an answer to everything. We still felt that this was a little unusual. So instead of shipping the goods that day I showed my voucher—printed by the EFTPOS machine—to the lending manager at my branch of the bank, who did not express any concern about it. We waited until we verified the next morning that the funds were in our account before we shipped the goods. We took what we considered to be all reasonable precautions and did everything that we could think of that was feasible.

Several days after we had shipped those goods, we got another phone call. The customer was delighted with our service and wanted to buy some more things. A series of such orders was placed, and they increased in value as they went along. On at least one other occasion I similarly discussed the transactions with the lending manager at my local branch of the bank, and again there was nothing said about it. At the time, this scam had been going for a couple of months. The bank knew about it. If they had wanted to, they could have put out an alert that the computer industry was being targeted and they could have monitored merchants' accounts. There were any number of things they could have done, but again they did not do a thing. They let it all happen.

Senator FERRIS—You never actually saw the customer?

Mr Bond—No. The same gang targeted other computer companies in Melbourne and elsewhere in Australia. In fact one member of the gang was arrested at Mulgrave by the Victoria Police when he aroused suspicions. I understand from the Victoria Police that this gentleman, who was a low-level player in the operation, had in his possession details of over 300 credit cards. The Victoria Police could not establish the identity of this person, even after about half a dozen tries, and ended up charging him under the first name that he gave. I believe he was jailed for a period and subsequently deported.

Senator FERRIS—When you started shipping these goods, were they always to the same address?

Mr Bond—No. I think there was more than one address. There were two addresses, I think. After I dealt with this first gentleman for a while, he said he wanted to introduce me to a friend who was in the same line of business and who also wanted goods. I think there were actually two addresses involved for two different companies.

Senator FERRIS—You were not able to have the goods seized at the delivery points?

Mr Bond—In the case of the final shipment, when we were advised by the freight company—it was actually the state manager of DHL who advised us that he suspected that there was a problem—I did not know what to do. I said to him that I was not sure what my legal rights were here. I had got money in the bank, I had been paid for the goods, I did not even know if I had still got title to the goods. So I said, 'Can you stall the goods as long as you can, and I will get back to you.' I immediately rang Cardlink Services, who operate the credit card facilities on behalf of most of the banks—all except Westpac, I think. The response from the person I spoke to at Cardlink Services was 'No. Everything sounds okay, but we will do some further checking and get back to you.' When they eventually got back to me several hours later and confirmed that, yes, it was a scam and that I would be held liable for it, I immediately contacted DHL and

asked that the goods be held. But by that time they had been picked up—$55,000 worth of goods.

CHAIR—You had asked them to hold them, hadn't you?

Mr Bond—Not exactly. I had asked them to stall, because I was not sure if I could ask them to impound the goods for me.

Senator FERRIS—A question of ownership arises if the transaction had been approved.

Mr Bond—Yes. I expressed those misgivings to the manager and left it up to him to see what he could do to delay them, to stall.

Mr SERCOMBE—What had aroused the suspicion of the DHL fellow?

Mr Bond—He had been contacted by another computer dealer who had asked him to hold a shipment of goods because they had not received payment. That was what the manager said. I understand from further discussions that it was in fact a credit card problem. I want to make one other point. We got quite an amount of material from the bank in the process of discovery, when it looked like we might go to litigation. Included in this material was a note on an informal survey conducted by a Cardlink Services employee. That person spoke to quite a number of merchants and found that in every single instance the merchant believed that once they had received authorisation for a credit card transaction liability lay with the bank.

The marketing message is getting across to the merchants that this is a safe secure means of accepting payment. It is only when the merchant is unfortunate enough to be targeted by criminals that they find that the legal interpretation is quite different. They find that in fact the words 'authorised' and 'approved'—which are nowhere defined in any of the bank documentation that we have received to have special meanings—in the bank's interpretation turn out to mean virtually nothing. They do not mean a thing.

Senator FERRIS—Mr Bond, I apologise that I have to leave. You have given us some very good information that we will raise with the Bankers Association tomorrow. I am sorry that I cannot stay for the rest of your evidence.

Senator McGAURAN—Where liability lies is an important discussion for this committee. To clarify how the scam works, I understand that the card is not a stolen card, because the owner would cancel it; it is a live card, and someone has the full details of it. Is that right?

Mr Bond—That is correct. The extent of the details would seem to be quite considerable. These were quite large transactions, and they would have exceeded the credit card limit of a lot of cards. So it was not simply a matter of knowing the credit card number and expiry date; it was a matter of having some idea of the available credit on the card as well. That indicates to me that an inside job was going on there. Lo and behold, we received a letter via our solicitor from the bank's solicitors. It states:

The Bank suspects that the criminals may have also obtained credit card account information from one or more dishonest employees in one or more of the financial institutions who issued the credit cards.

I can table that letter.

CHAIR—The card used for the transaction was a live card. Was it a stolen card or was the number scammed from somewhere?

Mr Bond—I believe that the card was most likely not stolen, because had it been stolen the cardholder would have taken some action. I believe the cardholders had no knowledge that their card details were being used in this manner.

Senator McGAURAN—There was a case in the paper recently about a similar scam being undertaken at a service station. The person at the service station got all the details of the cards and was passing them on. This is common enough.

Mr Bond—But that would not give details of the credit available on the card. These people seemed to be able to pick with unerring accuracy cards that had a high amount of available credit.

Senator McGAURAN—You said that on the flip side where you sign the card there are serial numbers.

Mr Bond—The CVC.

Senator McGAURAN—They would get hold of those serial numbers too, wouldn't they? The person getting the details would be looking at the card, so that is not quite a check and balance.

Mr Bond—They could, yes.

Senator McGAURAN—You indicated that the police knew who the crime syndicate was. Is that correct?

Mr Bond—No. I do not think I indicated that. I indicated that they did make an arrest in Melbourne but they could not establish the identity of this person. In the end I believe he was jailed for a few months and then deported.

Senator McGAURAN—What is the profile of that person?

Mr Bond—I never saw this particular individual. I have no idea of his age or anything. The only characteristic that I knew about him was that he appeared to be of African origin.

Mr CAMERON THOMPSON—Were the payments that went into your account from the card operator or from the bank?

Mr Bond—From the bank, yes.

Mr CAMERON THOMPSON—Which bank, by the way, was involved in this?

Mr Bond—That one—the Commonwealth.

Mr CAMERON THOMPSON—Over what period did the payments go in?

Mr Bond—A period of approximately a month.

Mr CAMERON THOMPSON—There was a total of $140,000-odd dollars in payments?

Mr Bond—Correct.

Mr CAMERON THOMPSON—That would have involved how many different transactions?

Mr Bond—This occurred in 1996. The final transaction alone was $55,000. I think there were probably about half a dozen transactions in all.

Mr CAMERON THOMPSON—You said that this gang were heading overseas. Where were they heading?

Mr Bond—London, Heathrow Airport.

Mr CAMERON THOMPSON—So the payment would arrive within, what, a day? You said it would be overnight, basically.

Mr Bond—Yes, the payment was in our account the morning after we conducted the transaction. The transactions were conducted through an EFTPOS machine. I should say by way of explanation that we purposely had an EFTPOS facility installed, because we wished to be able to ship goods all around Australia and get payment up-front. We got it installed in the belief that we were installing a safe, secure means of accepting payment from people who were ordering goods remotely. With regard to the orders that we received in these transactions, the negotiation took place over the telephone, and that was followed up subsequently with a fax, and the fax quoted the credit card numbers and bore the signature of the person purporting to own the cards.

Mr CAMERON THOMPSON—So all those payments went into your account. Did they take those funds back from you?

Mr Bond—After a few weeks we starting receiving letters from the bank asking us to forward them the signed vouchers. Sometimes we received the request in relation to the same transactions three, four or more times—we were inundated with paperwork—so I ended up sending them a form letter saying, 'You know as well I do that these were card-not-present transactions. Here is a photocopy of the printout from our EFTPOS machine. Please stop bothering us.' That went on for a period of months, and then the first we knew about the money being taken out of our account was when I had written some cheques in good faith and I started getting irate phone calls from a couple of people who had had these cheques bounce because the bank had taken money out of our account—it took us over our overdraft limit—and then proceeded to bounce the cheques. Then it withdrew the money piecemeal. I have a list of the amounts that they withdrew: there look to be about 20 different transactions on the list where they withdrew the money between 12 July and 20 November 1996.

Mr CAMERON THOMPSON—And they took $142,000?

Mr Bond—It was $141,151.50.

CHAIR—So they did not share any of the risk at all?

Mr Bond—No. The next thing that happened was that our overdraft blew out, so they started putting us on higher rates of interest. We could not trade because we had no facilities with the bank anymore; we were in diabolical strife. The next thing they did was send us a letter offering to help sell our house. At that point my wife virtually went into a state of nervous shock or something, and she is still recovering, so it had an extremely bad effect. I might add—and I would not necessarily want this to appear on the public record—

CHAIR—We need to go in camera. I have to ask the public to leave; unfortunately, even though you might be happy for them to listen, we do not have any choice whenever we go in camera. Will someone move that we go in camera?

Mr SERCOMBE—I move that we go in camera.

CHAIR—There being no objection, it is so ordered.

Evidence was then taken in camera, but later resumed in public—

Senator McGAURAN—Do you know of any similar examples where the bank has taken a limited liability? Maybe they just have you in the gun, Mr Bond—without trying to create tension or paranoia. Do you know of any examples of where they have accepted a liability or a limited liability? Is it all in the negotiating with the bank or do they have a strict policy of no liability?

Mr Bond—I believe they have a strict policy.

Senator McGAURAN—It is the same with everyone.

Mr Bond—Yes, there is no inequality there; they will get everyone.

CHAIR—Thank you, Mr Bond. I am really sorry that you have had such a rough time of it, and I can understand why you feel so angry about what happened to you. Obviously we want to learn some lessons from that. We have the Banking Association tomorrow, so obviously we will be raising your case with them—highlighting some problems and what it means to small business. Accept our sympathies for what happened to you. We will certainly take this example on board and see what practical implications it might have.

Committee adjourned at 4.38 p.m.