



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

WEDNESDAY, 16 SEPTEMBER 2009

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

TO EXPEDITE DELIVERY, THIS TRANSCRIPT HAS NOT BEEN SUBEDITED

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

The internet address is:

<http://www.aph.gov.au/hansard>

To search the parliamentary database, go to:

<http://parlinfoweb.aph.gov.au>

HOUSE OF REPRESENTATIVES
STANDING COMMITTEE ON COMMUNICATIONS

Wednesday, 16 September 2009

Members: Ms Neal (*Chair*), Mrs Hull (*Deputy Chair*), Mr Billson, Mr Bradbury, Ms Collins, Mr Georganas, Mr Lindsay, Ms Marino, Ms Rea and Ms Rishworth

Members in attendance: Mr Billson, Ms Collins, Mrs Hull, Ms Marino, Ms Neal, Ms Rishworth and Mr Georganas.

Terms of reference for the inquiry:

To inquire into and report on:

The incidence of cyber crime on consumers.

- a) Nature and prevalence of e-security risks including financial fraud and theft of personal information:
 - Including the impact of malicious software such as viruses and Trojans.
- b) The implications of these risks on the wider economy:
 - Including the growing economic and security impact of botnets.
- c) Level of understanding and awareness of e-security risks within the Australian community.
- d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:
 - Education initiatives
 - Legislative and regulatory initiatives
 - Cross-portfolio and inter-jurisdictional coordination
 - International co-operation.
- e) Future initiatives that will further mitigate the e-security risks to Australian internet users.
- f) Emerging technologies to combat these risks.

WITNESSES

CRANSTON, Mr Michael, Deputy Commissioner, Serious Non-Compliance, Australian Taxation Office 1

GIBSON, Mr Bill, Chief Information Officer, Australian Taxation Office 1

KONTI, Ms Bettina, Acting First Assistant Commissioner, Business Solutions, Enterprise Solutions and Technology, Australian Taxation Office 1

Committee met at 12.37 pm

CRANSTON, Mr Michael, Deputy Commissioner, Serious Non-Compliance, Australian Taxation Office

GIBSON, Mr Bill, Chief Information Officer, Australian Taxation Office

KONTI, Ms Bettina, Acting First Assistant Commissioner, Business Solutions, Enterprise Solutions and Technology, Australian Taxation Office

CHAIR (Ms Neal)—I now declare open this public hearing of the House of Representatives Standing on Communications inquiry into cybercrime. This is the fourth public hearing for this inquiry. The committee will take evidence from the Australian Taxation Office. I thank you for making yourselves available today; it is very much appreciated. Although the committee does not require you to give evidence on oath, I should advise you that the hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Would you care to make any opening statements before we start questions?

Mr Gibson—We are happy to go straight to questions.

CHAIR—The obvious question is what are the threats to the operation of the Australian tax office caused by the recent developments in cybercrime?

Mr Gibson—From our perspective we have a lot of mechanisms that protect the ongoing administration within the tax system. The bulk of the threats that are appearing from cyberspace are around things like identity theft. Phishing attacks are quite prevalent. They are not just targeted at the tax office but at banking institutions and so on. It is primarily identity theft that concerns us. We have a lot of controls, checks and balances within our internal systems to understand what some of the tax fraud matters are but cybercrime presents a different dimension to that.

Mr Cranston—I could add to that. If we are looking at the use of cybercrime for direct attacks on the tax system such as attacks involving websites on the actual system, where there have been no successful attacks, we want to distinguish that from identity crime where taxpayers can commit fraud on the tax system using electronic means, by lodging online and committing refund fraud. There are two aspects of that. Some of it is taxpayers just overclaiming their deductions, so that is more around falsification and I would not say that is in the scope of cybercrime. But some of the identity crime is where people have obtained file numbers inappropriately—stolen them, possibly through phishing schemes using the internet, or through other means—and then use those file numbers to lodge and get refunds they are not entitled to.

CHAIR—Are they lodging for refunds themselves or for someone whose identity they have taken up?

Mr Cranston—As I said, there are two aspects. The first one is where they are lodging themselves or through unregistered tax preparers. That is where you go to a tax agent who says, 'I can get an extra refund for you,' and you take advice from the unregistered preparer and you

overclaim, so you are getting a refund in excess of what you are entitled to. That becomes what we would call a normal compliance type of matter that we need to look at, and we are very successful in dealing with those. The other side of it, the stolen identities that you were asking about, is basically using somebody else's identity and lodging online and getting a refund into a bank account and stripping the bank account. The first one is more committing tax fraud. The second one is committing fraud on the tax system.

Ms RISHWORTH—Do they get in first, before the person who really owns the tax file number has put in a claim? Obviously if a second one came in that would be highlighted on your system somewhere. So do they try and get in before the real person has lodged their tax return?

Mr Cranston—Generally, most of them are file numbers from nonresidents, temporary visitors on visas, so those people with those file numbers may never have been prepared to lodge a tax return. So, to answer your question, yes, they have got in first with the file number. There are some other variations to it. Some of them do get in first and then later the right people want to lodge on their own file number, but that is a minority. Most of it is in relation to file numbers that were never intended to be used.

Mr GEORGANAS—The papers you have lodged with the committee show there has been a 31 per cent increase in tax fraud. How do you come to these figures?

Mr Cranston—That is the phishing scheme.

Mr GEORGANAS—There is phishing and malware—those are the two types.

Ms Konti—That is right. The information that we have reported to this committee is about a 31 per cent increase in IT security incidents. The actual number that we are talking about behind the percentage is 61 IT security incidents reported to us in the 2008-09 financial year. So the 31 per cent increase means that in the previous year there were 47 IT security incidents.

CHAIR—So there is a relatively small numbers base.

Ms RISHWORTH—If no-one does subsequently claim on their tax, if no-one then tries to lodge something, how does it come up for you that someone has falsely claimed on someone else's tax file number? If they never lodge a complaint, how do you become aware of it?

Mr Cranston—What we have in place is about protecting the system—prevention before cure. We have developed a number of detection and analytical models and we have learnt certain indicators or characteristics. For example, first-time lodger would be one of the characteristics. Then there are certain indicators or characteristics that identify something that is highly likely to be identity crime. That is one model, and that will spit out particular lodged returns and so they will not issue.

There is another particular model that learns off itself, so they will pick up more patterns and trends and they will go back into the system before they are actually issued and identify another further amount. So basically it does provide us with a lot of assurance, and when we have gone back and tested those, from last year we used this particular model in a post environment and even this year we have learned we have got about a 95 per cent success rate with that.

CHAIR—I have one more question in relation to false ATO sites. I understand from your submission that, with the large increases in the number of people online, there has been some difficulty with fake ATO sites being set up and people going on and divulging personal information thinking it is the ATO. I understand there was a site being hosted in the Ukraine that was doing that. How prevalent is that and what is the ATO doing to try and reduce that risk or to protect people from that?

Ms Konti—I can answer that. The type of cybercrime that we are seeing more and more often around the tax office is in fact these phishing attacks, where there will be people who host sites that look like the tax office and offer a very credible tax office image that are specifically designed to lure taxpayers into providing personal information. When we discover one of those—and the discovery is either through AusCERT, a not-for-profit agency that we have partnerships with and they can sometimes alert us to these, through our own discovery mechanisms or in fact through having them reported to us by a member of the community—there is a security action plan that then gets kicked off as a result of that. We work with the AFP and the High Tech Crime Centre to basically identify the site and to shut it down. Then we have a number of communications mechanisms available to us through our website and through various media releases in order to be able to alert the community to this going on.

CHAIR—When you say shut it down, how do you do that if it is located in the Ukraine, outside the jurisdiction?

Ms Konti—I understand that we can shut down the site and prevent it from being able to be available. To find out exactly how that happens, I would have to take that away.

CHAIR—I would be very interested to know.

Mr Gibson—Each of the sites has unique network identifier and the High Tech Crime Centre, in conjunction with the internet service providers all round the globe, works to identify a network address that is doing this. They have a way of completely turning that off so that, even if the site is still trying to be active, it is denied access to the internet. That address is made invalid. We can get some better explanation for the committee on that.

CHAIR—I would very much appreciate that.

Mrs HULL—You were asked previously about the 31 per cent increase and you went on to say how many incidents that actually was. Could you give us an indication as to the extent of those incidents? Can you give us an example of what they entailed: is it significant fraud, is it minor? Can you give us an explanation of what types of incidents took place there?

Ms Konti—By far the majority of those IT security incidents that were reported turned out to be a form of phishing attack of the kind described by Ms Neale, so that would have been one of the 61 reported in the 2008-09 year. Of those that were not phishing attacks, all of them turned out to be quite minor. We define IT security incidents as 'a potential'. It is only upon investigation that we either discover that it is a real phishing attack or a real cybercrime attempt or something that could be like a lost laptop that someone has reported to us that we then go and recover. Other types outside the banner of phishing have tended to be of the more minor type.

Mr Gibson—To be quite open, it is extremely difficult for us to assess the impact on the community unless we can see that reflected in some way within our systems. Where we see a tax file number has been compromised, we have a lot of mechanisms, as Michael was saying, that can detect that and flag it as a suspect, or out of pattern, type of behaviour. Those ones we can quantify, and they are the sorts of things we have referenced. But in terms of, ‘Is that phishing attack? What is the extent of the impact more broadly on the community?’—because they do not just look for tax file numbers, they will look for credit card numbers—we cannot quantify that. Perhaps financial institutions and credit card companies could, but it is very hard for us, quite honestly. We do not have access to the consequential impact information.

Mr Cranston—The only thing I could add to what Mr Gibson has said is in relation to a number of those phishing attacks. We have identified that three were used to get identities to come back into the tax office and get identity crime refunds. We have actually got three investigations currently in place for those. Basically, they were just offering employment, again, to non-resident visitors. You come onto this website, provide your name, your file number and date of birth et cetera, and they use those particular details to attack our system.

Mrs HULL—When you talk about the non-resident, years ago in the economics committee we did a report, *Numbers on the run: review of the ANAO audit report No.37 1998-99 on the management of tax file numbers*, where we found there was an enormous amount of tax file numbers being put up in backpacker accommodation—you would just go in and select your tax file number. Do you think that is still a problem, where people come in, get a temporary tax file number and dispose of it inappropriately?

Mr Cranston—I think the first step is that we have got identification checks, so the person may get the file number appropriately. We have also got a lot of messages in the community which say, ‘It is your file number, you should protect it.’ There is evidence to say students will just hand that over for a fee to groups or syndicates. Apart from the messages we send out, we control that behaviour by what I said before about assistance. We will more than likely stop anybody using that particular file number and getting the inappropriate refund. Then, of course, there are follow ups after that. Once we have identified that we will do some more work in relation to that to try and identify people using it. It may lead to investigation and more serious approaches to deal with that sort of mischief, like prosecution.

It is a suite of things, but we have not identified inappropriate obtaining of file numbers. If you are here as a non-resident, you do need a file number—especially if you are working—and you need to lodge a tax return.

Ms Konti—The other service that we offer to citizens who believe that their tax file number might be compromised is to close that one down and issue them with a new one so that they can feel more protected.

Ms COLLINS—About the 61 breaches of security and the 35 prosecutions—how difficult is it to actually investigate and prosecute, and what other tools do you need to make it easier for you to be able to do that?

Mr Cranston—It is extremely difficult in identity crime, and there are two aspects to it. The first one is that you have actually got to find the person who has committed the crime. That is

very difficult, because it has got to be a person. The second thing is that often it is getting the evidence that the person had the intent to commit the crime. Even if you have suspicions about a person, you have got to have the evidence that they actually did it. It is difficult.

You spoke about those figures. The number of prosecutions for refund fraud last year was 38. I want to have the record amended, because we said 35. Ten of the 38 were in relation to identity fraud. The rest were more in relation to falsification—lodging online but overclaiming their own expenditure—and those cases are not as difficult as the identity crime matters.

Ms COLLINS—Is there anything that governments can do to make it easier?

Mr Cranston—There are a couple of things where we are working with other agencies. It is really about sharing intelligence. I think we have come a long way in relation to that. There are a couple of strategic forums that try and share best-practice models in relation to that—sharing better ways and methodologies in working in this space. I think it is important. For example, the ACC are actually developing a list of compromised identities so we can start sharing that data, which may help us identify whether these identities are used with any Commonwealth agency; if they are, you should be concerned. In relation to our laws, I think there is a particular piece of legislation in parliament at the moment around identities, for the Criminal Code. I am not an expert on that—I think you would have to speak to the Attorney-General's Department—but I think that may assist in dealing with people who have harvested identities and have not actually used them yet.

CHAIR—Yes. We had evidence given to us earlier that at the moment, unless you actually utilise the identity to commit some sort of fraud, it is not a crime to steal someone's identity. The legislation that is presently before the parliament will make taking someone's identity information a crime in itself, so you are correct.

Mr Cranston—The particular code we use is the criminal code 'financial benefit by deception', so there has to be a financial benefit.

Mr BILLSON—On that topic, my understanding of it is similar to what you are describing now—that you actually need to use the information or, under the amendment, have an intention to deal with it. I certainly hold the view that holding that material should be an offence, and it seems as though the legislation will not reach that far. Do you have a sense of whether the extent of criminality can be simply the holding of information, even if it is not being exercised or applied whether for financial gain or for other purposes?

Mr Cranston—That is a hard question to answer. From a tax perspective, our concern would be more about whether people have actually used it on our system.

CHAIR—I will just give you a bit of a caution. If you have not actually seen the legislation, I do not know if you should give evidence to us about what its effects are.

Mr Cranston—Yes, that is why I said I would rather not comment on that.

Mr BILLSON—Moving on, then, your tax file numbers have a utility in their own right. Other people look to them as a proxy for a whole range of other things. Have users of your tax

file numbers—not the people to whom they were issued but others who have relied upon them—come to you to say, ‘Look, we’ve found this, this and this with our dealings’? Do you have that kind of relationship operating?

Ms Konti—I believe that employers and financial institutions collect tax file numbers in order to be able to not apply a higher rate of withholding against earnings. The employers and financial institutions do report to us on an annual or even quarterly basis the information that they hold, and we undertake some matching. They also, from time to time, report to us things that they think might be suspicious for us to follow up.

Mr BILLSON—With the ABN process, I imagine all that is ripe for simplifying some of that front-end regulatory requirement, but now those business entry points have a degree of overlap with other jurisdictions—whether you get your ABN, your register, your business and all these kinds of things. Has that highlighted any new challenges in terms of security of that information? In terms of other people using it, there is some suggestion that there is legislation that lets third parties vary their personal and business information under that collaborative arrangement. I am just wondering whether you have had any experience or observations about that.

Ms Konti—The Australian Business Number is a little bit different to the tax file number in that it is a public number. There is a lot of publicly available information that is connected with an ABN that is available to all of us to look up through the Australian Business Register site.

Mr BILLSON—There is a suggestion that others can vary the information that sits behind the ABN and there are questions as to whether you are an organisation that has the scope to vary the information or whether there are others who can impact on that information other than the person to whom the number was issued.

Mr Gibson—What we might do with that one, given that it seems fairly complex, is we might take that on notice and come back with an expanded response on that particular question.

CHAIR—We would appreciate that.

Mr GEORGANAS—The ATO says that, as improvements of security in the finance sector take place, the cybercriminals are looking for new markets and governments are the next market. Do you see an increase in cybercrime in the ATO and if so, are there any new forms that could take place in the future that you can foresee or that you are already looking at?

Ms Konti—The increases that we have seen so far are in relation to phishing attacks and people posing as the tax office in order to try and siphon personal information from members of the community. We have seen an increase, as we have reported to you, over the course of the last year. One of the possible reasons for that could be the tax bonus that the tax office administered recently where we basically asked people to make sure that they updated their information so that we could get them their \$900. We did see an increase over the course of that period.

Mr GEORGANAS—I received many emails from bogus sites saying ‘put in your details so you can receive a bonus’.

Ms Konti—We are seeing the vulnerabilities here as lying in the community, the extent to which people in the community are aware of what is going on out in cyberspace and the need for us to continue to assist in that awareness and education about how people can protect themselves.

Mrs HULL—What are you doing in the education programs to make people aware of that? The bonus issue is a pertinent point in that it is sometimes the case that you just respond to these phishing emails. You may not do a lot of tax transaction online but you email prolifically. It is an issue that we confront every day. There is a view that everybody does these things online, so they automatically get the pop-ups and the warnings when they go online to ATO. That is not so much the case. The fact is many people do not do that but they certainly use email all the time, so when these are coming in they do not necessarily click that they should not be responding because they have not done this online. They just assume in this day and age that the ATO, government departments and organisations, such as yourself, have access to their information. What are you doing to engage, educate and assure people of the need to protect their privacy?

Ms Konti—There is quite a lot of information that we have put in our submission in relation to this. The point that you make about people not necessarily regularly interacting with the tax office in the normal course of business is a valid point. It is difficult for the tax office—with the reputation that we have—to want to get out there and issue an education message when most people do not want to hear from us that often. Nevertheless, there are a range of things that we do on our website, but of course people would have to go to our website to be able to see and receive that information. Any time that we are made aware of a phishing scam or an attack by someone posing as the tax office, we have media releases and other forms of communication like that available to us to help inform the community about current things that are going on.

Again, on our website we have special links about identity theft and the steps that people could take to protect themselves from those sorts of things. Our website also has links off to a number of other government-run sites like Scam Smart and Stay Smart Online that have even more information about how we can protect ourselves.

Mrs HULL—It is assumed that everyone can use websites and that if you are on a computer and you even use email then most definitely you are going to be into websites, googling and searching, and doing all sorts of things. That is actually not the case. Is there a view that you need to do something to look at educating those people who are not able to get to websites and may not have the ability in regional Australia to access websites anyhow because we do not have the technology.

CHAIR—Don't worry we're helping you with that!

Mrs HULL—I hope I live to see it. It may be that there needs to be another active form of education process. Maybe you are relying too much on putting your warnings on internet sites.

Mr Gibson—I think taking a proactive approach to community awareness and education is absolutely at the heart of a lot of this because the threats are, in a sense, generic. They are not just at the tax office. They can be at financial institutions or anything that is about your personal affairs. We think that probably a campaign would be more effective if it were coordinated in some way across both government and private enterprise because we go out a great deal in the

media. These phishing attempts are always there whether they are targeting the tax office or another institution. In addition to the passive awareness and education that we do via our website, if there is a campaign against the ATO—and we had 61 last year so that means probably a couple of times a month we are in the media—colleagues and I get interviewed and talk with journalists and online radio. Our emphasis is in saying, ‘If you are not expecting it and they are asking you for personal information, do not provide it.’ We say, as the banks do as well: ‘We will not ask you to divulge to us personal information. We will push something to you perhaps, but we will not ask you or require you to enter online to us, personal information via an email.’ We are very firm on that. I think that if that type of communication campaign were coordinated across the government agencies and private enterprise, it would be far more effective. It would be less confusing because we might express it in a different way to how a bank expresses it.

Mr BILLSON—In a tax office way!

Mr Gibson—We do think that is a strong point that we would like to leave with the committee.

Ms COLLINS—We heard evidence from the AFP about broader public education being necessary. How strong or how overt do you think a public awareness campaign would need to be? The AFP suggested something like the AIDS campaign in the eighties. How drastic do you think we have to be? How big a problem do you think it is?

Mr Gibson—We all know the threat is real and our concern is that the threat is increasing. We were actually thinking of something like the Slip, Slop, Slap campaign. That type of protection.

Ms COLLINS—That was our other example.

Mr Gibson—It is something that is to the point, leaves a mental image and so forth for the community. If we talk too technically to them and put too many qualifications and say, ‘Watch for this and watch for that,’ it will get very difficult.

Ms COLLINS—Do think it would be effective, though? Do you think a broad public education campaign would work?

Mr Gibson—I think so. I do believe so, because if it is simply ‘if this looks odd, don’t do this’ or ‘don’t divulge personal information’ there are a number of key messages that you could get through, I think.

CHAIR—There was a suggestion that there are a relatively small number of fairly simple mechanisms that, if adopted by consumers and users, would greatly reduce the capacity for cybercriminals to intercept information and misuse it. It suggests that a coordinated approach—you must all be caucusing—including both government and the private sector might very well be useful in achieving that.

Mr Cranston—Yes. I think a coordinated approach could still be supported with specifics around your own organisation—file numbers, for example. If people ask for credit card details, you do get concerned, but I think something like a file number probably does not concern most

Australians as much as credit card details would. So I think we need to be consistently backing up our awareness from the ATO in relation to that.

CHAIR—Of course, yes. Everyone has their own sorts of issues.

Mr BILLSON—The irony around that is that the advice we got, which was quite troubling, is that most people do not care enough; if it is a financial transaction through a bank or something, there is a sense that they are inoculated against great harm. We were having a conversation about how HIV-AIDS campaigns and Slip Slop Slap and anti-smoking messages try to make very vivid the harm of not changing your behaviour. But the feedback we are getting from the AFP about this area is that most people do not give a stuff because they just do not think that it is going to have a huge impact if someone gets that material. Now, in the cases you have given us, the harm is harm to the taxpayer in most cases, and I do not see people screaming to change their behaviour to do something they think is reducing a potential loss of revenue to the tax office! I do not see that. So I am wondering if you could describe to us the personal harm and consequences that in your experience flow from tax file numbers and the like being pinched, to help us understand what would motivate people to change their behaviour. It is a nuisance, it is annoying, it is a pain in the neck, but even with banking transactions people think: ‘Oh, it’s all right. I’m not going to lose too much. I’m not going to worry about it; I’ll just get new account and all that.’

Mrs HULL—I think it is because the banks are giving the money back; they are actually protecting their clients, and that is the AFP’s line—that there is not so much of an incentive there to change your behaviour because you are actually getting your money back and you are not getting the loss.

Mr BILLSON—It is harm minimisation, almost.

Mrs HULL—Yes.

Mr BILLSON—Like PayPal. PayPal inoculate a person against fraud. They say, ‘We’ll cover it; if our systems aren’t good enough, we’ll cover it for you,’ and people go, ‘Oh, okay.’

Ms MARINO—Just along these lines—sorry, did you want to say something before I asked my question?

Mr BILLSON—I would like them to say something, like an answer about what some of those consequences were!

CHAIR—Sorry; I thought it was just a comment.

Mr Cranston—One example is that a question was asked before about identity crime: was it that they had got in before the real taxpayer? And, yes, there have been instances of that. So sometimes—

Mr BILLSON—Can we just follow that through. If they make that case to you, then what happens? Do you say, ‘Someone else said that; you rack off?’ or do they then need to make the case that it is not from them and then the harm to them is just some—

Mr Cranston—Yes, the harm to them is just inconvenience. The tax office will remedy the situation. But naturally it would be a concern and it would be an inconvenience to the taxpayer.

Mr Gibson—My concern is that this is all focused on identity protection and privacy and so forth. People may feel, ‘The banks or the tax office will do the right thing by us personally because we have not been culpable in this regard,’ but I just think that the escalation of these attacks is real and that there are other things that are important to people from a personal and identity perspective where they will need to understand that, while they might have some protections in some dimensions, in those other areas they may have some vulnerabilities. So I do think that just that potential for scaling-up would warrant us thinking: is an awareness campaign on general identity theft and protecting personal details something that we should be pursuing?

There would be a range of secondary benefits, whether it would be financial institutions or the ATO and other government agencies that would benefit from the knock-on effects of that. We have an active compliance program which we make very public. We will say, ‘We are looking at tax affairs in the following categories of work and so forth.’ We know that when we talk like that it is a deterrent. It causes people who, maybe unwittingly, might err to get advice and put their tax affairs in order. So there is that deterrent effect. I think raising the awareness is a very similar approach.

Ms MARINO—On these types of questions, how many times in the last couple of years that you are aware of has the tax office had to advise someone that they cannot use the online services because they have been compromised? How do you let them know through your system that they have? For a business, how long is it before they are actually able to deal with you again?

Ms Konti—Just for clarification, are we talking about circumstances where an individual’s identity or a business identity may have been compromised?

Ms MARINO—Yes, or you are aware through their contact with you that their system has been compromised. Do you have any capacity within what you are doing to know whether there is a problem with that linking computer?

Mr BILLSON—If you are worried that your digital certificate has been compromised, how long does it take to get a new one?

Ms Konti—In the case of a digital certificate, if someone rings up and reports that potentially their digital certificate has been compromised then we can issue a new one. The current amount of time that it takes to get a new one is something like five to eight business days, and that is an issue with our current digital certificate process that we are aware of and are in the process of fixing.

Mr BILLSON—What about Ms Marino’s question? If you think it has been compromised, how do you arrive at that conclusion and tease that out?

Ms MARINO—Yes. How do you establish that they have been compromised and then what process happens from there for you?

Ms Konti—This is probably more in your area, Michael.

Mr Cranston—In relation to the file number abuse, when there is suspected to be misuse of a file number or a stolen file number there are immediate inquiries. Often, if a particular person says, ‘I haven’t even lodged my tax return,’ that matter can be dealt with very quickly. The file number will be locked down and a new file number will be issued immediately. I can take on notice the time that all takes. Timeliness is very important for that, so I think it does happen rather quickly.

Mr Gibson—We will take that on notice. There is another example in the last few years that I recall. A tax agent’s premises were burgled.

Ms MARINO—Yes, ‘compromised’.

Mr Gibson—Their equipment was stolen and so forth. That was a real scenario, and we could report back on how we handled that as an example of quite well-proven and exercised internal processes in terms of how we deal with that information being potentially compromised.

Ms MARINO—Given the potential for increase in that, I think the timing issue will become more relevant.

Mr Gibson—Yes.

Mrs HULL—You have just raised the case of the tax agent’s office being burglarised. What specific standards and systems do you have in place for the registration of businesses like tax agents and what sort of security they have? Do you have a set of standards for the security measures that they have to have on their systems before they can be a tax agent? Is there a role for auditing these tax agents? What do they have to comply with in order to be able to deal with the tax office? What are the standards that they have to comply with? Is there an audit to ensure that those standards are being upheld?

Mr Gibson—I think there are two dimensions to that, and I am going to ask Michael to answer on one of them. In terms of the technology side of it, we have a Software Industry Liaison Unit, and we do a lot of work with developers of things like accounting practice management software. It is only those legitimate software packages that can interface with the ATO. Through that liaison unit, we have quite good engagement about standards and so forth.

As to tax agents, in terms of certification, we do not certify tax agents, I do not believe. I think that is an accreditation that comes from a professional association. If that is not correct, I will come back, because I am an IT person rather than a tax person. But I am sure that is the case. So those professional associations have accreditation and quality assurance processes that they run within—

Mrs HULL—And that is in conjunction with the ATO? Do they have a set of standards to meet in relation to their connection with the tax office? Do you set out a set of standards that all of their members must meet?

Mr Gibson—I will need to take that on notice, unless Michael knows.

Mr Cranston—We will take it on notice.

CHAIR—I have a question to follow up on that. You have talked about the timing of reporting to taxpayers where there have been breaches. I suppose the whole premise of that question was that there is a protocol in place that requires the ATO to actually report to a taxpayer when you become aware that their tax file number or their information has been compromised. Can we confirm what that protocol is in those circumstances as well?

Mr Gibson—Yes, will do.

Mr GEORGANAS—Amazingly, I was going to ask a very similar question. In the case of receiving the bogus email to begin with and you report the bogus email that is requesting your information to the ATO, what is the procedure from there on from the ATO side? I have rung in and I say, 'I have received this email. I know it is bogus, because X, Y, Z. They are asking for all my information. It has got your letterhead on there and all the details of the tax office and it looks authentic. I have not responded to it and I am not going to respond to it, but I am letting you know.' What is the procedure from there on? What would happen in that case?

Ms Konti—Our Security Incident Response Team is the team that this goes to. They are the ones that immediately launch the investigation and the shutdown processes that we talked about before.

Mr GEORGANAS—When you say 'shutdown processes'—the host website? Okay.

Ms Konti—So our focus is very much on limiting the harm by shutting that down as soon as we possibly can. We work with the AFP and AusCERT and agencies like that in order to be able to achieve that. Our very next priority, or in parallel to that, is getting the information out to the community about the fact that this exists.

Mr GEORGANAS—I know that this is a hard question to answer, but how long would it take to shut that host website down?

Ms Konti—I would have to take it on notice. I think that it is very fast, but we did not come prepared for—

Mr GEORGANAS—I suspect the criminals then would go onto another host site.

Mr Gibson—Some of them are very sophisticated and just hop around, yes.

Mr GEORGANAS—In case of this last one, the bogus one, it was going around for a few months at least, I think.

Mr Gibson—We will include that and bring it back too.

Mrs HULL—You mentioned in the beginning that because people are not enamoured with the ATO, they may not want to come and hear what the ATO has to say et cetera. I am actually having a forum and the first people I invited to present were the ATO. But it struck me that for that very reason, if people are feeling that way about the ATO, then they would probably respond

much more quickly. It might be a response in haste in order to ensure that they are doing the right thing—it is a bit like a policeman driving past and you know you are doing 100 kilometres but you still think you are going to be booked for speeding in a 100 kilometre zone. Is there an ability to come back to us with information about what could be done to ensure that there is a strategy being worked up to deal with the people's perception of the ATO and whether or not you are trying to help them or hinder them? They stand to be more vulnerable, purely as a result of the feeling that the ATO are seeking answers from them and they need to respond straightaway. Could you think about what might be happening with that, or is anything happening and, if it is not—

Ms Konti—I want to make sure that we understand your question well enough. You are suggesting that the ATO is seen as a feared agency. For example people who receive an email purporting to be from the tax office might respond very hastily because they do not want to be in trouble, so you are asking what the tax office is doing about trying to shift that reputation.

Mrs HULL—Or even if the ATO is aware that this may be creating a problem for people and how they might try to respond to that issue or how they might look to deal with that issue if it were recognised this could be a problem for the consumer.

Ms Konti—In relation to helping particularly in the cybercrime space, we will take that away and come back to you. To note, the tax office has been doing work for a long time to try and improve its reputation as not only a respected but also a friendly agency which will not only assist people in understanding their obligations to the tax office and to government more broadly but also one which will also take a firm hand to those who do not want to comply.

Mr Gibson—With some success as well.

Mr BILLSON—On page 6 of your submission you made some points about increasing vulnerability, and cloud computing was one that was raised—I can see the fiscal architecture opening that up. But you touched on virtualisation software. I imagined what that meant and did not get very far. I have tried to imagine a bit more and I think you mean Second Life and things like that where you can trade and transact. Is that what you meant? Because I did not know what 'virtualisation software' meant. I have just tried to fire up Second Life where you are in a 3-D virtual world. I know there is increasing commerce in these virtual worlds and I am wondering whether you are saying people might inadvertently provide personal details about themselves to engage in these activities. That is the best I could come up with. I have no idea what you meant. The bullet point I am referring to reads:

paradigm shifts in the way IT is used, such as cloud computing and virtualisation software where new opportunities for cyber crime might occur.

Mr Cranston—It would be really early for the ATO in this particular space, but we know these things exist and if you are talking about crime, potentially some of these sites are used as areas where you can trade and there is potentially income that should be taxed by the tax office, so that is probably one concern. I think there is also potential where profits or proceeds of some crime could be somehow laundered through that. That is not particularly a tax issue but tax fraud and then the laundering of it could become a tax issue.

Mr BILLSON—So I was on the right page generally with what you meant there.

Mr Cranston—We will take it on notice and if there are any other aspects to it we will provide that information to you.

Mr BILLSON—On the trading side of it, as I understand it, you can subdivide property and pick up virtual cash and then use that to buy other virtual things. It is not quite the Bartercard but I was imagining you might have needed to set up some kind of account.

Mr Cranston—It is very new for the ATO. Our intelligence in this area is really new.

CHAIR—But it is not really buying anything of real value.

Mr BILLSON—Is it real money?

CHAIR—No, it is all fake.

Mr BILLSON—That is why I was trying to draw out what the angle was in the submission, because it claims it is quite contained. I was just wondering why you had that there—that was all.

Mr Gibson—I think there is an IT technical architecture question underneath that as well as potentially with those social networking sites as well.

Mr BILLSON—So beyond the cloud there is the architecture.

Mr Gibson—We will try and clarify that in plain English for you.

Mrs HULL—Was the tax office sufficiently engaged in the new identity fraud legislation that is in front of the House? We have had witnesses who have suggested that unlawfully obtaining information—for example, tax file numbers and other information—should be a criminal offence.

CHAIR—Excuse me, Mrs Hull, we had some questions about this legislation before and I think the witnesses said they had not actually seen the legislation, so it is a bit hard for them to answer questions about it.

Mrs HULL—I understand that they had not seen the legislation, but what I am asking is: were you engaged in it? The question I am asking is: were you asked? Was the tax office asked to engage in this legislation?

Mr Cranston—I will take that on notice. Sometimes with legislation like this, if it is relevant to the ATO we are asked for a response. But I do not know if we were engaged in this particular legislation.

Mrs HULL—The second question, if you would take it on notice, is: if you were engaged, do you think the offences in the legislation are broad enough to capture the concerns that the ATO might have?

Mr Cranston—Yes, I will take that on notice.

CHAIR—I think it is fine taking it on notice because there may well be other sections of the ATO that were engaged on that aspect of it.

Mrs HULL—Okay.

Mr BILLSON—Madam Chair is keen for us not to drift too far into that.

Mrs HULL—I think it is interesting.

Mr BILLSON—Me too.

CHAIR—Do you have questions about cybercrime?

Mr BILLSON—There was one. We are just mopping up the terrific work that the committee secretariat do—and they will bring crummy sandwiches if we don't ask all the questions that are here! The question was around forensic analysts: are you involved with private forensic analysts and can you explain the US system of accrediting computer forensic laboratories?

Mr Gibson—I cannot explain the system. If you would like us to explain it to you, we have a very strong forensics internal capability, as does the likes of the AFP, and we work very closely and collaboratively in that regard. We have a strong forensics capability because we do various site visits and we have a whole lot of data that we need to try to understand and it contributes towards evidence for any criminal prosecution and so forth. I will be able to answer that question about the standard setting of laboratories. I will need to go back to my forensics team and have them answer it, but we do have a very capable and strong local forensics capability here as part of the ATO.

Mr BILLSON—In relation to the design, such as with the BAS and the like where you have tolerances that you would expect a contributor of a kind of enterprise to sit within and then you focus on deviation outside that, is a similar model applied for the tax file number use as well? Is that part of that, rather than the content of the information received or maybe the frequency of the material?

Ms Konti—Those analytical models that we apply across the activity statement and income tax returns and to be able to identify identity fraud are all in the arena of the tax office's business in ensuring compliance with the tax system—so, yes.

Mr BILLSON—As a supplement to that, on a second tax file number issue, the bane of our lives is people not paying their child support liabilities and that symbiotic relationship you have with the Child Support Agency. Does that also come into it, where you see an application for a tax file number that looks like, sounds like and probably is someone who has a liability but is looking to start over again? Is there any overlap there with your work, where it is a person's own identity but they are seeking to recast it for the purposes of their interactions with your agency?

Mr Cranston—We do provide information to the Child Support Agency—specific information that is requested of us. I will take on notice the question about when a file number is

compromised and the matching of the identity of that particular file number in relation to Centrelink and other agencies such as Child Support. I am sure we follow up on that.

Mr BILLSON—We have a dilemma at times with people claiming that someone is in a position to pay, and from all the material it looks as though they should be, but for whatever reason that is not working its way through. I could only imagine they were defrauding their own identity to create another one of themselves and maybe the datamatching has not quite caught up. I do not know why it is.

Ms Konti—Yes, in order to avoid paying child support, for example.

Mr BILLSON—Yes, or catching a backlog of liabilities and the like.

Ms Konti—We can say that the Child Support Agency, by law, are able to access certain aspects of the information that we hold at the tax office.

Mr BILLSON—I was thinking more about the matching exercise. If you had a valid case file in a Child Support Agency matter and you knew someone's tax file number, and the data-matching is all ready to go, but then someone actually changes one of those data points—that is, they vary their tax file number or whatever—would that be caught up in your system?

Ms Konti—It is more likely to be caught up in the Child Support Agency compliance mechanisms.

Mrs HULL—When you have these issues of breaching and it is about a refund, is the money normally to go directly into a bank account or are they seeking a cheque to be posted out? If you have got somebody claiming a refund based on tax file number, do they want it to go electronically into a bank account or do they want a cheque?

Mr Cranston—In relation to the identity crime refund?

Mrs HULL—Yes.

Mr Cranston—That would be going into a bank account.

Mrs HULL—Okay. So it is an electronic refund into a bank account.

Mr Cranston—Into the account, yes.

Mrs HULL—If a tax file number is attached to my name—whether I am a temporary resident or whatever—and somebody uses my tax file number to claim a refund and they want the refund lodged electronically in a bank account, obviously there has to be an account with that same name.

CHAIR—They set up a fake one.

Mrs HULL—So they set up a fake bank account. To set up a bank account, you have to provide a significant amount of information and proof of identity to the bank. If that refund goes

in there electronically, how do you prove that that person is not the person whose tax file number it is? How do you prove that is a case of identity theft, that that is a different person? Surely they would have had to provide an enormous amount of information to be able to set up the bank account in the first place. Isn't this what identity theft is all about—you can't just say 'it's not me'? How do you prove that that person is not the person that is entitled to that refund and that account has been compromised?

Mr Cranston—There are a lot of aspects to that question—

Mrs HULL—Yes, I know. I just do not understand it either.

Mr Cranston—because in some cases they use the bank account of the person who owns the identity but they will also have a credit card that they can go and use in an ATM. So it is not always about a criminal falsifying a bank account. In other cases they have opened up bank accounts, sometimes in other names and with other identities, and got away with it.

Mr BILLSON—They can access the account, even though they might not have created it.

Mr Cranston—They may not have created it, but they have got the credit card, and sometimes they have been bought.

Mrs HULL—That is exactly my point. How do you prove that somebody else has accessed the money that you have deposited electronically into an account if that somebody else is outside and, through phishing expertise or whatever, has been able to go into that account? How do you prove it was not the person who owns the identity?

Mr Cranston—There is a suite of things we do. We will know it is an identity crime, and to find the person who actually committed it we will use things like surveillance capability—whether they are accessing through ATMs or they are regularly attacking our systems, so they use internet cafes. Or they will use it through a particular IP address and we can actually identify where they live. So we can say, 'The computer they used was at this location, and you live there.' From that an investigation starts, there are a lot of other things that we need to understand, and it really depends on the particular situation. Banks have surveillance cameras that we—

Mrs HULL—So I can say to you, 'I didn't lodge that tax return. This is my account and I didn't take the money out of my account that you put in it,' and you are going to believe me.

Mr Cranston—Are you working back from the deposit and saying that is your account?

Mrs HULL—I have an account and you are answering my questions, saying: 'Somebody may not have created an account. They may just be able to get into your account, and they have lodged this falsely.' Then it comes into my account and they have the ability to somehow get this out of my account as it has come in. I am going to say to you, 'I didn't lodge that tax return.'

CHAIR—I think Mrs Hull is concerned about how the consumer proves it was not them.

Mrs HULL—Yes, how do I prove that I did not lodge that tax return and take that money out?

Mr Cranston—I have not seen a situation where a consumer still residing in Australia has had moneys deposited in their accounts that somebody was using. What I was saying before was that you may have handed over your file number, the account details and the credit card as a package and sold that to somebody who has now used it, and you have left the country. I have not experienced or heard of any situations where somehow another person has used a consumer's account and had access to that account. That would be very difficult to do, unless they were part of the conspiracy to commit fraud.

Mrs HULL—Good.

Ms Konti—The risk that you identified in that scenario, even though we might not have seen it, goes to the question that Mr Billson asked before: what is the message that we would give to the community about what is the harm? There is a bit of a picture about what the harm could be that you have just described to us.

Mr Cranston—The banks also have fraud units and they provide high-risk methodologies. They would say, 'This is a potential identity crime fraud,' and give us the details, and generally they are right.

CHAIR—Thank you very much for attending.

Resolved (on motion by **Ms Collins**):

That this committee authorises publication of the transcript of the evidence given before it at public hearing this day.

Committee adjourned at 1.43 pm