CRIMINAL CODE (IDENTITY THEFT) AMENDMENT BILL (NO. 2) 2009

Second Reading

Resumed from 14 October.

MR A.J. WADDELL (Forrestfield) [4.13 pm]: Identify theft is a growing epidemic. It is something that has been sweeping through Western Australia and has touched my electorate in recent times. It is one of those odd crimes because it does not happen at a point in time. It does not have any residual marks and it does not leave anything on a person but it can have an incredible impact on somebody's life. I would like the house to understand that identity theft is probably not a new crime. I suspect that it has probably been going on for decades in various forms.

Mr C.J. Barnett: Stealing passports.

Mr A.J. WADDELL: Yes, it involves stealing passports and forging all sorts of documents. We are now living in a time when we use a level of technology to carry out our day-to-day activities that bypasses the need for physical items. When we talk about identity theft and credit cards being stolen, we are not talking about the physical credit card being stolen; we are often talking about the information that is contained within that credit card. I am sure that most of us have been guilty of playing fairly loose and fast with some of our identity over time. I have assisted a number of people in this house with some of their technological problems with their computers and so forth. They have been relatively pleased to reveal their passwords for their accounts to me. In many cases they have very simplistic passwords. That might not seem like such a threat, but if members were to pause for a moment and contemplate the information that runs through their email accounts and the fact that they often link their financial institutions and so forth through their email accounts and the ability for somebody to access their email and therefore trigger a series of events that would allow them to access some very private confidential information, it would not be too difficult to see that that could be done relatively easily. I suggest that people here are relatively sophisticated. They are certainly not members of the community who are completely unaware of this risk.

During question time today the Attorney General indicated that he had some issues with this bill. He felt that it was not state of the art; it was based on a South Australian act that was probably passed when identity theft of this type was just being identified as an issue and maybe we could do better today. I am completely convinced that the Attorney General is correct in that respect. I suspect that this bill does not go far enough. I hope that the bill that the government will bring forward will go further. I still support this bill because something that goes half the way or three-quarters of the way is certainly better than something that goes none of the way. We need to recognise that today there will be dozens, if not hundreds, of people in our state who will be affected by identity theft. Tomorrow there will be more and the day after there will be more. The sooner we bring about action, the sooner we can begin to combat this scourge.

There are three points in the explanatory memorandum explaining the nature of this bill. First, the bill will make it an offence to obtain or deal with another's identification information for the purposes of committing an indictable offence. That seems fairly straightforward. Second, it will make it an offence to possess equipment capable of being able to make identification material or being used in an offence against this act. I suspect that that is probably the crux of the criticism that has been made against this bill—that we are not dealing with the communication of information. Communication is very cheap because the perpetrators of identity theft are often not within our jurisdiction or are working in cahoots with people who are not within our jurisdiction. Identity theft can happen anywhere in the world and can attack somebody quite locally. I regularly carry out transactions all over the world. I wonder how my credit card company copes with the fact that one minute I am spending money in London, the next minute I am spending it in China and a few minutes later I am probably spending it here in Perth. I have been contacted by my credit card company on several occasions to ask whether they are legitimate transactions. I usually say, "Yes, that's me, three o'clock in the morning, shopping online."

Mr C.J. Barnett: You need weeknight trading.

Mr A.J. WADDELL: I do not need it; I have online trading.

Ms J.M. Freeman: At three o'clock, you need a life!

Mr A.J. WADDELL: I agree that I may need a life.

I was recently contacted by my credit card company asking me whether I had spent 27c in Thailand, to which I indicated that I had not and I was greeted with, "Thought so." The credit card company's security software had detected an unusual transaction. I queried the nature of this transaction. I was told that these companies generate random credit card numbers and they keep throwing them at the system until they get a hit. They can throw

millions and millions of numbers at them and when they get a hit, they start to scale it up a bit more and then a bit more. They start taking small amounts out of people's accounts, people often do not notice the small transactions and they get away with it. If we multiply that by tens of thousands, we see that they are making considerable money. That is probably where the criticism of this bill lies.

The third point interests me most. The explanatory memorandum states —

> Enable a judge, after recording a conviction against the offender, to issue a certificate to the victim whose identity has been obtained confirming that the person's identity was stolen by the offender and other information that would help the victim explain it to financial institutions, credit providers, service providers etc.

This is the critical element.

Mr C.C. Porter: Which provision are you referring to?

Mr A.J. WADDELL: This is in the explanatory memorandum—the third point, explaining what an offence is.

This is the critical point, because when we think about identity theft we think about inconvenience. Somebody has made a fraudulent charge to my credit card and I must go through the effort of getting that reversed. Ultimately, who wears the cost? We assume that it is the big ugly corporation out there. We all know that ultimately that cost flows back to consumers, but within that larger corporate sense it seems to be a somewhat victimless crime. The problem is that it is not, because proving to these organisations that an identity has been fraudulently used and that the customer is not responsible for these charges can be quite a hurdle. This bill goes some way towards assisting people in proving that to these organisations.

I was the victim of a petty theft back in the 1990s. I left my suit jacket on the back of my chair and went to a meeting in the conference room of our office. I came back to find that someone had come quite brazenly into our office, searched through the various rooms, found my jacket and ripped my wallet out of the pocket. Even though I reported the theft within half an hour of its occurrence, for the next nine months I was inundated with statement after statement from my credit card company showing these $50 transactions. These people were smart enough to sneak under the radar. They knew that if they spent less than a certain amount, nobody would check to see whether the credit card had been stolen. This was back before things were quite as electronic as they are today. On top of that, they also took my Commonwealth Bank Keycard, as it was then, and walked into the Commonwealth Bank, forged my signature and withdrew money from my account—something that I certainly had not expected. It took me about six months to clear up the mess that was created for me, in replacing all the cards, changing everything, letting everyone know that I now had different numbers, and then having to go through every statement systematically, identifying which charges were mine and which were not. But I got off lightly.

Mr M.P. Whitely: It's good training for being a parent.

Mr A.J. WADDELL: Yes, I think it may be! I have yet to experience that, but I see it coming!

I was doing a bit of reading on this matter, and I came across an article that quoted Detective Senior Constable Rod Shelton from the Queensland police fraud and corporate crime group. He said that organised crime rings are now making more money from identity theft than from the drug trade. He goes on and explains some of the problems associated with identity theft —

> "It's very difficult. We estimate it can take two years and $20,000 to clear your name.

That is $20 000 out of one's own pocket to clear one's name; to go through the credit agencies and so forth to indicate that all of these transactions did not necessarily involve the cardholder. The article continues —

> While you might be able to clear your name, there can be little hope of catching the person who stole your identity.
>
> "If they're overseas, there's very little chance at all. With computers, email and the internet we just don't know who people are.
>
> "Depending on the international obligations of different police services, sometimes we can try to work out who it is, but most times we'll never know."

We need to acknowledge that we live in an extraordinarily complex environment. We, as a state legislature, can pass laws that impact here in Western Australia, but when we are dealing with international organised crime, there are limits to what we can achieve. There is therefore an obligation upon us to focus on the remedy rather than necessarily the criminalisation of the problem. The remedy here is to help our citizens recover from a fairly traumatic event. We need to do that by empowering the citizens to go up against large corporate entities. We

need to recognise that they will be dealing with organisations that operate by the numbers, by computers and by particular procedures that do not deal very well with people in unusual circumstances. We must look at it from the credit card providers' point of view. How are they to differentiate between somebody who just does not want to pay a bill and somebody who has a legitimate claim? We need to create a pathway to enable people to identify themselves as victims of identity theft and obtain a certificate to that effect that has the force of law and will make the credit providers stand up and take notice, so that it is not just a story that somebody is running up.

In my reading I came across the case of a chap called Roderic from the Gold Coast. He did not give his surname. It seems a lot of this sort of thing happens in Queensland. He was talking about an event that happened to him. He did not discover that his identity had been stolen until he received a letter from a car company congratulating him on the new car he had purchased, which was a bit of a surprise to him. He then found over the succeeding months that loans were being racked up against his name, mobile phone accounts were being opened and all sorts of things were happening in his name. He went on to say that the hands of the police were largely tied because they had to wait for the financial institutions to recognise that there had been an identity breach. He was not taken seriously for about two and a half years; he could not get anyone to listen to him. His whole life was, and sometimes still is, completely spent sorting out his identity. He lost his job, his marriage was under extreme stress, and he estimates that it cost him over $10 000 to clear his name.

I came across another report on the effect of identity crime. It reinforces the point that this is not a victimless crime, and it is a crime that reverberates long after its initial occurrence. It is very traumatic for people who have had a very good credit record to suddenly have a collection agency hounding them to prove that they have done nothing wrong. They are having the usual collection agency tactics used on them, because the agencies are used to people disowning their debts. Victims of identity theft really have no experience in dealing with that type of problem. For up to 20 per cent of people who suffer identity theft, it takes about two years to work out that it has actually happened. I have been guilty of not really monitoring very closely what happens on some of my statements, and not noticing a dollar out here and there. I sometimes wonder what a particular entry was for, but it is not worth a phone call to sort it out. Only in the second or third month might a person notice something unusual on his account and decide to do something about it. I am led to believe that some people never look at their account statements.

It is this secondary wounding of identity theft that is of critical concern to me here. People will experience continuous interaction with financial institutions and various debt collection agencies trying to indicate that they have done something wrong when they have not. It can really damage their view of themselves and it can damage relationships. Their families are often not particularly supportive; their work life is affected and they are unable to carry out normal activities. Trying to get a bank loan with a bad credit rating is very difficult. We really need to consider that, and that is an appeal for us to do something as fast as we can. This is a plea to the Attorney General, if he feels the need to proceed with his own legislation in the place of this bill, to consider the question of certification of identity theft, so that we can arm our citizens with a tool to combat the problems they face in proving to the banks and various other agencies that identity theft has happened.

We must also be cognisant of the fact that technology moves extremely quickly. Banks will say that they are secure, and that they are putting new chips on cards and all those sorts of things. That is all well and good. I remember when I visited the United Kingdom about four years ago, I rocked up with my Visa card to buy some fuel. I was quite surprised when I was asked for a personal identification number. I said that I did not have a PIN; I just press "OK" and away we go. We now have PINs here in Western Australia. However, I saw that the UK had introduced something much earlier than we had in that instance. The UK had to accommodate the fact that it was operating in a global environment. In our situation, the lowest common denominator tended to rule, which was no PIN, no protection.

Even though these security features are put on our cards, we need to recognise that often it is a marketing exercise by the banks to give us a sense of security. The security does not actually exist. I challenge people to use their credit card to pay for their next purchase and sign "Mickey Mouse" for it. I guarantee that the majority of those transactions will pass. That is because we, as a society, are not thinking about security and identity theft as a real problem. We take it all for granted that it will work out in the end. Unfortunately, it is only when we are victims that we realise it does not always work out for the good.

MR W.J. JOHNSTON (Cannington) [4.31 pm]: It is not my intention to speak for long on this bill, but I want to commend the member for Mindarie for bringing both the previous bill and this one to the house to deal with issues that are important in the community. Identity theft is clearly recognised by the community as a major issue. We can read about situations that are quite complex. For example, people assume an identity, not to notch up minor transactions on a credit card, but to create a bit of a credit history so that they can get a mortgage to

purchase a house. That major step is what they are after, so they can create that other identity to do something very large—not just notch up $20 or $40 on their credit card when they pay a bill.

When the McDonald's scam became apparent, I think it came as a real shock to people in Perth to learn that the arrangements that financial institutions have for the security of our identity were not as effective as people thought they were. The member for Mindarie, who had come to deal with this issue at an early stage before the matters highlighted in that case became apparent, has demonstrated the way in which he is approaching his role as the shadow Attorney General. He wants to be ahead of the game on these issues and make sure that proper protections are in place.

I listened with interest to the Attorney General's answers in question time today. If he makes a contribution to this debate, I will be very interested to hear from him about how the arrangements that are proposed in this bill can be improved. I have not heard anyone say that the arrangements in this bill are not worthy; it is just that they could go further. If the Attorney General wants to bring additional steps to our attention, we would all be very happy to consider them. Of course, to say that we can do more is not a reason to do nothing. Unfortunately, early this year the Parliament decided to not do anything, and we then had the situation that arose subsequent to our decision to take no action.

I have a friend who works in the information technology industry at a very senior level, and he does not use any internet banking because he believes that the security arrangements on internet banking are too weak, even though that is his profession. He is a successful person who has worked at a very senior level for various companies. I will not name them, because they might get embarrassed about their executive selling their services in this area but not personally using those services because he believes the arrangements are inadequate. These are serious issues, and the community needs protection.

Australia was one of the early adopters of EFTPOS and credit cards. We were a leader in that regard. I remember visiting the United States in 1985. By that time, people in Australia were very used to using plastic cards, not just as credit cards, but to access their bank accounts. When I went to the US, people still could not effectively transact from one state to another. If a person banked in California and went to New York, he could not do any daily banking transactions in New York because the banking system in the US was so fragmented, whereas in Australia, even by 1985, we were very used to the idea that no matter where we went in Australia, we could transact our affairs. It is a huge benefit to the community to have the ability to go everywhere and use not just credit cards, but our own money as we proceed. However, I believe that people have a high expectation of the security arrangements, and it is true that those security arrangements are not as good as they should be.

I will listen with interest to the Attorney's criticism of the bill, but it appears that what he is saying is that we are not going far enough—not that the steps we are taking are not worthy, but that somehow we have not gone far enough. I say to the Attorney that we now have the opportunity to do what should have occurred earlier this year. We will support this legislation and go further in the future. That would be welcomed by me and, I imagine, by others. Alternatively, some amendments could be proposed to improve this bill if the Attorney thinks that we need to go a bit further. Either way, I think that the community can recognise that the Labor Party is ahead of the game on this issue. In Parliament, we were raising the issue of identity theft before it was something reported on in the popular media. It reflects the energy and the effort of the shadow Attorney General that the Labor Party got in front of the media circus on this issue. Therefore, I commend the bill, and will wait with interest to hear what the Attorney says.

MR C.J. TALLENTIRE (Gosnells) [4.37 pm]: This bill is one that I support wholeheartedly. It is certainly one that has come ahead of the sorts of concerns that people in my electorate have been expressing. In essence, the bill is about government playing its part in maintaining consumer confidence in our banking system. People who have come into my electorate office have told me about the misfortunes they have suffered, the concerns they have and how they now prefer to use cash. They are losing confidence in all the good points of our sophisticated banking system, with its strong emphasis on technology. That is why this legislation is so urgently needed.

One person in my electorate office told me about her experience and how she was able to trace things back and eventually realise that her problem was probably due to transactions she had made at McDonald's a few weeks before. Her credit card had been used by someone else. In one instance the amount was $109, and on two separate occasions after that the amount was $436.35. It seemed from the statements that the perpetrator of this theft was located in the city of Montreal in the Canadian province of Quebec. Fortunately, her bank was able to reimburse her very quickly—within about two and a half weeks. I have been looking at some announcements by the Australian Bankers' Association. It realises just how dangerous it is that the community perception of the security of our banking system could get so seriously undermined by these sorts of problems. Therefore, the Australian Bankers' Association has taken it upon itself to make sure that people are reimbursed as quickly as

possible. That is the industry playing its role, but clearly government must play its role too. This legislation is responding to that. As the member for Cannington was saying, the member for Mindarie, our shadow Attorney General, is to be commended for his foresight for getting ahead of things and having this legislation ready to go before this problem had grown to the proportions that we now see in our community.

I think the advice from the Australian Bankers' Association is a salutary reminder of just where this could go. As I say, at the moment the banks seem very prepared to reimburse people as quickly as possible, but they are giving people advice to take action to ensure that this does not happen to them or to mitigate or reduce the extent of possible financial loss. The banks are also suggesting that people should in fact lower their credit limits. That is a good thing for some people. I know that many of us receive letters from financial institutions urging us to increase our credit limits, and perhaps that is because the banks like us to spend big on credit cards and then have big interest bills to pay, which helps their profitability. However, the message is now going the other way. Perhaps people should reduce their credit limits so that if their identities are stolen, they will have a ceiling on the extent of the losses that they might incur. I think that indicates how potentially serious this problem is and how urgently we need this legislation.

Another aspect that has come up in my electorate is that people are saying that not only are some retailers or fast-food outlets notorious places for skimming devices, but also this problem is manifesting in some shopping centres as a whole—it is the virus-type concern that people have. I have heard from retailers in shopping centres in my electorate that word is getting around that there may be skimming devices in their shopping centres, and as a result they are seeing a reduction in patronage. Therefore, the Criminal Code (Identity Theft) Amendment Bill (No. 2) 2009 is a very serious piece of legislation that needs to be passed as quickly as possible so that we can ensure that our commercial and banking sectors are not undermined by something that could be a real threat to the profitability of both small and big retailers. Indeed, I gather that the rumour going around on one website was that skimming devices were rampant in the Coles stores. I do not know what Wesfarmers was able to do to counter that; probably its best tactic was to keep relatively quiet about it. The last thing any retailer wants is that kind of bad publicity. I think we need to acknowledge that the banks are trying to do their bit, which is seen when they make rapid restitution to customers who have amounts debited illegally from their bank accounts or credit cards.

I commend this bill to the house and I look forward to hearing from the Attorney General about the details that he is talking about. I understand that he has some interest in transmitting devices that are associated with skimming devices. No doubt there are ongoing technological changes to skimming devices that mean that the legislation will have to evolve in time, but I think that, more than anything, we must have good legislation in place as quickly as possible.

MR J.M. FRANCIS (Jandakot) [4.44 pm]: I will keep my contribution to the debate on the Criminal Code (Identity Theft) Amendment Bill (No. 2) 2009 fairly short, but I want to make a couple of points and tell my little personal stories on these issues.

Ms J.M. Freeman interjected.

Mr J.M. FRANCIS: No, the member is starting to believe in conspiracy theories!

My first story happened in about 2003. I remember I was at HMAS *Creswell* and I was buying a new laptop from Dell online. My mum and dad lived up the road in New South Wales, and for whatever reason I gave mum the money and asked her to put it on her credit card. We had the choice of buying this $2 000 laptop—it would have been the second half of 2003—by giving the credit card details over the phone or using Dell's online order form. Much to my own silliness I said, "I'm not quite sure if online is the most secure way of doing it; let's do it over the telephone so that you know you're speaking to a real person." I can tell from members' faces that they know where this story is going! Of course, this is Dell—it has one-third of the world's retail market for computers. It is a reputable company, so I thought that surely I would have nothing to worry about. We rang and gave the credit card details over the phone, and $2 000-odd came out. The great thing about Dell is that people can watch their laptop get built, so to speak; they can track it online and monitor the assembly and the shipment. People can also customise the size of the hard drive and all those things. Two days later I went to use the credit card and, sure enough, it was over the limit. I thought that was a bit strange; there should have still been a few thousand dollars on it. We rang the bank and we found out that there was another transaction for exactly the same amount made to some Russian mafia company in France somewhere. Clearly, some guy who worked for Dell in Malaysia was writing down credit card details and of course Dell refused to have any liability for it—Dell did not want to know about it. However, it was interesting that it was exactly the same amount of money to the cent.

The second great story, which is a little more embarrassing, happened this year. I have a Visa card —

Ms J.M. Freeman: So you learnt nothing from the first experience!

Mr J.M. FRANCIS: This one gets better! I had a Visa card and I started —

A government member interjected.

Mr J.M. FRANCIS: I do not know whether I should be telling this story in Parliament! It is almost like my stories last night about the metal lights—halides—above the fish tanks and the police thought I was growing marijuana!

A government member: You know you are in *Hansard*!

Mr J.M. FRANCIS: I know. Anyway, I am not one of these people who religiously check their credit card statements. I am religious but I do not go through my credit card statements every single month; I just have a quick scan of them. I did notice that for the past 12 months an amount had been coming off my Visa card and I noticed that generally it was the same amount, but the company had changed and it was an American phone number. Of course I tried to ring this phone number and I suddenly realised that I had no idea what this $71, or whatever, that was coming out of my credit card every month was for. I thought that I had better find out. The weird thing is that when people put in a claim because someone has been taking money from their credit cards illegally, there is a three-month statute of limitations. The credit union that I bank with could only investigate and repay me for some very dodgy porn site taking my money, which I can absolutely assure the house I have never visited in my life!

Several members interjected.

Mr J.M. FRANCIS: My wife knows about it too—trust me! The site had been taking $71 —

Dr M.D. Nahan: What was this dodgy porn site?

Mr J.M. FRANCIS: I can tell the member for Riverton it was in the United States. I was hoping he might know more about it than me!

The point I am making is that I was in this position in which I guess $500-odd had been stolen from my Visa card over the past 12 months. There was nothing I could do about it other than to lodge a claim. I did get the last three months' worth credited back to me—$200-odd—but I had to write the rest of it off. The most frustrating thing about it is that I use this credit card regularly. My car insurance, internet access, mobile phone, health insurance and all those things are paid for with that one credit card, which is probably why it slipped through the keeper for so long. I have no idea how those people got my credit card at the end of the day. The only way I could stop it from happening was to cancel the credit card and get a new one. That means that every so often I get a phone call from someone to say, "You have not paid your health insurance this month—your credit card has been rejected"! I have to say, "That is right, because I have changed the credit card details." I am finally sorting this nightmare out.

The point is that people are stuck in these situations, and I sympathise wholeheartedly with people whose details are stolen and whose details are scammed. It is morally wrong to steal someone's money, and the people who do so put other people to great inconvenience in their lives through no fault of their own.

Ms J.M. Freeman interjected.

Mr J.M. FRANCIS: It has occurred to me. I have given it some thought because I have just been through this in the past few months. Luckily enough, it was not identity theft as such; it was my credit card details. My whole identity was not stolen. To this day I have no idea how the details got out, but ever since, I have to say, I have been far more cautious about how I use a credit card. Ever since my 2003 experience I had this faith that the safest way to use a credit card was online; never again would I give numbers over a phone, especially to someone in a foreign country. Unfortunately, the great people at McDonald's Cockburn—up the road from my electorate—have found that theirs has been one of the more targeted McDonald's. People have skimmed information off cards onto data machines. I am aware that that is still subject to an ongoing inquiry, so I do not want to speculate on exactly how it was done. I have had a change of heart from saying, "I'm not going to provide my details over the phone anymore; electronic transactions must be perfectly safe", to now taking very good care and giving great consideration when using a credit card electronically and online.

I, like the member for Forrestfield, like to shop online. I have 252 points of feedback on eBay! I normally use PayPal and I have never had a single problem with PayPal. I think it is an outstanding company. It provides brilliant insurance for people who make transactions online.

An opposition member interjected.

Mr J.M. FRANCIS: No, I am not on its payroll! We now have to start being very careful, because people who are motivated by greed, who are a bit more IT savvy than the rest of us, get up to all kinds of shenanigans to get hold of our money. One does not have to be very IT savvy to be more IT savvy than me! I am a bit of an analog man in a digital world, I suspect!

Having been through these two experiences, I sympathise greatly with others who have suffered similarly. I am still not sure what the answer is. My credit union, which was bound by the rules of, I guess, Visa, provided excellent service in getting my money back, but only for the last 90 days. Unfortunately, any transactions before that were basically written off. The only way out of it was to cancel the credit card. I sympathise with what the member is trying to do, but I am not sold on whether it is the right way to do it. I will be listening with great interest to the rest of the debate. It is something that is a bit close to my heart through personal experience. Although I sympathise greatly with the intent of the member's legislation, I am cautious about the way we should go about dealing with this matter. I will be paying very close interest to other members' comments.

MS A.R. MITCHELL (Kingsley) [4.55 pm]: I rise to indicate that I will not be supporting the Criminal Code (Identity Theft) Amendment Bill (No. 2) 2009. It is not because I do not support the intent of the legislation, because I actually believe that something needs to be done, but I am confident that the legislation that is being prepared by the Attorney General will be more comprehensive and probably prepare us better for the future than what is proposed in this legislation.

There is no doubt that identity theft is a very frightening experience. It is very traumatic and it is something that leaves one very scared about what is going on around us. I have to be honest and say that I am very fortunate that I have not had any experience of these sorts of things. But talking with people that have, I sense the utter despair of the realisation that someone has taken information about them. Unfortunately, once upon a time a person could probably say to others, "Were you careful with that product? Were you careful where you left your valuables? Were you careful about where you made a transaction?" Nowadays it is completely different. Nowadays it is not about whether I left my handbag on the front seat of the car or whether I left my diary open that had all my codes to get into certain accounts. It is much more sophisticated than I can comprehend. I am probably a bit like the member for Jandakot—I am not into that world—although, I will be very honest, I use a lot of those facilities because it is convenient and easy. I am also, probably similar to the member for Jandakot, not the sort of person who double-checks everything all the time. I do not go through my credit card statement every month. I am sorry, but I never have. I have multiple credit cards. I have multiple codes that I need to remember. I do not always remember them and I have got them listed in a place that I probably should not. But they are the sorts of things that we now have to be conscious of, because this whole situation has turned around so much.

As I said, I am very fortunate that I have not personally experienced identity theft. I have travelled much. I have made sure that I have done the best I possibly could when I have been travelling. I have made sure that I have used hotel safes. I have been fortunate to stay in hotels that have safes in the rooms. I have used such facilities so that I could protect myself as much as possible. I tend to be a very careful person. I make sure that the things that I need are close by me at all times—basically under my arm. People laugh at the size and weight of my handbag, but I say that my life is in my handbag. My protection is to have it with me the whole time. Having said that, it is not with me at the moment; it is in the office! It is those sorts of things that I try to make sure I do. What goes on in the wider world is far beyond me. I think it is a great risk when people do not understand what is happening. That is why I said that I support the intent of the proposed legislation but I am not going to support it because I believe the Attorney General is preparing much stronger and more comprehensive legislation.

If we think about what we need our identity for, there are very few places one can go that some sort of proof of identity is not required. Photographic identity is the obvious. How many times do we have to give a code? How many times do we have to give something else? Perhaps I had better talk about myself. How many times are we asked on the phone, "What is the code?" I say, "Can you give me a clue?" because it will be one of a number that I have. How many times do we say, "Just use this"? I am sure that if anyone really wanted to, they could work it out. There are not many places we go to now where we do not have to produce some form of identity, whether it be verbal, visual or any other. Passwords and codes are constant.

Those sorts of things are going to be a big part of our future. That is why I believe that it is really quite essential that we develop legislation that will be prepared for the future, and not quickly adopt something that sets us back—I think the Attorney General used the phrase "the 2003 version". I think it is very important that we work towards getting the best legislation for this situation now and that we do not rush something through that is not quite right. I have been assured by the Attorney General that the legislation that he is preparing is very, very close to being ready; hopefully it will be ready within the next week. For that reason alone we should make sure that we get the best legislation, not just quick legislation. I commend the member for Mindarie for doing

something along these lines. However, we have the opportunity to make sure that we get the legislation right; hence, I have chosen not to support the legislation in its current form but to wait and see if we can get the best one. As I said, our identity is what we are about, it is something we must protect, and it is something we must put a lot of time and effort into making sure that we protect people in society. Obviously, they have to do some of their own work in their own protection factors, but we also need to make sure that we get the best legislation to protect those people.

MR J.E. McGRATH (South Perth) [5.00 pm]: I will take just a few minutes, as the member for Wanneroo is very keen to speak on this amendment bill put forward by the member for Mindarie because I believe the member for Wanneroo has been a victim of card skimming.

I am a person who uses credit cards. I have a credit card with just about every bank that offers them. I have always lived by the rule: why use your own money when you can get credit? Sometimes that is a good thing and sometimes it is a bad thing. However, it is a concern to see that credit card skimming has extended around the world. Some years ago I told my wife to be very careful when she used an automatic teller machine. The biggest fear back then was about being mugged. There were a lot of incidents of people, particularly females, being mugged at ATMs. We were warned about not using ATMs unless someone else was around and to be careful about using them in fairly quiet spots at night and times like that. Now, with modern technology we have seen the rise of this far more insidious crime of people getting the details of people's cards and getting into their accounts.

I am also a bad money manager in that I do not check my bank statements, which my wife continually reminds me about. I am inclined to just look at the bottom line and think that things are going okay. I would not know generally what was going in and out of those bank accounts, and I suppose my credit cards are the same. I think I am saved by the fact that there is very little credit in most of my cards; therefore, if anyone got hold of them there would not be much at the end of the rainbow. I always say that if I keep the balance close to the limit, there will not be much there for skimmers. That is my safety net.

I have been reading a bit about skimming as I have been listening to the other speakers. We do have to be careful. There are various steps that we should be aware of and we should take. We need to be ever vigilant. I recommend that people look at the internet and google card skimming, as I have done. There are many warnings for consumers. Some of the top warning signs, for instance, are: when shop assistants take a card out of the sight of a customer to process a transaction; when people are asked to swipe their card through more than one machine; when people see a shop assistant swipe the card through a different machine from the one they have used; when people notice something suspicious about the card slot on an ATM, for example, an attached device; and when people notice unusual or unauthorised transactions on their accounts or credit card statements. I guess most of us would have noticed when we have checked our statements—this happens often with credit cards—that a quite different name appears on the statement from the name of the organisation we bought something from. I have wondered where I have spent $275 and then realised when I finally checked the statement that I had bought something at a franchise and it was processed through a name I did not recognise. I think, therefore, that we are all aware that we have to be careful in this world of credit cards. The risk that we are talking about now is one that has arisen because skimmers are very clever. The internet has allowed them to work on an international basis. People can be scammed from any other country, as the member for Jandakot has experienced.

Other advice is to keep credit cards and ATM cards safe by not sharing personal identity numbers with anyone; do not keep any written copy of the PIN with the card; check bank account and credit card statements when they are received; if a transaction cannot be explained report it to the credit union or bank; and choose passwords that would be difficult for people to guess. People can often, for example, guess someone's birthday or someone's wife's birthday. If I had played in the 1969 grand final, that might have been an obvious one. I did not quite get to that level.

The member for Mindarie is obviously very keen for this amendment bill to be accepted. I am confident that the Attorney General, with whom I have discussed this matter, is aware of a very acute problem here. I believe that some legislation will be coming into the Parliament, possibly as early as next week, and I am very keen to support that legislation. At the same time, I understand that the member for Mindarie in opposition has foreseen a problem and has been very keen to put some protective measure in place for the people of Western Australia. As a government, however, our duty is to make sure that the legislation that comes forward is the best possible legislation, that all the boxes are ticked and that we bring in penalties for people who insidiously steal from unsuspecting Western Australians. We need very strong penalties; we need to make it as difficult as possible for people to commit this offence; and we need to make sure that we have the best possible methods for tracking down the people who commit this offence. Once people are apprehended for identity fraud, we must have proper

penalties in place. I am therefore confident that the Attorney General will do that and we will see some very positive and forceful legislation presented to the house in the next week or so.

We in this house, including members on the other side who have spoken in this debate, acknowledge that this is a serious problem. There is no getting away from the fact that we live in a world of high technology and people are often asked to produce proof of their identity. I do not think there are any secrets any more. Most of us do not have many secrets about our credit or business transactions or about our tax file numbers and things like that. The days of total anonymity in that regard are well and truly gone. I personally have no problem handing over some of that information. However, at the same time, we need to put in place the highest form of protection so that the average person can be reasonably confident that he will not be caught by the crime of identity fraud . I will be interested also to hear what the Attorney General has to say later today. However, I would now like to hear from the member for Wanneroo, who I believe has some first-hand experience of identity theft. The member for Wanneroo is obviously a far more affluent person than I am, as someone has obviously targeted him as a person who had plenty of spare cash! I am sure the member for Wanneroo will be able to make a contribution to this very important subject.

MR P.T. MILES (Wanneroo) [5.10 pm]: I am reminded of that old joke we used to tell about the bank manager ringing a person up and telling him that the bank had found out that his wife's credit card had been stolen, and when the person finds out how much the thieves have been spending, he says that they are spending less than his wife! The incident I will relate to the house happened after a Wednesday evening sitting of the house. I got home, made a cup of tea and sat down, and at about 9.30 pm I got a phone call—which I thought was very odd.

Mr J.M. Francis: Did you have sugar in your tea?

Mr P.T. MILES: No, I do not have sugar in my tea, but I have a proper pot of tea, not your scabby dippy-dippy teabags!

Mr J.M. Francis: That's very English of you!

Mr P.T. MILES: Yes.

I received a phone call from a representative of the ANZ bank, who told me that their security system—namely, Falcon—had detected a transaction in Italy that night for a large amount of money. Unfortunately, I am very similar to the member for South Perth in that my bank accounts are very scarce of money. Living in a marginal seat, I tend to spend it as fast as it comes in.

Dr M.D. Nahan: Not overloaded?

Mr P.T. MILES: Definitely not overloaded; overdrawn, maybe! The thieves had been unable to withdraw money.

During the phone call the bank representative asked me where I was, and I said I was sitting in my lounge room, having a cup of tea. They asked if I was in Australia or overseas; I told them I was definitely in Perth.

Mr J.M. Francis: They didn't ring you on your home phone?

Mr P.T. MILES: No, no, they rang me on my mobile.

I told them I was at home, having a cup of tea and trying to catch up on some relaxation, and they told me that this event had happened 15 minutes prior. Fortunately, the transaction had been unsuccessful, but it caused a lot of aggravation for me and my wife because the debit card, not the credit card, was skimmed. If that happens, the bank immediately freezes the account and cancels the card, and basically the person has to start again. As we all know, that means we cannot use either internet banking or phone banking. Fortunately, I had no money in the bank anyway, so it did not make any difference for the couple of days until another emergency card was sent out to me. The bank really did well and I congratulate it for the security services it has in place.

However, once we had gotten through that initial half-hour of the phone call, the bank also wanted to know roughly where I had been using my card. As members of Parliament, I do not think too many of us in this house remember which automatic teller machines or EFTPOS facilities we use, or which banks we use.

Dr M.D. Nahan: I do!

Mr P.T. MILES: Does the member?

Dr M.D. Nahan: Yes.

Mr P.T. MILES: That is why the member has more money than I do!

Between us, the bank employee and I worked out that the card had been skimmed, funnily enough, in the member for Mindarie's electorate, at the Clarkson ANZ ATM at Ocean Keys. The bank representative then

proceeded to tell me what I should look for to avoid this happening again. Basically, if there is no flashing light by the slot where the card is inserted, do not push the card in, because it means that there could be a device over the top of it and that somebody is skimming or photographing the card and all the rest of it. The bank then emailed me some pictures and asked whether I had seen this or that; I did not know because it was too long ago. The bank reckoned that the data had been captured on the Sunday, and by 9.30 pm on the Wednesday—our time—the thieves were using the card in Italy to access my bank accounts. In this electronic day and age of emails and systems, they do not need to do too much to get some of our money.

Mr J.M. Francis: Did they get your details from the ATM or because of an EFTPOS transaction?

Mr P.T. MILES: At that point they did not know whether it was an ATM or an EFTPOS transaction, but it was done electronically. They had a card.

Mr J.M. Francis: So the money was not taken out of an ATM and put into someone else's account?

Mr P.T. MILES: No, they attempted to use a forgery of my card at an ATM in Italy.

Mr J.M. Francis: So they skimmed the details of your card and made a replica card?

Mr P.T. MILES: Yes.

Mr J.M. Francis: They recorded your personal identification number and magnetic strip and made a replica card and used that in Italy?

Mr P.T. MILES: That is correct; yes.

Some credit card companies and banks now produce cards with little microchips on them. I had thought that people who have one of those have a fairly good chance of not being skimmed. But after what happened to me, I do not trust any of that any more.

During my time on council we had a bin outside for all our council papers—all the bills and acts and all that sort of stuff. Because we got so much of it, we could not just put it in the normal recycling bin; we were actually provided with a secure bin. That was done because a couple of City of Wanneroo councillors had been visited in the night by people who had taken documents from those bins. We then had to start leaving those bins inside our garages. Time and again we hear the police telling us to take care with our identity and to ensure that we cover our hand when we are keying in PINs on the doors to our offices or at ATMs. I am probably one of the ones who knows what I am supposed to do but does not do it because I am always rushing from A to B. Not only that, even my five-year-old knows my ATM PIN. He also knows his mother's PIN, and he even knows her iPhone number and how to get into that, which is even more of a worry because he keeps downloading games!

Mr I.M. Britza: And he's five years old?

Mr P.T. MILES: He is five years old. The member has only got a two-year-old, so he has three more years; start saving!

We should also take care with what we put in our yellow recycling bins at home. I bought a shredder to use at home and I shred my bank statements and all the rest of it. We have to, and we have to convey that very important point to everybody, because there will be somebody who will want to try to take something from us.

Dr M.D. Nahan interjected.

Mr P.T. MILES: We do not need bank statements for that.

Dr M.D. Nahan: Yes, you do.

Mr P.T. MILES: No, we do not—go and see the member for Carine; he fixes it!

I have read through the Criminal Code (Identity Theft) Amendment Bill (No. 2) 2009, and I have also spoken to the Attorney General about it. I think the intent of the bill is quite clear and quite good, but it does not quite go far enough. We know that if we get a very good lawyer—we know that the member for Mindarie, who is not in this place currently, is sometimes a very good lawyer—that lawyer will be able to find a clause to get somebody off, if need be. There are some holes in this bill, and I understand that the Attorney General wants to fix those problem areas. It is not just about the collection of data from our ATM and bank cards; it is also about transmitting that data by mobile phone or email, or any other means that will enable the data to be sent across the world in days, resulting in the loss of people's funds.

To further safeguard my accounts I have limited the daily withdrawal amount to $1 000. That can become an issue if two people go shopping separately and then decide to go out for dinner that night. They might be unable to withdraw any money because they have spent over the $1 000 for that day. But I would rather work around that than get skimmed again and take the chance of losing money. Fortunately, I did not lose any money, but the

biggest problem was that it was about a month before I could get all my systems back online, such as my banking details, phone banking and all the rest of it. That is the important thing. I think we need explore that further, and I understand that the Attorney General will talk to us about that a bit later.

Members should remember that it is also important to not leave stuff in their cars. I was at a residents' meeting on Monday night in Banksia Grove. The Neighbourhood Watch lady told the residents that kids are walking through the neighbourhood, and that, first of all, they try the door of the car, and then they look though the window into the car. Quite often we pay a bill and leave it on the front seat of the car. Everybody has a mobile phone with a camera, making it easy for somebody to take a photo of our bank details and then take the mobile phone. Also, people might go to somebody's house and look through the bin for personal papers so that they can start accumulating the data to steal the person's identity and then steal money. That is how it is done. They can get a birth certificate and a few other personal details, although I do not think that people always need to show their birth certificate to prove their identity. As long as a person can prove that he is paying some utility bills, he can get credit at some of the large department stores.

When it comes to personal data protection, perhaps some advertising should be undertaken. It is hugely important to mums and dads, who do forget when they are picking up their food at the local IGA or Coles, depending on where they live —

Mr C.J. Barnett: Or what time of the day it is.

Mr P.T. MILES: I was wondering whether the Premier would come in there.

Members will notice that the bigger stores, including the IGAs, are putting the EFTPOS unit up high, allowing everybody to see the PIN that a person is keying in. I understand from the recent McDonald's case that people were skimming and taking the data from people's cards and photographing people keying in their PIN. As a consequence, they are able to steal those unsuspecting people's money later. With the McDonald's situation, what made it an easy crime, which the offenders got away with for a long time, was that they were stealing small amounts of $9 or $10. People would not really notice whether they had been skimmed for $9. If such a transaction was made every couple of weeks, the person would think that either he or his wife had just bought a burger. It costs about $10.45 for two burgers and a coke.

I am now leading up to the point that it is McHappy Day this Saturday and I will be flipping burgers with the guys at the Wanneroo McDonald's store, which I frequent a lot because it is the best place to find Sergeant Bob O'Sullivan, who is the police officer for the area. The Minister for Police is not in the house, but Bob O'Sullivan is excellent on issues of crime prevention and getting down to the nuts and bolts of what is going on in the community.

I will draw my comments to a close and allow other members to contribute to the debate. I ask members to please start observing where they leave their credit card details, bank statements or whatever. Whilst we trust our friends, we need to be vigilant about where we leave our credit cards and bank statements in our home. We have been reminded a few times that we now find ourselves in a different situation. None of us is rich by far, but people think we are and will try to steal our identity if they can to ascertain what we have or to steal what we have.

MR A.P. JACOB (Ocean Reef) [5.23 pm]: I will very briefly follow on from the member for Wanneroo's comments in praising Sergeant Bob O'Sullivan, who is an excellent local police officer. He works very hard in the area and I add my compliments to those of the member for Wanneroo. He writes a column in the local newspaper and frequents as many Neighbourhood Watch and residents meetings as he possibly can.

I refer now to the Criminal Code (Identity Theft) Amendment Bill (No. 2) 2009. Identity theft is a very complex and fluid issue; it is constantly changing with information technology. Almost everyday we can say that there are newer and more readily accessible means through which people can illegally appropriate somebody's identity.

I would typically like to think I am somewhat insulated or protected from this problem, but not because I am diligent in observing my credit card statements. I am as guilty of being lax in that area as is the member for Jandakot. Perhaps it is mainly because my wife keeps a very close eye on the accounts via the internet. That is not because she is worried about identity theft, but because she is the budget master and watches my spending quite closely.

Mr C.J. Barnett: She is worried about you.

Mr A.P. JACOB: She is worried about me, the wise young lady that she is. She monitors our accounts very closely. Often if I have made a transaction I receive a phone call within half an hour. I feel secure in knowing that somebody is watching my accounts very closely.

A government member interjected.

Mr A.P. JACOB: She is indeed my falcon. I will probably be in a lot of trouble for saying that, because she reads what I say in *Hansard*. She watches me very closely.

Several members interjected.

The ACTING SPEAKER (Mr P.B. Watson): Members, I know it is a happy group on the government side of the chamber, but it is very hard for Hansard when members are talking and laughing. I ask the member to address his comments to the Chair.

Mr A.P. JACOB: My point is that even though I have a very diligent person in my household keeping an eye on our accounts, we are clearly still fallible, and I can say that after hearing the experiences of other members.

I am sure that all members have been contacted at some point by a Nigerian prince or some such person via the internet who wants to deposit millions of dollars into their bank accounts.

Mr C.C. Porter: His name is Bruce.

Mr A.P. JACOB: I thank the Attorney General for mentioning his name, because I came very close to being caught out. It was quite distasteful actually, given the timing. A couple of years ago I had an email from the Congo. It was bizarre. A lot of these people randomly type in names of people and one of them typed in my name, Albert Jacob, and sent a message saying that I had a connection with the Congo. This particular email talked about the estate of an Albert Jacob from Congo and asked me whether I would like to claim it. Members can laugh, but we all get emails of this sort, because these people apply them to the law of averages. However, I stopped and read this email, because my father was actually born in the Congo. My grandfather worked there for decades and I am named after my grandfather. My grandfather was Albert Jacob and he worked in the Congo. I read that email and took it seriously for a minute—probably for more than a minute. But given that it was a Congo email address, I thought that it was unlikely. I think I made a wise decision not to follow it up.

A government member: It could have been real.

Mr A.P. JACOB: It could have been real, but I would rather not take a risk. Members can see how easy it is to get caught. If these people send out a thousand emails, what does it matter if they get only a 0.1 per cent hit rate? It is only an electronic process. My point to this story is that there is no limit to the creativity that these people can apply or to the changes to technology. Whichever way a program can be written, somebody will seek it.

One part of this bill that I question is proposed section 440F, which excludes an attempt to commit an offence. Many of the perpetrators of internet thefts or email chains will be outside our jurisdiction. No doubt many of them live overseas. However, it is possible to set up an overseas email account from Western Australia. When the government drafts its legislation, it should consider the inclusion of a provision to deal with an attempt to commit an offence so that we are not waiting for these people to get a hit. If somebody is working from a computer down the road and is building up a Nigerian email address to try to get people's identity through the internet, how long do we wait for that person to pick up somebody's identity and run with it? I am not a lawyer, but I do question proposed section 440F of this legislation.

This is a very complex area of legislation and, as such, it should be as thorough as possible in the first instance. Given that the Attorney General has flagged that he will be drafting a version of this legislation using government resources, I am more than happy to express my strong support for the intent of this bill. However, I will vote against this bill because there is an opportunity to use the resources of the Attorney General's office to introduce a watertight bill so that we can get around this issue and provide protection for years to come.

MR C.C. PORTER (Bateman — Attorney General) [5.29 pm]: My contribution will be to talk about some of the legal aspects of the Criminal Code (Identity Theft) Amendment Bill (No. 2) 2009 and some of the legal aspects of the government's bill, which, as has been correctly indicated, will be in the house shortly. One thing that struck me when I have spoken in this place on matters involving legal principle is that members' attention spans become somewhat short. I have been trying to work stratagems around that. It occurred to me while I was listening to the contributions to this debate that I did lecture in criminal law at the University of Western Australia for two years and, similar to many of members present, the students often showed something of a short attention span. I would hit that 45-minute mark, papers would rustle and there would be a blank face competition staring back at me and I would have to try to find some way of amusing the students to try to get my point across. I thought I would do what I did with my students and tell a story that I used to tell them to try to illustrate a point that is pivotal to the issues that are meant to be dealt with by the member for Mindarie's legislation and that will be dealt with by the legislation that the government will put before the house shortly. It relates to the issue of attempts—attempts to commit offences. What would be the case, members of the house, if the police, for one reason or another, in a lawful search went into a house full of people who perhaps were from the Congo and they found an enormous amount of equipment, the sort of equipment that looks like it has come from a

Tandy store? The police knew that these were people of low repute, and they had fairly strong suspicions that this equipment was going to be used for the purposes of placing a device in a McDonald's EFTPOS machine or a skimming device over an automatic teller machine. What would the police do without the laws that have been proposed by the member for Mindarie and without the laws that we will shortly bring to this place? Generally speaking, they would charge those people, or seek to build a brief against those people, for attempt to do another offence—an attempt to steal, for instance, the stealing being the taking of money from someone's bank account.

The law is very particular about how attempts work and what one has to do and not do to be charged with an attempt to do another offence—an attempt to murder, steal or whatever it might be. I will give an example that I think will illustrate that and that government members, being all good conservatives, will like very much. It is an example involving a fellow named John Stonehouse. John Stonehouse had a trade union upbringing. He joined the Labour Party in the United Kingdom at the age of 16. He was educated at Taunton's College, Southampton, and later at the London School of Economics and Political Science. He was an economist—apparently a very, very good one—and he became involved in a cooperative enterprise and was a manager of an African cooperative society in Uganda. That is interesting but it has nothing to do with his later fraudulent behaviour. He was then elected as a Labour member of Parliament in the House of Commons in 1957 in a by-election. He was the member for Wednesbury. He had previously contested a range of seats before that. He served as a junior minister for aviation, then in the colonial office and then as Postmaster General under the Wilson government. When the Wilson government was defeated at the 1970 general election, he was not appointed to the shadow cabinet. He obviously had some time on his hands.

In 1970 John Stonehouse set up various companies—he was a very erudite economist and a very learned man—to try to secure himself regular income outside of his parliamentary duties, which is very much a feature of British parliamentary life. In 1974 he ran into some financial trouble and basically started cooking the books of his various financial enterprises. He then became aware—I am not quite certain how; I think to this day no-one is—that the Department of Trade and Industry was looking into his affairs. He decided that his best choice was to flee the jurisdiction. We should keep in mind that he was still a sitting Labour member of Parliament at this time. All of the documents, including those relating to the investigation, became declassified in 2005. They make for fascinating reading. In any event, in or about 1974 or 1975 he spent enormous amounts of time rehearsing his new identity. He was to assume the identity of Joseph Markham, the dead husband of a constituent in his electorate. Knowing the constituent and knowing that the husband had recently died, he started assuming the identity of Joseph Markham.

Mr J.M. Francis: Did he vote for him as well?

Mr C.C. PORTER: I am not sure. That might be in the declassified documents. He maintained a pretence of normality until he pretended to suicide on 20 November 1974. He left a pile of clothes on a Miami beach and everyone, for all intents and purposes, presumed that Mr Stonehouse had committed suicide and died. Obituaries were published. No body was ever found, as will become obvious by what I am about to tell the house. In reality, rather than having committed suicide by drowning at a Miami beach, he was en route to Australia. He was hoping to set up a new life with his mistress, who also happened to be his secretary, Ms Sheila Buckley.

Mr J.E. McGrath: A famous case.

Mr C.C. PORTER: Yes, it is a very famous case. When the police caught him, they had mistaken him for Lord Lucan, who was involved in another famous case. John Stonehouse assumed the identity of a dead constituent, took his secretary and came to Australia. Only a month after he had been in Australia, the police apprehended him on Christmas Eve, thinking that he was Lord Lucan, another famous absconder. Interestingly, he applied for what is known as the Chiltern Hundreds while he was still in Australia, which is one of the ways for an MP of the House of Commons to resign. Then he decided not to sign the papers. In any event, he was extradited to the United Kingdom and deported from Australia. That was about six months after he was discovered in Australia. He returned in June 1975 and was remanded to Brixton prison until August. Throughout that period, he continued to act as an MP. That is one of the quirks of the British system, which is remarkable in itself. It speaks volumes for having a written constitution. In April 1976 he resigned as the Labour Whip, making his party a minority government. He was very important at the time.

John Stonehouse went on trial and he was convicted for fraud and attempts to fraud. He tried to get at his insurance money, amongst other things. One of the issues that was critical in the trial was the idea of what is an "attempt". Interestingly, he also conducted his own defence at trial, another no-no. There is a very famous saying about what actually constitutes an attempt to an offence, in this case an attempt to a fraud. Did he actually mean to defraud the world at large? I think it was a matter of getting insurance money by deceiving people into thinking that he had actually died. There was a very famous statement by one of the law lords who had considered what would constitute an attempt. In a moment I will describe how one has to have some intent but

one has to do an act that is more than merely preparatory. What that act might be will depend on all the circumstances at the time. In this matter, Lord Diplock took what appeared to be a proximity requirement very, very far to something that resembled a last-act test. He said that it may be necessary for the offender to have crossed the Rubicon and burnt his boats, to have gone so far along the line of offending that he was all but committing the offence. There have been various formulations of that test as the law has developed. That is a very extreme version of a test for attempts.

I return to my example of going into someone's home under warrant and finding a range of equipment. Perhaps an enormous amount of credit card data has been found stored on a thumb drive or perhaps something has been found that is capable of fitting inside a McDonald's EFTPOS and transmitting the swipe data. The way the criminal law would generally and traditionally go about that is to charge the person with an attempt to do another offence. But a problem has arisen. It will be a problem in all cases but it may be a problem in many. First of all, one has to prove the intent to commit the eventual offence but then show that that person has done something that is more than merely preparatory. It might be that the mere possession of the types of equipment that we are talking about, which people are able to buy from a Tandy store, is not in itself more than merely preparatory.

The two other very famous cases about the law of attempts are both Queensland cases—the Crown v Chellingworth and the Crown v Edwards. One of them involved a very famous incident where an individual was charged with an attempt to have sex with a horse. He was caught by local police standing naked behind the rear end of a mare and in a state of excitement. This was a case from the 1950s. It was held that he had not done something that was more than merely preparatory. The law has wound back from that extreme test of attempt. We might ask ourselves what else could he have done in that circumstance. The students loved that example. It is hilarious.

We have now wound back but there still has to be some considerable proximity between one's acts—what one has done—being in possession of something and the actual offence.

The ACTING SPEAKER (Mr P.B. Watson): Member, I know you are trying to address your group, but it is proper procedure to face forward so that Hansard can hear. I know that you like to play to the crowd, but if you could just talk to the front it will be clearer on the microphone. The people at this end are feeling a bit left out.

Mr C.C. PORTER: They are also a good crowd.

This is the idea of the offence of attempt, and this is where the criminal law falls down in this particular area. That brings me now to the case of David Hicks, which I think is also very illustrative of the types of problems that we are dealing with here. There was a lot of debate about David Hicks, and he was charged, as I recall, with two offences. One of them was the offence of material support for terrorism. Supporters of Hicks' return to Australia made much of the idea that no such offence existed under Australian law at the time. Had David Hicks been returned to stand trial in Australia, the offence would have had to be created, and David Hicks would have had to be prosecuted retrospectively for an offence that did not exist at the time of his actions. There is obviously a very large degree to which we all feel that retrospectivity is very unpalatable. There was argument amongst the American prosecutors, particularly the American prosecuting colonel, that the idea of the offence of material support for terrorism had always existed in American criminal law.

Even more interesting was the idea that Hicks was also going to stand trial for the offence of attempted murder. This is incredibly interesting, because a person must first of all have had an intent to commit the eventual offence and then done acts that were more than merely preparatory. I am not sure about the circumstances in which he was caught, but it was said by many who criticised the idea of an attempted murder charge that he had not actually done anything that was preparatory, let alone more than preparatory. Some people said that the best that could be alleged against Hicks was that he had a gun at the time of his arrest and was intellectually or philosophically prepared to use it to shoot US soldiers, had he been in the right place at the right time; he just lacked the opportunity to do that. In those circumstances it would have been very difficult to charge and successfully try David Hicks for attempted murder, because although he was in possession of the tools of his criminal calling, and he may have had some form of intent, he had not done acts that were more than merely preparatory.

The kind of offence that this legislation is trying to create, amongst others, is the idea of trying to criminalise the very possession of the tools of the trade. If I were to apply that to David Hicks, it would be criminalising his possession of a gun and also his possession of the intent to use it for a criminal purpose. It is very interesting that what we do not do in criminal law is charge someone for thinking about doing something criminal. This was very put pithily recently, when I read that if that were the case, even Jimmy Carter might have found himself stoned to death under Sharia law. In a 1976 *Playboy* article, Jimmy Carter said this —

> I try not to commit a deliberate sin. I recognize that I'm going to do it anyhow, because I'm human and I'm tempted. And Christ set some almost impossible standards for us. Christ said, "I tell you that anyone who looks on a woman with lust has in his heart already committed adultery". I've looked on a lot of women with lust. I've committed adultery in my heart many times.

Jimmy may well have done that; I am not disputing that. But the point that he is trying to make is that that intent, or that thought, even though he might have possessed the tools of his trade for lust—they may have been on him—those two things in combination are generally not an offence.

Mr J.M. Francis: He was a submarine officer.

Mr C.C. PORTER: That is not a matter that I can comment on.

We are creating new offences here. The first offence that we are creating is stealing someone's identity. I will come back to that whole idea in a moment, but it is the idea of using or supplying someone's identity, possessing someone's identity with intent to commit an offence; alternatively, what I have initially been dealing with here, possessing equipment that could be used, in the case of the member for Mindarie's legislation, or, in what we will present, to make, use, supply or transmit identification information. We are trying to create special circumstances because the law of criminal attempt somewhat falls down in this particular area.

I might now talk briefly about some of the comments made by the member for Forrestfield. I listened very intently to what he had to say in his contribution. No doubt when the government's legislation reaches the consideration in detail stage he will have much to contribute. I will be listening very carefully with a view to considering any suggestions that he can make. The one thing that has struck me about the developmental process of this legislation is that the technology is changing at a pace faster than this Parliament can ever hope to keep up with. Drafting legislation broad enough to at least give us some breathing space over the next five to six years, or even the next three to four years, is very important. That is why it is worth waiting the extra week or two, because there are some significant improvements in the breadth of the behaviour that will be covered in the government's legislation.

What was also interesting about the contribution of the member for Forrestfield was that he used, colloquially, as everyone has used it, and as I have used on occasions, the idea of "identity theft". It is interesting, because if we go back to Mr Stonehouse, who assumed someone's identity, identity theft was not what he was ever charged with. The reason for that is probably that someone's identity is simply not a thing under our Criminal Code that constitutes property that is capable of being stolen. It is the equivalent of saying that someone's personality has been stolen. Maybe some of us need to do that, I do not know, but it is just not something that the criminal law in this jurisdiction recognises as capable of being stolen. In fact, the bill that will be brought before the house by the government will be talking about identity crime rather than identity theft. This was a matter that came out yesterday in relation to the arson legislation. The Criminal Code contains a definition of property that is very wide. The term "property" includes real and personal property, and anything animate or inanimate capable of being the subject of ownership. Someone's identity does not necessarily fall within that definition. Their credit card might, and even arguably some details stored in some area about them might, but simply assuming an identity—saying that I am the member for Forrestfield or the member for Riverton—and passing myself off as another person might constitute a fraud but it is not necessarily a separate offence such as what we would call identity theft. This legislation, in part, cuts into the area of attempts to offences, with respect to the idea of equipment, and it also goes into the area of creating a new offence, which is the assumption of someone's identity—pretending to be someone else through whatever means are available. It is a delicate process to try to get that absolutely right.

I will return now for a moment to the idea of attempts or inchoate offences. Understanding the circumstances in which someone possesses the offending equipment or the tools of the trade is so critical in the drafting to make sure that we have it absolutely right, because the equipment is already quite variable in the current state of knowledge and technology, and it will no doubt be different in six months' time. The mechanisms and processes will be different in a very short period. Section 4 of our Criminal Code sets out what it means to commit an attempt at an offence. There must be a person who intends to commit an offence—that is the mental element. That person must begin to put that intention into execution by doing an act that is more than merely preparatory to the commission of the offence. However, the person cannot fulfil his intention to such an extent as to actually commit the offence. There must be the intention, and a person must do something that is more than merely preparatory but must not go so far as to have actually committed the offence. The member for Ocean Reef made a very important point when he was quizzing the reason that the member for Mindarie stipulated in his legislation—something very similar will happen in the government's legislation—that a person cannot be charged for one of these offences and charged with an attempt, because if we were to try to do that we would be

covering exactly the same facts with two quite different offences, and these are meant to be stand-alone offences. There may be a time when we determine to charge someone with an attempt to steal, on the facts, because we think they are doing something that is more than merely preparatory. Not only have they been caught with all the skimming material, but they are standing over the automatic teller machine bolting it on, in which case there would probably be very few problems in proving that they had attempted to commit another offence such as stealing. An intention speaks for itself and juries are instructed all the time that that is a mental element of an offence; someone has to have an intent to do a certain thing, in this case something criminal.

I come back to the issue that I raised with the idea of Stonehouse, Chellingworth and Edwards; that is, this idea that we have to ask ourselves this question: how far must the accused have gone in possession of the equipment to have been said to be committing an offence—an attempt? The problem in a nutshell is that simply finding people in possession of the offending equipment is not going to be enough to say that they have done something more than is merely preparatory because in many instances the equipment might itself be quite benign. It might be the sorts of things that anyone who is a boffin in the area, and has an interest in it, could have on him or in his study or attached to his computer. Some of it might be as simple as a computer program that is able to transmit and collate data. Therefore, we cannot criminalise someone's mere possession of that sort of equipment. We are having difficulties criminalising people where we can show they have an intention to commit an offence but are also in mere possession of the equipment, which is what we are trying to do here. In Williams, which is one of the Queensland cases, is probably the best description of what an attempt to an offence is that I have read. It states —

> *... the first step along the way of criminal intent is not necessarily sufficient and the final step is not necessarily required. The dividing line between preparation and attempt is to be found somewhere between these two extremes; but as to the method by which it is to be determined the authorities give no clear guidance ... for that would mean the discovery of a legal formula universally applicable to the enormous variety of method by which nefariously inclined individual persons apply their infinite disparity of intellect and capability to the carrying out of criminal intentions. This is just a long way of putting the evergreen truth—each case depends on its own facts.*

I think that gives some idea of what an attempt is and why criminal law is very much struggling to try to keep up with technology in this area.

What are the types of offences that legislation in this area and the other jurisdictions has tried to come up with and has tried to enshrine in law and make criminal? I will just go through not a summary of the member for Mindarie's bill but look at basically the types of offences that we can have. Firstly, we need to have some definition of what identification material or identity material is that is broad enough to determine whether people are in possession of it. Generally speaking, the types of offences we are looking at are the offences of making, using or supplying identification material; that is, the actual material that goes to someone's identification. Then there is the offence of possessing the material with some kind of intent to commit a criminal offence. Finally, there is some kind of offence for possessing the equipment people can use to make the material. In my view, that is perhaps one of the most critical features of any legislation of this type because it covers that scenario of people who have equipment that could be used to enact criminal intent but all they have done is possess the equipment. It is absolutely critical. The complaints, which I will go into detail on later, that I have about the member for Mindarie's legislation is that that critical offence criminalises the possession of equipment with intent, but only the possession of equipment that is used to make identification information or material. The problem with that goes back to the genesis of the South Australian act, which the member for Mindarie has followed in this legislation. In 2003 what was the skimming offence that everyone was concerned about? It was people putting a rather cumbersome block over an ATM and also having a camera on the ATM; the block that sits over the front of the card insert slot would read the card and the camera would read the personal identification number as it was being put in. That sort of equipment, we could imagine, might be found in someone's home and we might be able to prove his or her intent to use it and therefore we could prove the offence of possessing the equipment that could make identification information, which would be the offence. The member for Mindarie's bill does that. However, the bill does not go the step further. In 2003 the types of offences that we saw at McDonald's were distant, but we are now seeing them. The equipment that was used in the McDonald's scam is very, very different from the type of equipment that we might describe as the equipment that we use for making identification material. The type of equipment that slides into an EFTPOS machine does not make the identification material; it transmits it. It simply shoots it off in cyberspace to somewhere else.

Mr J.R. Quigley: Does it shoot off into cyberspace to take money out of someone else's account?

Mr C.C. PORTER: That is quite correct; yes.

Mr J.R. Quigley: Therefore, that is using personal information for the commission of an offence.

Mr C.C. PORTER: That is right and it might be caught at that point in time. But imagine this, member for Mindarie: we find the chip that goes into the McDonald's EFTPOS machine at someone's home during the course of a search warrant for this or that. At that stage it is not being used; it is merely sitting there. Those people are merely in possession of equipment that might be later transmitting. If we can prove the intent in that case, then we have the offence.

Mr J.R. Quigley: And if it is used in the McDonald's situation, it would be caught by new section 440D(1).

Mr C.C. PORTER: I do not think that is necessarily the case and if the member argues that then he must necessarily argue that he never needs the substitution attempt offence, which is what possession of the equipment plus intent will be.

I might just add to that the point that the other offences in this legislation all sit around—there will always be overlaps—the decision of a prosecutor to try to determine which is the best charge to judge under. That is a complicated decision and there will not always be clear delineation between the offences in this case. The point is that we must have an offence in legislation of this type. If we want to even stay close to keeping up with the criminality, we must have an offence that makes it unlawful to possess equipment with intent where the equipment is very, very broadly defined because it is hard enough to prove the intent. Once we have overcome that barrier, we have the situation whereby we can prove that an individual has committed the offence of possession of equipment of a certain type broadly defined, plus with intent.

I will now make a couple of comments about some of the other contributions from members opposite. The member for Gosnells raised the issue of the temptation that people in commerce and trade now have to revert to cash or decrease their credit limits. My inclination is to believe that in the not too distant future there will not be such a thing as cash; it simply will not exist any more in the way that western societies have come to view it. Although no doubt some core of society will always keep money under the mattress and so forth, these types of offences will be important because not only are we such an electronic economy, but also a reversion to cash is very difficult. One of the matters raised by the member for Gosnells, which was echoed by many members on my side of the house, was that in addition to creating criminal offences about the use and supply of identification information, about the possession of identification information with intent, and about the possession of equipment used to make identification information with intent, is that other than criminality, other than losing money, and other than people breaking the law, there can be enormous inconvenience occasioned to someone who has had his identity assumed or used by another person. That is something that the member for Mindarie's bill does, and again it is something that the government is conscious of and will be in the bill that we present to Parliament; namely, we have to provide some kind of mechanism to assist the victims of an information offence of this nature in court by granting them some kind of certificate as to their identity so that they can show the world at large that they are who they say they are and are not the person from the Congo or wherever it was that the member for Ocean Reef was the subject of a fraud from. Therefore, that also becomes very, very important.

I will return to the genesis of the South Australian legislation, which the member for Mindarie has chosen to replicate. For its time, in 2003, it was a good bill. However, what the member for Mindarie inserted—the South Australian legislation, which he has copied—was recommended as the model legislation for Australia by the Standing Committee of Attorneys-General Model Criminal Law Officers' Committee's final report into identity crime, although it was not actually the bill that was recommended as the model law by that very erudite and learned group. The South Australian legislation was the first legislation in any jurisdiction to even attempt to deal with the issue and it was that legislation that the model criminal code group started to look at in terms of producing the best possible legislation that might be replicated amongst the states.

Debate adjourned, pursuant to standing orders.

Sitting suspended from 6.00 to 7.00 pm