Australia & New Zealand's National Identity Theft Support Centre

Committee Secretariat
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

17 October 2014

Dear Committee Secretariat

iDcare Submission to the Inquiry into Financial Related Crime

On 6 October 2014 the Commonwealth Minister for Justice officially launched iDcare as Australia's national identity theft support centre. The launch took place after some eighteen months of intense planning, testing and engagement across Australia and New Zealand with business, government and individuals throughout the community impacted by financial crime.

This submission is brief. iDcare would welcome the opportunity to provide evidence by way of hearing should the opportunity present. The views presented herein are those of iDcare and not necessarily of member organisations or contributors to our work. In consideration of the Committee's terms of reference, this submission focuses upon the:

1. character, prevalence and impact of financial related crime in Australia;
2. the methods and practices used by the perpetrators of financial related crime (including the impact of new technologies);
3. the relation to identity fraud – credit card fraud in particular;
4. the functioning of current legislation, and in particular, victim certificate legislation pertinent to identity crime offending.

Character, Prevalence and Impact of Financial Related Crime in Australia
In 2003 the founder of iDcare and a colleague at the University of Sydney produced Australia's first comprehensive study on identity fraud impacting the Australian community. That very same study was repeated throughout 2013 and 2014, with the results due for publication in late 2014. The intervening ten year period has seen a rapid evolution of financial crime impacting Australia, something that largely mirrors the developments in transnational commerce, government service delivery, and mobile communications. The most notable difference is the size and impact just one individual alone can have on the Australian community now, being exponentially larger than what one could have achieved ten years early. The financial crime market is multi-faceted. It is dynamic, largely follows, if not leads, technology-supported product and service delivery, and has created its own illicit identity marketplace eco-system. Such an eco-system is driven by the need for criminals across the world to buy and sell stolen credentials, account information, and personal identifiers to other criminal participants anywhere in the world anonymously.

The last ten years has also seen the advent of ideology-based financial crime, where motives aren't based solely on making a financial gain from the theft of personal and financial

information, but rather on making a political or ideological statement. A common manifestation of this is *Hacktevism*. iDcare's view of this form of crime is quite a personalised one. Although only recently launched, iDcare has responded to over 800 individual clients since September 2013 when our phone lines were connected, and word of mouth generated pre-launch engagement. Some of these clients have been victimised from *Hacktevism*, the consequences of which can have quite different impacts to individuals. Unlike mainstream financial crimes that involve the theft of a real person's identity, ideology-motivated identity theft victims don't have a specific illicit transaction to focus upon remedying. They are often left without any indication of if or when their personal informaton will be used – creating at times higher levels of anxiety than what iDcare typically sees in responding to other forms of identity theft and misuse.

iDcare estimates that some 1.1 million Australians and New Zealanders are impacted by identity theft and misuse every twelve months. This statistic is drawn from a multi-method approach to collecting data on the prevalence of identity theft and misuse, involving random telephone surveys, internet-based questionnaires, data extraction from industry and government, and victim focus groups. The forthcoming report on our work will provide considerable depth to this detail. Suffice to say, the quoted statistic is only a subset of a much broader financial crime challenge confronting both countries.

Identity theft and misuse means the theft or assumption of a pre-existing identity (including credentials representing such an identity) with or without consent, and, whether, in the case of an individual, the person is living or deceased. There are typically two aspects to this crime. The first is the initial compromise of the identity information or credential. The second is its on-use. Both of these aspects may occur simultaneously, whilst in other cases it may be years between when the personal information was captured to when it was used fraudulently.

The Methods & Practices Used by the Perpetrators of Financial-related Crime

In many ways it is the crime of the new millennia. The more government and business seek to adopt heightened measures of identification authentication and verification, the more criminals will seek to commoditise and target legitimate personal information and credentials. Like the constant change of technology-related product and service delivery, the financial criminal environment and broader identity eco-system is akin to an arms race that will only every see a continued escalation of measures and counter-measures.

iDcare is witnessing firsthand the devastating impact of technology driven identity theft and misuse. We see a much broader identity eco-system at work, where conventional ways of viewing what is and what is not a financial crime has become largely redundant. For example, the real impacts of identity theft and misuse are largely masked by the very nature of how government and business define and categorise such events. A fraudulent credit card transaction involving an eCommerce purchase may be categorised as *Card Not Present* fraud, but this is only one of a much broader identity eco-system challenge confronting that consumer, and ultimately impacting that person's confidence in their engagement with the broader system. iDcare gets a significant number of clients that have that one credit card transaction issue. What most institutions don't know is that credit card transaction is only one of a number of identity theft and misuse related risks to that individual. A vast majority of iDcare clients need to respond to multiple identity theft and misuse risks, in addition to that one transaction. At times we deal with instances where a client's entire hard drive has been compromised, and all of the identifying information and credentials kept on that hard drive (including the credit card information). We deal with people that have experienced

break-and-enter of their residential property, where birth certificates, passports, credit cards, and tax returns have been compromised. iDcare deals with a much broader identity risk eco-system than individual agencies or institutions have any visibility about. We see how difficult it is for individuals to navigate their way through an often complex and unseen maze of government and business. It is not uncommon for people to reach into iDcare that have been at a response to their circumstances for years.

Technology is largely a part of the risk environment, but often this is in concert with other events. Australia and New Zealand are targets of cold-call scams, which often leads to mass identity theft events. Most of the more devastating cases iDcare responds to are those where a cold caller has gained remote access to a personal computer, laptop or device and literally sucked the contents out of those technologies. iDcare has developed an ID First Aid Kit to assist individuals confronting these events.

However, technology and its adoption by business and government has also attracted criminals to new forms of identity theft and misuse. The use of mobile phone text messaging as part of the security authentication process of business and government has given rise to iDcare witnessing illicit mobile phone porting. In such instances, with very minor identifying information, a criminal can literally port a mobile phone number from one carrier to another, often via a mobile phone third party (such as a mobile phone reseller), in order to "steal" the mobile phone number and not the mobile phone. The iDcare client wakes up one day to find that their mobile phone doesn't work. Unfortunately it's not the batteries. A criminal has stolen their identity, taken over their contract, and moved their number to a new carrier all to gain access to the text message accreditation measures.

Financial Crime, and in particular, Credit Card Fraud

The silver lining to the dark cloud that is financial crime relates to credit card fraud. Of the 1.1 million Australians and New Zealanders impacted by identity crime and misuse each year, the vast majority of these individuals experience credit card fraud. The vast majority of this cohort need to respond to transactions that occur using only their credit card credential information, not personal information that can be easily linked to an individual. The response to such events is typically non-invasive, and leads to the suspension of a card itself, a typically quick investigation by the financial institution, and a replacement card re-issued. iDcare does observe considerable variance in the way such events impact on individuals. Australia's major financial institutions are typically quick to respond and generally handle iDcare clients well. However outside of such institutions, more variability exists on how customers are treated, what information is passed, and the overall customer experience from such events.

An important aspect of credit card fraud that is often overlooked is the role of the retailer or merchant. This area is one that is receiving a lot of attention at the University of the Sunshine Coast, which has a research fellowship in identity security. The University is undertaking research on the risk and knowledge diffusion that occurs between the consumer, retailer, merchant bank, consumer's bank, credit card company and the on-use retailer site. It's a complex eco-system for the one event. A system where the knowledge of risk is not equal amongst participants, and one that often results in inadequate prevention and knowledge sharing. The role of the retailer, particularly the eCommerce retailer, is critical in mitigating the risk of credit card fraud. iDcare in 2013 and 2014 has undertaken fourteen focus groups with victims of identity theft and misuse. The findings, which will be published later this year, indicate that the knowledge and direction of blame from such events held by consumers is grossly distorted compared to what has actually occurred. This

is an area central to the research being undertaken, and one that requires much more collaborative and educational based engagement between consumers and retailers.

The Functioning of Current Legislation

Two aspects of current legislation are worthy of preliminary comment for the purposes of the inquiry. The first relates to Commonwealth victim certificates and identity crime[1]. Individuals can apply for a Commonwealth victim certificate only if these three key elements are proven:

- a person makes, supplies or uses identification information (yours, or a third party's)
- they do this intending that either they or someone else will pretend to be you or another person (who is living, dead, real or fictitious)
- the act of pretending would be done to commit or help commit a Commonwealth indictable offence.

iDcare receives a number of calls from clients who begin the conversation by saying "I want a victim certificate". However, given that less than 6% of identity crime perpetrators are arrested and successfully prosecuted, the chances of someone being eligible is remote at best. The second issue with the current framework is the purpose and value of such certificates. The certificates are designed to 'help support your claim that you have been a victim of Commonwealth identity crime. You can present the certificate to an organisation such as a government agency or business…to negotiate with them to re-establish your credentials or remove a fraudulent transaction from their records' (Cwth Attorney-General's Dept, 2014 – see footnote). iDcare is not aware of any successful issuance of a victim certificate for identity crime, within either relevant State equivalent measures or the Commonwealth. This is not from a lack of interest. iDcare receives a number of calls from individuals that express interest in obtaining such certificates, but in all instances fall at the first hurdle of the essential element – someone has been successfully convicted of an identity crime offence.

For individuals that experience identity crime, a certificate that can formally acknowledge their status needs to be efficiently delivered and not reliant on a person being convicted. Most identity criminals are not brought before the courts. Most response measures required of organisations to assist a person need to occur immediately or as soon after their personal information has been compromised as possible. Both of these realities make the intent of a victim certificate for identity crime relatively meaningless. iDcare could play a future role as being an organisation that cuts across all levels of government and industry. In our own way, the anonymous and free service we provide individuals achieves much more than a certificate. We would welcome much greater focus and review of this regime and encourage relevant parties to work with iDcare in mapping a more palatable way forward for members of the community impacted by identity theft and misuse.

The second legislative area worthy of attention is the field of mandatory data breach notification. iDcare's sister organisation in the United States, the Identity Theft Resource Center (ITRC), nationally collects and distributes public information on data breach events impacting the United States community. Such events are typically defined as occurring when an entity that holds personal information experiences a compromise of such information

1 http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/VictimsofCommonwealthidentitycrime.aspx

where the details have been unlawfully passed, stolen or accessed. iDcare is working with the ITRC in building an Australian and New Zealand equivalent capability. The purpose of such reporting is to provide individual members of the community knowledge that their personal information may have been put at risk, and to work with them and the impacted organisation in building response measures. Under the current framework individuals are unlikely to be afforded the oppportunity to mitigate such risks through a lack of knowledge of the vent occurring in the first instance. Usually any such indication that something has occurred is typically through a media story some months or years after the initial compromise or through the re-issuance of a credit card. Both ignore the broader risks a person confronts in the wider identity eco-system.

The data breach environment is only set to escalate as more and more personal records and related information holding are kept online in an Internet-facing environment. The key distinction between the work of the ITRC and the work program being developed by iDcare, is that the breach notification in the United States is mandated by law, both as a federal model, as well as an individual State legislated instrument. In Australia and New Zealand at present it is not. Our Privacy regimes are strong in relation to the conditions under which organisations can collect, store, transfer, and destroy personal information. However, both countries fall short in having specific measures on what is required when the worse case scenario actually occurs. There are guidelines and advice available on the respective privacy agencies, but these are not mandatory. iDcare would welcome a greater focus on the benefits of mandatory data breach notification regimes and models and their suitability for Australia. It seems a juxtaposition that our emphasis falls short on when things actually need a response.

Final comments

iDcare is in a unique position. We are a joint public and private sector initiative. We see at the grass roots the impact of financial crime on the individual members of our community, as well as work with government and business at all levels across all jurisdictions. The financial crime prevention environment is a crowded space. However, iDcare is Australia and New Zealand's only dedicated response capability to individuals that provides tailored and specific guidance on what is required when things do happen. iDcare does not have a recurrent funding model. It is a member based organisation. Membership allows iDcare to share intelligence and accredit members to our Code of Practice to lift standards in response. The sustainability of our funding is a critical priority and one that will ensure the Australian and New Zealand communities maintain its only dedicated support service that is independent, cuts across all jurisdictions, and provides impartial advice on how individuals can find a way to best respond (see idcare.org).

iDcare tests organisation response measures to identity theft and misuse events across industry and government. Our work is akin to a 'secret shopper', where we literally examine what is publicly available for individuals that need to respond to identity theft and misuse, we call the institution or agency concerned, and we measure a raft of response variables to get an accurate sense of what our clients are likely to confront. iDcare does this to ensure the advice we provide our clients is timely, accurate and doesn't 'sugar coat' what they can expect to endure when responding to an event. The last thing iDcare wants to do is provide the wrong advice and give any false sense that the journey with a specific organisation is going to be different than what they might expect. iDcare has a pretty good sense of what organisations are good, and which ones focus less on customer service – arguably at a time when customer loyalty is on the line.