



Association of Building Societies and Credit Unions

29 June 2007

The MCCLOC Secretariat
Criminal Justice Division
Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

Per email: criminal.law@ag.gov.au

Dear Sir/Madam,

MODEL CRIMINAL CODE – IDENTITY THEFT DISCUSSION PAPER

Abacus – Australian Mutuals appreciates the opportunity to comment on the *Model Criminal Code - Discussion Paper: Chapter 3 – Identity Crime*, which proposed the introduction of an identity theft offence. We apologise for the delay in making this submission and appreciate the additional time provided to make these comments.

Abacus is the peak representative body for credit unions and mutual building societies. Our members are Authorised Deposit-taking Institutions and Australian Financial Services licensees regulated by APRA and ASIC respectively. Our members are also regulated by the new *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, which imposes extensive and ongoing customer identification obligations.

Our members are mutual companies, where their members are their owners, providing competition and choice to the retail banking market. With more than 4.5 million members across Australia, the mutual sector is highly aware of the risks connected to identity theft, the implications for business and consumers and the challenges associated with prosecuting perpetrators.

We support the inclusion of identity fraud and identity theft offences in the Model Criminal Code (MCC) to close gaps in the enforcement regime that allows identity thieves to avoid prosecution. We believe harmonising the current patchwork of identity crime offences in a way that recognises the national impact of these offences is essential to building a credible and robust response.

Model identity crime offence

Capture, use or transfer

We support an offence that covers the capture, use or transfer of information. This is an appropriate response to the nature of personal information in terms of its creation and movement.

With or without consent

We agree that consent by the party whose identity is used or assumed is irrelevant. Instances of friendly-fraud should not be able to escape the reach of the proposed new offences.

Scope of 'personal financial information'

We do not have any immediate concerns about the proposed definition for '*personal financial information*', which is based on the South Australian and Queensland approaches. However, we do believe the definition should be cast widely, to ensure it can target malicious behaviour and activity and remain effective into the future in the face of rapid technological change and criminal ingenuity.

We caution against too narrow a scope that could exclude data extraction where there is no physical *skimming* or where interception-based scams involve information garnered that is not on its face '*personal financial information*'. Although, we also recognise the counter-argument that if the existing definition is too broad it could create a situation where responsible financial institutions could be prosecuted for collecting information through legitimate use of ATMs or the legitimate production of cards.

Ultimately, we believe any proposed offences within the MCC should be drafted widely to operate as an effective deterrent and as a remedial measure against those who possess relevant materials and information, attempt and actually undertake identity-based frauds or hold or use information produced by these illicit activities.

Alive or dead, real or fictional

We support an offence that encompasses real as well as fictitious identities. Passing off any identity, whether based on a dead or alive, real or fictitious person has a direct impact on both the person whose identity is used and on the targeted merchants, card issuers or financial institutions.

Intent to commit another offence

With regard to our comments under *Possession of equipment to create identification information* (below), we generally agree with the principle that using another's personal identification information to escape domestic violence, in a period before a death certificate has been issued or by minors to enter a club or purchase alcohol should not necessarily attract a penalty under the proposed offences. The offence should, in our view, be appropriately targeted at the detriment caused to individuals and business and other stakeholders of identity crime and identity theft where the offender intends to capture, use or transfer or otherwise fabricate identification information that may be used to commit another offence.

Penalties

We understand the view in terms of imposing a 3-year penalty for these offences that is aligned with comparable offences under the South Australian and Queensland legislation. In that context the proposition is to recognise a distinction between preparatory and other offences. However, we believe the penalty for these proposed offences should reflect the seriousness in which they are regarded and the intention of the legislature to identify Australia

as a hard target for these types of fraud. We believe that the insidious nature of these types of fraud suggest that a 3-year penalty may be insufficient. Accordingly, we believe a 5-year maximum penalty (commensurate with the MCC skimming offences) is preferable.

Certificate following conviction

We support the proposition that identity crime and identity theft represents an immediate threat to a person's financial resources but also represents a significant risk to their future use of their own personal identification information. In the financial sector, after resolving liability issues around unauthorised transactions, the impact of identity crime on a person's credit reference is perhaps the next most significant issue.

We support the ability for identity crime victim to be able to obtain a court-issued certificate that supports their claims of identity theft. We believe further thought may be required in relation to when a person can seek such a certificate. Requiring a victim of identity theft to wait until a successful prosecution occurs may subject them to a lengthy delay and no relief in the meantime. A certificate should be available – subject to satisfying certain evidentiary conditions – at an early stage and also for those victims where the perpetrator cannot or has not been identified.

Whenever the certificate is available, we support the principle that it is merely a notice and that it offers no remedial action and cannot compel any restorative action on any third party or related stakeholder, such as a financial institution.

On-selling identification information

For completeness, we support inclusion of an offence for the on-selling of identification information. We cannot readily identify a situation where a person might on-sell personal identification information without having constructive notice at least that their activity might be facilitating a subsequent identity crime or theft. Nevertheless, we support the inclusion of a specific on-selling offence to capture these situations. Some further clarity around the reckless element may be required for a more complete understanding of when an on-selling offence might arise.

Possession of equipment to create identification information

A key feature of any nationally-focused response is the need to avoid the requirement that an identity theft offence be attached to an associated criminal act. This construction is a significant barrier to an effective regime that criminalises identity crime. We cannot, for example, readily foresee circumstances where a person will have in their possession *skimming* equipment for bona fide reasons unless they are an issuer, production centre or provider of legitimate card services¹. This may particularly be the case for electronic manifestations, where the offence should include computer and other device misuse² that is preparatory to the commission of an offence.

¹ Abacus believes that these offences should be drafted in a way so that legitimate card production services are either not captured by the scope of an offence or there are adequate exceptions that carve them out from the proposed regime.

² For example but not limited to, unauthorised modification or damage through the overcoming of security systems.

Accordingly, we have previously supported the approaches adopted in South Australia and Queensland where possessing preparatory materials and offences of attempt directly criminalise identity crime, without the need to attach an associated act such as theft, fraud or forgery. However, to deal with situations where legitimate reasons can be established, we accept that any the proposed offence could include a rebuttable presumption with an onus on the possessor of the preparatory equipment to establish their legitimate right and lawful purpose for possessing such equipment.

This approach is comparable to the South Australian identity theft legislation, *Criminal Law Consolidation (Identity Theft) Amendment Act 2003*, which includes offences for holding stolen identity information, using that information and, relevantly, the production and possession of prohibited material, which includes the materials used to undertake identity thefts. We believe applying this type of approach to identity fraud and identity theft offences would create a more comprehensive and effective regime.

Further, at common law and under the various crimes' legislation an '*attempt*' is an offence only where there is an accompanying act evincing that intention. We believe that in addition to possession of preparatory equipment and actual identity theft offences, the Model Criminal Code should also include attempt offences. To do otherwise could fail to provide an effective prosecutable remedy where an identity theft is discovered before it is fully executed or if it is executed without fruition.

Conclusion

We believe appropriate legislation is required to seek to stop this type of activity and to send a clear message to perpetrators that Australia is a hard target, with laws in place that are capable of exacting significant repercussions upon perpetrators.

Abacus supports bolstering the Criminal Code to ensure Australia remains a hard target for identity thieves. *Skimming*, together with *phishing* and other frauds, are increasing in their frequency, sophistication, costs and harm. Upgrading the MCC to include appropriate offences for these activities is necessary to protect Australian consumers and business.

For more information about Abacus or the comments in this submission please contact me directly on (02) 8299 9033 or at jmoyes@abacus.org.au.

Yours sincerely



JOSH MOYES
Senior Adviser