Consumer Identity Fraud Experiences with the Existing Credit Code Provisions

1. Overview and Content

1.1 Individuals who experience identity fraud or who are at risk of identity fraud are generally advised to contact Credit Reporting Agencies (**CRA**) to obtain a credit report and ban. During the period of the ban (the default period for which is 21 days unless extended), access to the individual's credit report (or 'file') is effectively "frozen." As such, the relevant CRA will not use or disclose the individual's consumer credit report or the personal information contained in that report to a Credit Provider.

1.2 Obtaining a credit ban is a crucial measure for individuals responding to the misuse (or potential misuse) of their personal information. However, the current processes for obtaining such a ban are confusing, inefficient and unnecessarily onerous for consumers. Because many consumers have a credit report with more than one CRA, they are required to individually contact each of the three main CRAs: Equifax, Experian and Illion (formerly Dun & Bradstreet). This process creates delays and increases the risk of individuals suffering harm as a result of identity fraud. The problem is exacerbated by the current practices of CRAs. Individuals have frequently cited a lack of transparency, difficulties in communication, and the attempts of CRA staff to sell products, as key obstacles in obtaining a credit ban or report.

1.3 The difficulties associated with applying for credit bans and reports is also consistent with consumer experiences in seeking corrections to their credit reports. The identification of enquiries that are deemed to be anomalous by the consumer is a common way identity fraud and misuse is detected. Self-detection rates for consumers in the identification of identity compromise and related fraud has remained consistently high (approx. 78% of all cases reported to IDCARE since 2014). In such cases the consumer relies heavily upon timely access to credit reports to

identify entries that are indicators of fraud, and from there, seek any necessary corrections.

1.4 Like reports and bans, corrections are equally problematic. Because reports are issued by CRAs, consumers naturally seek corrections via these organisations. However, in many cases, the CRA will advise consumers to take the matter directly to the credit provider that appears as an entry on the report. Adding to the consumer's friction is unfamiliarity with the credit provider. Some credit providers are not directly connected with the organisation that the criminal has engaged, such as Esanda or Macquarie Finance, on behalf of a car dealership. This further adds to the convoluted nature of response for the consumer and the difficulties in correcting a situation that is not their doing.

2. IDCARE

2.1 IDCARE is Australia and New Zealand's national identity and cyber support service. It is a not-for-profit Australian charity that was formed to address a critical support gap for individuals confronting identity and cyber security concerns. IDCARE's primary service offering is a call centre staffed by specialist identity and cyber security counsellors and analysts who apply a human-centred approach to identity and cyber security. In the course of its practice, IDCARE has collected data from over 79,000 engagements from members across the Australian community since its launch in October 2014, including their dealings with CRAs. During this period, IDCARE referred approximately 11,400 consumers to CRAs in order to apply for a credit report and ban. In addition to these consumers, IDCARE received approximately 16,340 reports from consumers who had experienced credit misuse, that by inference, would have been captured as an enquiry on their credit report. This equates to approximately 460 engagements a week from consumers to IDCARE that would benefit from accessing their credit report, implementing a credit ban, and/or correcting entries on their report. Recently completed research that examined the journey of IDCARE clients over 12 months revealed that approximately a third of these consumers didn't complete their ban, report or correction activities because they felt the processes were too onerous, heightened them further, and/or

did not see why they should be the ones to invest the time into correcting when they weren't responsible for accepting the credit application from the criminal that impersonated them. On average consumers spent 23.1 non-consecutive hours responding to the misuse of their identity in order to obtain credit. This included broader system response efforts, including report and ban applications, as well as credit requests, police reports, and related prevention/response measures. Around 39% reported experiencing psychosomatic impacts from the response experience (stress, anxiety, sleep disruption, nausea etc). These impacts differed with the type of compromise and misuse the consumer had to respond to – crimes where remote access of their personal device was obtained by a criminal, cyber stalking, and relationship scams were recorded as amongst the most impactful response journeys.

2.2 These views, along with the broader data set, form the basis for the observations and analysis contained in this briefing.

3. Consumer Experiences and System Performance

3.1 For some individuals, a CRA is one of the first organisations they engage for assistance. In these instances, however, individuals have generally expressed frustration and dissatisfaction with the CRA's handling of the matter. When asked whether, given the choice, they would remain a customer with the relevant CRA, more than **85%** of individuals said no.

3.2 As a matter of course, IDCARE also requested victims of identity fraud to give a rating of the service and level of care they received from each organisation they contacted. IDCARE also undertakes "secret shopping" exercises every quarter across the credit providers and CRAs and measures organisational performance against a number of standard measures. These measures include relevance and accessibility of web content, call transfer counts, waiting time tests, provision of escalation content, and dependency measures on other organisations. These two independent measures are then combined to provide a score from 1-10, with 10 representing the highest level of consumer satisfaction, and 1 the lowest (akin to a Net Promoter Score). The average rating of the service provided by CRAs was 2.81 (from October

2014 to December 2018). CRAs have consistently been the worst performers in terms of client engagement across all industries and sectors since 2014. In contrast, the same customers who engaged with CRAs were also asked to rate their experience with IDCARE on a scale of 1-10, with 10 representing the highest level of satisfaction, and 1 the lowest. The average consumer rating for IDCARE was 9.32 (from October 2014 to December 2018).

4. Common challenges

4.1 Victims of identity fraud highlighted fundamental inadequacies in the services provided by CRAs. Firstly, customers expressed frustration with being connected to overseas call centres. The language barrier created an additional obstacle to the resolution of their matter. One customer, for instance, remarked that his call was always redirected overseas and that he received conflicting information each time he contacted the call centre. Another found the call centre staff to be "difficult to understand" and the advice they provided "was not easy to follow." The second challenge that individuals encountered was getting through on CRAs' phone lines. This resulted in delays, which in turn increased the risk of individuals suffering harm as a result of personal information misuse. These delays also created further – and unnecessary – difficulty and frustration for individuals experiencing identity fraud.

4.2 The most common complaint, however, was with respect to the conduct of CRA staff, who were consistently identified as prioritising commercial interests over the needs of identity fraud victims. Many IDCARE customers commented on the efforts of CRA representatives to sell various services and products. In some instances, individuals were not informed of CRAs' free services and consequently were persuaded to purchase products offered by the agencies. One of the individuals who contacted IDCARE had experienced identity fraud after her driver's licence was stolen from her letterbox. She later discovered the fraud when she applied for a line of credit and was rejected due to bad debt. It was not until she contacted a CRA that she discovered that there were multiple accounts in her name. She expressed disbelief at the approach of the agency: "I cannot believe that I have to pay money to get protected." Another victim of identity fraud encapsulated the key issues,

describing their experience with a CRA as a "nightmare": "I cannot understand their call staff, they are not helping and are blocking my request for a ban." After their interactions with one CRA, some individuals also remained unaware of the need to contact other CRAs to obtain a reporting ban. This put them at risk of further identity fraud.

4.3 Protecting children when they come of age from credit misuse is also problematic under the current system. CRAs are prohibited from creating reports or files on minors (individuals under 18 years of age). However, the compromise of identity information, and in particular, high risk credentials such as driver licences and passports can impact and does impact children. Criminals have shown a propensity to "wait it out" or sell stolen credential information to other criminals for future misuse. There does not appear to be a preventative measure, such as a ban option, for individuals when they come of age. A report needs to be in existence for a ban to be placed. The same issue extends to adults who do not have had a credit report (or file) with one CRA, and therefore cannot place a ban on a non-existent report. This favours criminals, who can wait until an individual turns 18 or does initiate a credit application with a credit provider that has a relationship with a CRA that previously has not had a credit report relating to that consumer. IDCARE provides disaster response assistance to the Commonwealth Government for Australians that are deceased or assumed deceased. For example, in the 12 months proceeding the MH17 disaster, IDCARE was engaged by the AFP to develop an identity protection framework on behalf of next of kin. It had become clear in that incident that Australians, including children, had experienced identity misuse within 72 hours of the plane crash. Australian children had online accounts set up in their name. Adults had experienced unauthorised credit card expenditure, and mobile phones and two-factor authentication in accessing accounts had been compromised.

5. Emotional impact

5.1 Customers' disillusionment with the process of obtaining a credit reporting ban was reflected in the language they used to describe their emotional state. Individuals

most commonly described them self as feeling “overwhelmed” and “anxious.” Several also felt “angry,” “irritable,” and “frustrated” by their experiences.

6. Enhancement Considerations

6.1 When asked to identify the “ideal solution” to the problems they faced in protecting their identity a number of themes have emerged consistently over the last five years:

6.1.1 A call for IDCARE to assist consumers in coordinating amongst the CRAs their application for reports, bans and corrections related activities. This has been a common theme from both consumers and has been the subject of discussions between the CRAs and IDCARE for some time. This could be established through IDCARE taking on the responsibility for customer KYC and connecting via API to each of the CRAs online application processes. Agreed workflows would determine whether each individual CRA then communicates directly with the consumer or via a hub / interface managed at IDCARE. Experian has suggested that CORREX could be applied for this purpose and Equifax in 2015-16 suggested that IDCARE could subscribe to their own platform. This enhanced consumer process would require IDCARE, as an NFP charity, to cover its costs only and work with the CRAs to develop an appropriate investment/cost recovery model.

6.1.2 An abolition of the 21-day initial credit ban period and a shifting of this to a model whereby the consumer determines the period of time a ban should be in place. This shift would allow consumers to “switch-on” their credit report when they seek credit. Such a model would necessitate the latent capture of key credit scoring data, but during the ban period, such data would not be available to credit providers.

6.1.3 Explicit guidance and compliance with ban, report and corrections processes is required to give consumers certainty. If a correction is

requested from a consumer to a CRA, the CRA should be required to notify the credit provider that such a correction has been requested. This could work in a similar way to 6.1.1, whereby a "one to many" communication approach for victims of identity fraud is advanced (rather than consumers having to make multiple contacts). Similarly, credit providers should apply consistent response standards so that consumers are not having to adapt to different application / response measures imposed on them.

6.1.4 The OAIC and Attorney-General's Department consider policy and legislative change that would allow for greater protections for children and individuals who have had their identity information stolen but may not have an existing credit report that can be subjected to a ban.

7. Concluding Remarks

7.1 IDCARE acknowledges that CRAs operate in commercial and competitive environments. That the provisions in the Code relating to identity fraud and identity theft are a cost to such organisations. Our organisation believes that greater cost efficiencies, improved consumer experience, and enhanced reputational value can be achieved with appropriate amendments to the Code. This will require leadership. IDCARE would welcome the opportunity to work with ARCA and the CRAs to co-design these measures to enhance consumer experience and confidence.