Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	IDCARE (Identity Care Australia & New Zealand) – www.idcare.org
Contact details *(one or all of the following: postal address, email address or phone number)*	PA: PO Box 412, CALOUNDRA QLD 4551 TEL: 1300 432 273 EMAIL: contact@idcare.org

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? YES / **NO**

Your submission

Introduction

Identity Care Australia & New Zealand (IDCARE) was launched by the respective Ministers for Justice in Australia and New Zealand as our national identity support service. IDCARE is a joint public-private sector entity, a not-for-profit organisation, and a registered Australian charity. At its core, IDCARE provides specialist identity security counselling to members of the community that confront the compromise and misuse of their personal information. Since our formal launch in 2014, IDCARE has provided in excess of 65,000 counselling hours, directly assisted over 16,500 clients online, via our website and through our national telephone service, and shaped how corporate and government leaders prevent and respond to the compromise of personal information. We see firsthand as a frontline service the impact that data breach events have on the community, organisations and markets. We know what works in terms of effective response and have been involved in a number of data breach response efforts, both in partnership with impacted organisations as well as independently when dealing with the fall out and serious harm caused to their customers. There is a need to appropriately consider the effectiveness of response efforts. These efforts, and the draft Bill presented, require strong recognition that data breach events can be very complex to unravel, contentious as to where vulnerabilities have been exploited, and highly fluid as to the precise impact and harm caused to individuals. This submission aims to cast further light on the precise impacts data breach events have on members of the community, business and government. It presents unique insights from IDCARE that highlight opportunities for the draft Bill to support good practice and consider and further develop provisions where such practice is not feasible or has been ignored. IDCARE welcomes this important initiative by Government, we extend our gratitude to the Commonwealth Attorney-General's Department for their leadership in bringing this Bill forward for consultation, and welcome the opportunity to participate, inform and support future developments in this important area.

Our Organisation

Our organisation is unique. We are Australia and New Zealand's only organisation resourced with specialist Identity Security Counsellors and with a mandate to provide direct frontline service support on identity security issues. We deal with people in crisis every day, who have learnt that their identifying information has been compromised, in some cases further misused, and now live with the knowledge that they are not likely going to get that information back. The reality for people that experience data breaches, particularly involving the hands of criminals, is that the misuse could occur at any time. Our role is to offer emotional and practical support to our clients every step of the way until they feel that they have done what they can to respond and mitigate the real risk. In effect, IDCARE empowers our clients to get back in control.

Our specialist staff draw upon a contemporary and every evolving library of over 900 response plans tested and updated from across the Australian and New Zealand public and private

sectors. This library represents critical information on what is required of individuals by organisations to effectively and efficiently respond to compromise and misuse events, such as data breaches, and for them to mitigate future risks. It is a massive undertaking by IDCARE to maintain this library, but it is fundamentally essential. The risk managed here is that the unique and tailored response plans provided to our clients are contemporary, relevant and reduce harm.

Australian Data Breach Environment

IDCARE collects empirical information about the Australian data breach environment from four sources:

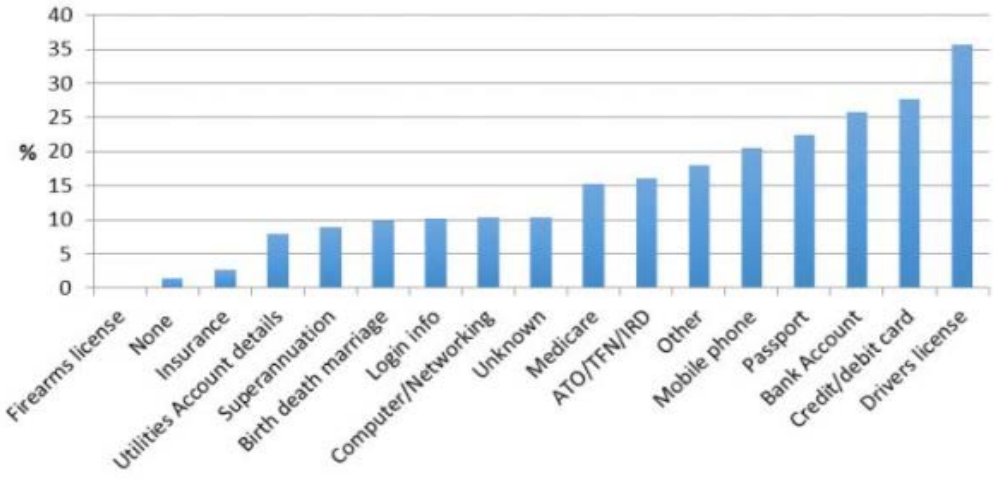
(1) From individual clients that access our National Case Management Centre via our hotline, web-form, or email;
(2) From organisational partners that work with IDCARE to respond to detected data breaches;
(3) From independent testing by IDCARE of organisational response measures from non-partners that gather critical insights on what individuals may experience when having to respond to the compromise of their identifying information; and
(4) From IDCARE's National Identity Lab that proactively monitors illicit marketplaces online that buy and sell compromised identifying information.

These sources present the following summary statistics about the nature of the Australian data breach environment over the past 12 months:

- The most valued credentials for criminals involved in data breach activities are driver licence information, credit and debit card information, bank account logins and passwords, and email login details;
- The average number of days taken between when the compromise of identifying information occurred (the breach) and when it was reported by organisations to the individual impacted was 405 days;
- In the most recent 2,500 cases managed by IDCARE where identifying information was reportedly breached, 32% of individuals detected a further misuse of this information (in other words, the exploitation and abuse by criminals of the identifying information obtained);
- In cases where the compromise or data breach resulted in a further future misuse, the average time taken by the criminals responsible for such events was 72 hours;
- Only 11% of organisations from a sample of 221 organisations within IDCARE's response library provided online guidance to impacted individuals about what they could do to mitigate harm following the compromise of their information;
- The most common response advised publicly from a sample of fifty of the last publicly reported data breaches was to provide a copy of the individual's credit report. However 84% of these organisations made statements to the effect that the "information was not sensitive" or "it was information that was already publicly available";
- From a sample of 1,732 individuals that were impacted by the compromise of their identifying information from an organisation in 2015, 72% were most dissatisfied with the response provided because it made no real difference to reducing their enduring risk of future misuse;
- The average client satisfaction score from individuals that engaged with organisations responsible for data breach was 1.8 out of ten. This means that on average individuals aren't just dissatisfied that the response will be inadequate in mitigating real risk and remedying the compromise, they are willing to promote their views to others about this.

IDCARE relies upon two sources of information to inform our organisation and our partners of what credentials are most valued by individuals that are responsible for data breaches that use hacking as a means of compromise. The primary source is from our clients, who communicate via our national support line, details about the nature of credentials that have been compromised, and in some instances, further misused by identity thieves. The following graph captures the

credentials of most value to criminals involved in the intentional attack against organisations and individuals via hacking during the October-December 2015 quarter.



Graph: Identifying Credentials Targeted from Breaches Involving Hacking (Oct-Dec 2015)

The Graph reaffirms the dependence on driver licence information for hackers and identity thieves. The usage of driver licence information throughout the Australian identity ecosystem is the most prevalent form of evidence of identity. Even driver licence issuers depend on driver licence details. The very nature of the credentials compromised can inform the risk assessed in relation to future misuse. Clients of IDCARE are provided an indicative assessment on the likelihood that future misuse will occur. This is largely influenced by the nature of the credentials that have been breached. Some credentials, such as computer login information and email accounts, can obviously enable criminals to obtain other forms of identifying information. The cyclical nature of our identity ecosystem means that one type of identity credential compromise can enable the compromise of other credentials. In the past six months IDCARE has seen a 324% increase in unauthorised mobile phone porting events. These acts relate to the unauthorised transfer of an individual's mobile phone number to another carrier without the true identity knowing. The reason for this escalation is because of the growing reliance by industry and government on the use of second factor authentication controls that rely on SMS-based code or PIN verification. Criminals that port mobile phone numbers are likely to have compromised an individual's driver licence number. The driver licence is relied upon by telecommunication carriers as a form of identity verification during the porting process (to authorise the port). So the mere porting of the mobile phone number is but an indication that a more harmful and risky data breach has occurred with their driver licence. Something that can be used extensively by criminals to exploit an identity due to its reliance across the identity ecosystem in Australia.

The second method used by IDCARE is the monitoring of what identifying information is traded within illicit marketplaces utilising dark net anonymising technologies. In a report delivered to partner agencies in September 2015, IDCARE captured the following table that details the types of identity credentials sold on AlphaBay, Agora, and the Middle Earth Marketplace, their price in Bitcoins, and the converted Australian Dollar equivalent (at the time of the data capture). The table provides a strong indication of the nature of identifying information of value to hackers that are relied upon frequently by public and private sector organisations.

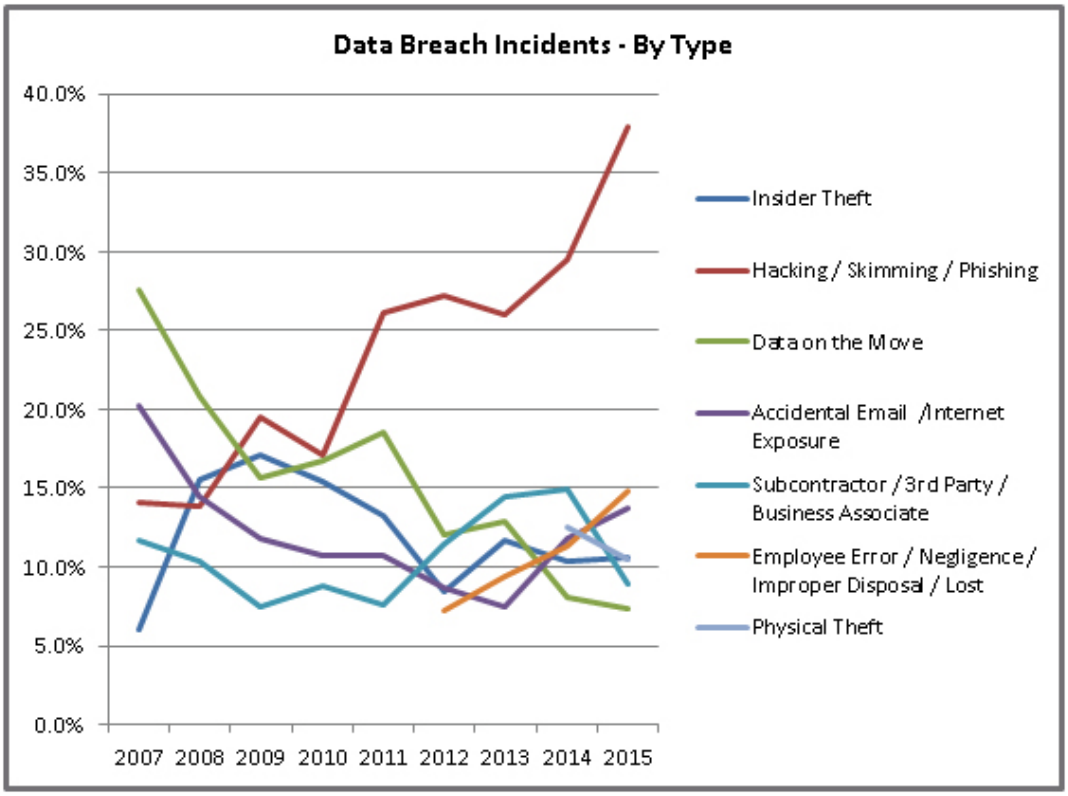
Table: Australian Credentials Sold within Illicit Marketplaces (June-August 2015)

Identifying Information	Marketplace	Bitcoin Avg Price	Aust Dollar Conversion
Australian State/Territory Driver Licence – Physical	Agora	Ƀ 1.11- Ƀ 1.2	$417- $450
Passport, Driver Licence & Customer ID Cards – Physical	Agora, Alpha Bay, Middle Earth	Ƀ 9.455	$3560

Australian Passport - Physical	Agora, Alpha Bay, Middle Earth	Ƀ 13.58	$5110
100 Point Pack – Driver Licence, Medicare Card, Bank Card - Physical	Agora	Ƀ 3.11	$1170
Full Pack ("Fullz") – Email account, Name, Date of Birth, Address, Phone, Mother's Maiden Name, Credit Card details, Social Media Account - Digital	Alpha Bay	Ƀ 0.067	$20
Driver Licence – Digital Scan	Agora, Alpha Bay, Middle Earth	Ƀ 0.2 - Ƀ 2.0	$75 - $750
Passport and Driver Licence – Digital	Agora, Alpha Bay, Middle Earth	Ƀ 0.2	$75
Bank Login and Password for Accounts with Balance of up to $100k – Digital	Alpha Bay	Ƀ 1.302	$490
Utility Bill (Telco, Water, Energy) – Digital	Alpha Bay	Ƀ 0.5 - Ƀ5.6	$188 - $2107
Email Account Login & Password – Digital	Middle Earth	Ƀ 0.15	$57

The dark net offers critical insights for organisations and individuals when building knowledge about the real risk and harm to come from serious data breaches. It is evident from the table presented and the information obtained direct from data breach victims that Australia's traditional identity credentials alongside our electronic username and passwords are of great value to criminals involved in this activity.

IDCARE's sister organisation in the United States is the Identity Theft Resource Center. Our partnership is strong and we share common objectives and ideas in best practice. The ITRC reported in January 2016 that the most prevalent type of data breach comes from hacking, skimming and phishing by organised crime. The following time series graph from the ITRC depicts the predominant involvement of criminals within the data breach environment:



Source: United States Identity Theft Resource Center, January 2016

Whilst the United States has its own unique identity ecosystem, the prevalence of identity compromise and misuse when adjusted per capita is very similar to Australia (ITRC, 2015; Attorney-General's Department, 2015; IDCARE 2014). The global nature of hacking, phishing and skimming also suggests that the Australian data breach environment may present similar findings.

The Data Breach Response Environment

In 2014-2015 the New Zealand Privacy Commissioner recorded more data breaches than Australia (121 versus 110). New Zealand, like Australia, does not have a mandatory data breach notification scheme. New Zealand has had some spectacular data breach events, the most notable in recent times involved the New Zealand Accident Compensation Corporation (ACC), that was responsible for inadvertently emailing identifying details of more than 6,000 accident claimants. This case caused enormous public outcry, not because of the comparatively small number of citizens impacted (when compared to recent Australian examples), rather because of the way it was handled. It is the handling of data breaches that is welcomed by IDCARE, as often harm associated with the compromise of personal information has little to do with the actual event, but is mostly about how individuals and organisations behave once a compromise becomes known. The relatively small number of data breaches reported to the Commonwealth Office of the Australian Information Commissioner would suggest that much more work needs to be done to educate reporting entities on the real risks and harm caused from the unauthorised disclosure or loss of identifying information. On this point, around one in five IDCARE clients present psychological and somatic symptoms and impacts following the compromise of their personal information. The most common impact recorded was heightened anxiety, depression and feeling uncommunicative.

In addition to the psychological and somatic impacts, there are many more forms of impacts experienced by individuals and these can be as diverse as the nature of how such events occur. IDCARE has been directly involved with five data breach response events in partnership with organisations over the past six months that present a window on such diversity. In two of the five examples, IDCARE was able to inform an accounting and payroll service provider that their systems had been compromised as a result of impacts being experienced by their clients that had called IDCARE's national support hotline. The clients at the time of engagement presented with misuse examples involving their tax credentials and bank account information. Through the course of the counselling service, IDCARE's Identity Security Counsellors observed a correlation between the clients and their accountant, work and/or payroll service provider. The evidence collected from clients prompted IDCARE to proactively contact the relevant organisations and work with them to: (i) assess the real risk; (ii) provide direct evidence of harm caused; (iii) mitigate future harm; and (iv) contact and directly support impacted individuals by tailoring our response plans. Under the draft Bill these cases represented instances where the organisation, once aware of the breach, took active steps in partnership with IDCARE to mitigate future risks and provide direct support via IDCARE to impacted individuals. No public notification was required as part of this response strategy.

Like other regulatory instruments placed on reporting entities, the onus within the current Bill is on the reporting entity to determine risk and harm. Without having sufficient insights into how illicit marketplaces operate, the nature of the credentials offered, and the buying, selling and misusing activities, such assessments will be difficult, and most likely, incomplete. Therefore, if the intention of the Bill is to encourage entities to act responsibly towards individuals that have had their identifying information compromised, this may be constrained from a lack of awareness of the nature of the harm (likely or real) present. This is particularly relevant for organisations that do not know what or who was responsible for the breach. IDCARE takes a broad approach to such instances, offering support to organisations and individuals that seek to cover a wide scope of impacts and risks of harm as presented in the following case studies.

Case Study 1: A tiler in Brisbane engaged IDCARE in March 2015 concerned that their work email account had been hacked. He had received a complaint from a client who was sent an email from the tiler's account requesting payment for work. The payment was to be made to another account not linked to the tiler. Within a week of the first client detecting the email, three other clients also came forward with the same concerns. IDCARE worked with the tiler to establish that their email account had been accessed and worked to assess the nature of the identifying information present, including names, addresses, telephone numbers, email addresses, and in some instances, credit card details, of some 132 individuals. A response for the tiler and the individual's identified as having their details accessed via the tiler's email account was developed. IDCARE assisted the tiler to engage, where possible, the impacted individuals. Not all of the individuals had current email or contact information. Email hacking for small to medium size entities is an enduring challenge and one that needs careful consideration under the proposed legislation. It is likely that the ability for small to medium size entities to effectively respond without the assistance of IDCARE and related support agencies would be severely limited.

Case Study 2: A client from Perth engaged IDCARE in December 2015 after they detected the establishment of several post-paid mobile phone accounts with three separate providers in their name. This was first brought to their attention when bills arrived from the telecommunications companies in the mail. Some eight weeks prior, the client had renewed their driver licence with the Department of Transport in Western Australia. The process most driver licence issuers use for replacement licences is to mail the new licence to a physical address (not using registered post). Our client contacted the Department of Transport some three weeks after applying for a renewed licence, concerned that the new licence had not arrived in the mail. The advice they reported as receiving at the time was to wait for up to six weeks. During that engagement the client alleged that the Department could not confirm whether the new licence had in fact been mailed. Having waited six weeks, the only mail to arrive was for several mobile phone bills that the client did not authorise. One of the mobile phone carriers was able to confirm to the client that a licence was produced to open the account in their name. The remaining telecommunication carriers would not confirm whether a licence had been used, citing privacy concerns in protecting the identity criminal. Notwithstanding the client experienced significant anxiety and frustration in having to engage eight separate organisations in order to effectively mitigate future risk, in this example a serious breach had occurred. IDCARE, in working with our client, established that a serious breach of their identifying information, in the form of a Western Australia licence, had not only occurred, but was presenting further harmful impacts to the individual. Their credit reports were revealing that they were not repaying debts. Their licence details, the number on which in most States and Territories remains unchanged throughout a lifetime, was compromised and continued to present as an enduring risk of future misuse. The Western Australia Police would not accept a report from the client, citing that the client needed to report to the Australian Cybercrime Online Reporting Network (ACORN), despite the fact that the crime did not demonstrate any online features. Without a police report number, it was not possible for the client to have their credit ban or suppression extended for a greater period of time to allow for additional mitigation measures to occur. In this example it is not clear as to what entity under the draft Bill provisions would be responsible for reporting and mitigating risk. Would it be the driver licence issuer? Would it be those responsible for delivering the post? Would it be the telecommunications carriers that accepted the client's stolen identifying information? Regrettably this case is the rule, rather than the exception. It highlights the complexity of the relationships and chains of events that present following the detection of compromised and misused identifying information.

Commentary on Specific Bill Provisions

Meaning of Serious Data Breach

Of specific interest to IDCARE is the draft provision that explains the determination of what circumstances constitute "real risk" (ref paragraph 26WB(3)). The draft provisions are sufficiently broad enough to cover instances IDCARE has observed that do create serious harm for an individual. It does however, remain somewhat ambiguous in its current form as to who actually interprets the "sensitivity" of the information - the person from whom such information identifies or the organisation that was responsible for its protection? It is IDCARE's view that organisations that have experienced data breaches and the clients and staff impacted can hold vastly different views on what is "sensitive", what is "harmful", and what are effective "mitigation steps". In December 2014 IDCARE was engaged by a Sony Pictures client following the alleged compromise of employee information, data files and emails. In that example, although it was a United States based entity, the harmful effects were felt by the client because of their perception

that the response offered by their employer was ineffectual and irrelevant. The employee revealed that they were offered "free" credit reports and monitoring in the United States. This was despite the fact that such an entitlement already existed under American laws. Secondly, the compromise of Australian and New Zealand passport, driver licence, credit card, banking and superannuation details demanded a uniquely Australian and New Zealand identity mitigation response. Responses that centred upon securing and monitoring efforts within the United States is of little value to Australian and New Zealand employees. The ability for criminals to rapidly buy and sell compromised credentials on line is well known. A compromise of details in one country can rapidly result in further misuse of the same credentials in another country almost immediately. Relevance of the risk mitigation measures to the nationality and geographic proximity of the impacted individual is very important – even within Australia. It is IDCARE's experience that for the most part, the general public are not aware that there are three credit reporting agencies on the mainland, but only one in Tasmania. Most IDCARE clients think that by getting one credit report from one of the credit reporting agencies they have a complete understanding of the risk. This is a false perception and one that IDCARE has seen advanced by companies that have attempted to respond to the compromise of identifying information in their custody.

Based on our experiences, IDCARE does strongly support the provision under paragraph 26WB(3)(i) that considers when the entity has taken, is taking, or will take, steps to mitigate the harm, and in particular, the ***timeliness*** of such measures and the extent to which they have been mitigated. The challenge of course, is the ability for the regulator or the entity to know how effective mitigation has been, as highlighted in the following case study.

Case Study 3: IDCARE's National Identity Lab monitors the dark net for examples where compromised identity credentials are being traded online amongst criminals. One such form, the Republic of Lampeduza, specialises in trading payment card information. Lampeduza participants cannot freely engage without "proving" to the administrators of the illicit forum that they can play a meaningful role as part of the broader illicit marketplace. Therefore, each user is required to nominate themselves for a role, such as a "carder", a "server host", a "malicious code writer", or a "money launderer (bank account provider)". It is common practice for "carders", those that perform data breaches to acquire payment card information, to have to demonstrate their value to the marketplace by committing data breaches. This is not new. The alleged Aussie Travel Cover hacker has been reported as performing the hack to prove themself to other hackers. Therefore the real risks for data breaches that involve hacking information may not (or ever) be known for some time. The breach is often a means to an ends, as is the case with Lampeduza. Those individuals that seek to become "carders", breach to become an accepted member of the forum, to demonstrate that they are worthy. What happens next, the selling, the buying, and ultimately, the on-using of this information is where individuals are most likely going to experience further real harm. This is something that the entity or regulator is not likely to be in a position to assess.

IDCARE proposes that the Bill consider the inclusion of a provision that recognises that the entity has obtained the views of impacted individuals or independent victim support services, such as IDCARE, as to the likely real risks of the information that has been breached and whether measures implemented have or are likely to mitigate harm.

Notification of Serious Data Breaches

IDCARE strongly supports the draft paragraph 26WC in requiring reporting entities to take reasonable steps in response to a serious data breach. The timings of such steps do influence the degree of harm that is experienced by impacted individuals. Criminals responsible for serious data breaches have been assessed as taking on average 72 hours to exploit the identifying information obtained. Individuals impacted by such breaches can spend in excess of one hundred hours in seeking to mitigate risk and respond to further misuse of such compromised

information. The longer an entity takes to inform an individual, the more harmful this will be for both the entity and the individuals concerned. This means organisations must act quickly. Where organisations have engaged IDCARE looking for our services to support impacted individuals, we have observed some organisations taking days to notify, not because they are assessing the nature of what has been breached, rather the time they take to craft the “right public message”. Our advice to organisations when responding to data breaches is tailored to the circumstances they confront and the very large library of tested mitigation strategies. But consistently, IDCARE’s position on communicating to impacted individuals is that waiting will not make things any better, in fact, it is likely to make things far worse. Communicating to impacted individuals does not mean that all needs to be known. IDCARE has received excellent feedback from businesses and their customers where they have acted quickly to inform, offered strong and meaningful support, and create a very real and genuine view that these organisations care about their customers’ identifying information. Given the criticality of time and the need to rebuild and restore confidence, IDCARE recommends under paragraph 26WC that the Department and legislators consider placing prescribed timeframes for personalised and public notifications given the imperative of time.

Kind of Information

IDCARE strongly supports the draft paragraph 26WB that provides flexibility in relation to the kind of information captured under the amendments. Given the nature of empirical data provided in this submission on what is compromised by clients and traded within dark net forums, as a minimum, IDCARE would encourage the regulations to capture identity credentials and related identifying information provided in Appendix B of the National Identity Proofing Guidelines. IDCARE is satisfied that the Bill as currently drafted has the ability to absorb future identity credential innovations, including digital identity information.

Conclusions

IDCARE welcomes the efforts by the Parliamentary Joint Committee on Intelligence and Security and Government to provide meaningful consultation on the refinement of the notification of serious data breaches Bill. On behalf of the many thousands of Australians that have benefited from our community service we sincerely thank you for what has the potential to become a key pillar in Australia’s mature approach to the response to data breaches. IDCARE stands ready to assist Government, the Department and the Office of the Australian Information Commissioner in further refining and supporting the effective implementation and operation of these provisions, particularly where entities need independent advice on the risk, a meaningful response to such occurrences, and a desire to place the needs of individuals impacted at the centre of our response efforts.