Australia and New Zealand's national identity and cyber support service

IDCARE SUBMISSION TO THE GOVERNMENT'S 2020 CYBER SECURITY STRATEGY DEVELOPMENT

IDCARE Submission to the Government's 2020 Cyber Security Strategy Development

Executive Summary

IDCARE congratulates the Government in developing and now renewing a national strategy on cyber security. Given the rapid change in the security environment and the impacts this is having on our community, there is no better time than now to recast and reset a new Strategy. IDCARE's submission highlights a unique lens on the cyber security environment. As a response and supporting mechanism, IDCARE receives reports from members of our community directly impacted by events where cyber security has been absent or failed. We know intimately from our privileged position how Australians across our country and travelling abroad are responding to cyber threats and the impacts they are having. From this vantage point we have focused our submission on the areas we feel most capable of contributing our views. There are many areas of cyber security we have not touched upon, and leave that for others with much more skill and expertise to do so.

Cyber security threats and the negative impacts these have on the Australian community are driven by a number of key influences. Our Submission highlights those that relate to Australia's deterrence positioning, the very nature of the globalised threat, the commodification of attributes and information that such threats seek to exploit, reflections on response as an exception to business as usual and the ownership of such risks, and the overall nature of the response system from an impacted individual perspective.

There are positive indictors of effective change across parts of our response system to cyber security threats. Major financial institutions and some elements of Government (at all levels) are starting to invest more in prevention, awareness, and reporting. But this context is a complex one for law enforcement and traditional methods of policing. Community attitudes towards response in this context is growing in discontent and this particular part of Australia's cyber security posture by Government is having its trust eroded. We hear this every day when IDCARE engages community members about their "response system" experiences. This is being driven by a posture that in our view is prioritising outcomes that are not in the interests of the community. We have arrived here because the previous strategy and accompanying resourcing did not focus on community impacts and response standards and experiences at an individual level. It is therefore unsurprising that this endures as a key weakness and vulnerability in the existing system and one that calls for the new Strategy to highlight a need for a National Community Response Plan.

We encourage Government to continue to bolster its diplomatic and foreign law enforcement relationships in an expanded network to include corporates dedicated solely to cyber security information requests, sharing, and response assistance. Established networks in our view fall short of the timeliness and insights required, and are largely the preserve of Government. Connected with this is a proposal in our submission for Government to establish a permanent Virtual Taskforce in partnership with key Government and industry stakeholders in relation to communication channel exploitation that reports via existing governance arrangements to COAG. The persistent exploitation of such channels and the ingenuity of the threat environment demands a much more agile and engaging approach than what currently occurs.

We position the role of Government as one that rationalises activities and responsibilities in relation to prevention and awareness, acknowledges the reporting of events by the community is no longer an outcome measure in its own right (at the exclusion of what happens next), and much greater effort and attention is spent on understanding the enablers of cyber security threats in our legitimate economy and their correction (including much greater emphasis on disrupting the criminals responsible). We have seen and predict an eroding trust in Government in relation to responding and deterring cybercrime if such changes are not addressed under the renewed Strategy.

The establishment of the Joint Cyber Security Centres across Australia in our view should be expanded to every State and Territory capital city. We encourage the Government to resource the establishment of Resilience & Response Hubs in each of these locations, including an expanded network of IDCARE Identity & Cyber Security Counsellors that can work alongside Government, law enforcement and corporate representatives in these locations to enhance information sharing, resiliency measures and rapid response to community members requiring immediate intervention. As an organisation we are experiencing inequality when it comes to our funding, particularly by the Commonwealth Government, and we encourage Government to take immediate steps to address this critical shortfall in resources.

Our submission offers ideas around how Government can explore existing levers it has to affect change. We would like to see specific areas of focus in relation to the applicability or extension of consumer protection and related product safety laws and their relevance to organisations that are found to enable transnational cyber criminals achieve their ends. We would like to see Government explore under the proposed Virtual Task Force additional controls, standards and regulations to ensure prevention and response measures are maximised in partnership with industry.

Existing capabilities, such as those provided by ASIC, AUSTRAC and the ACCC should be further explored, including the development of an expended national Project Sunbird equivalent (an initiative of the Western Australian Government) that is further enhanced with aftercare, persistent risk treatments, and a rapid response intervention capability utilising IDCARE's expert behaviouralists.

The great positive is that Australia has a number of ingredients to make the next Strategy one that achieves considerable outcomes for our community. We are clear in our view that the online environment has so many positives to give our country, but associated risks need to be appropriately articulated, prevention supported, and response to their manifestation much more appropriately considered.

1. Introduction

1.1 Thank you for the opportunity to submit our thoughts and share our experiences in relation to Australia's impacts, responses and strategies on cyber security. We welcome a renewed national strategy given the rapid pace of change across industry and government. The threat and its impacts on our community are affecting many Australians who have come to use technologies to improve their way of life. However, Australia's response to such threats and impacts is currently a long way from being equal to the task. This is a shared responsibility and not one that any individual Government (or agency), business, community group or victim cohort can pursue in isolation. Put simply, the exploitation of a networked world demands a networked response.

1.2 IDCARE was launched in 2014 by the Commonwealth Minister for Justice as Australia and New Zealand's national identity and cyber support community service. The organisation embodies what can be achieved when Governments and industry listen to the needs of our community in building a response service that addresses the emotional and pragmatic issues confronting people. Our role is unique and not one that duplicates others, nationally or globally.

2. Our Lens and Perspectives

2.1 To afford transparency and consideration of this submission it is important to recognise that IDCARE is a registered not-for-profit organisation and Australian charity. We are not a Government agency nor do we benefit from receiving annual government appropriation despite doing a large amount of work on behalf of Governments. Our funding streams, albeit a constant challenge, come from a few organisations in industry and Government who demonstrate leadership and genuine concern for the well-being of their staff and customers, and who take an ethical stance that referrals to IDCARE should be accompanied by a financial contribution to assist our organisation cover the costs of delivering our community services. We simply could not survive as an organisation without this funding support. This submission does not reflect the views of these funders, and for some, our thoughts and views may be somewhat controversial, but they are made in the hope of being transparent and meaningful for those charged with drafting our country's next strategy.

2.2 Often we view IDCARE as being the "canary in the coalmine" – an analogy to the overall health of the cyber security response system and its impact on the Australian community. An enduring challenge our organisation faces comes from a combination of a persistent and growing threat that feels largely untouchable, the exploitation of weaknesses in our information economy, and a large portion of the response system that refers cases to IDCARE without any equivalent flow of funding – perhaps reflecting that cyber security response is someone else's responsibility. Since 2014 IDCARE has responded to over 160,000 engagements from members of the Australian community who have experienced cyber-enabled crimes either resulting in the compromise of personal and account information or their online misuse. The demand for our service continues to grow exponentially (averaging at present around 57% per annum). By the end of 2021, IDCARE can expect to receive over 100,000 engagements per annum. Our service is heavily relied upon by the Australian Cyber Security Centre, ScamWatch (the Australian

Competition & Consumer Commission), the Department of Foreign Affairs & Trade, and the Australian Taxation Office – none of which contribute to the $1.4 million in costs their case referrals create for IDCARE each year. This needs to be addressed as a matter of urgency, and will be the focus of an engagement campaign in November 2019 called "making good" – where organisations will be asked to contribute to the costs they impose on IDCARE in caring for their customers and the community at large.

2.3 Despite this growth, our client satisfaction rating remains the strongest of any organisation in Australia (average 8.7 out of ten). We believe the reason for this enduring community sentiment is because we have found the right mix of empathetic care with the provision of the most up-to-date pragmatic response advice aimed at reducing harm for each person tailored to their needs and concerns. Our frontline staff are qualified counsellors, social workers and psychologists and we invest heavily in training them to become Identity & Cyber Security Counsellors. Such a cohort exists nowhere else. These staff work as case managers with individuals from all walks of life to provide expert care and knowledge on how best to address immediate issues and concerns, and build resilience to the inevitable risks of identity and account misuse that many of these crimes pose to our community. This is a free community service aimed at providing essential relief to those that now have very tangible risks to their online and offline environments.

2.4 We're told by foreign governments that this blend and service mix is a world's first. We've certainly had strong approaches by Governments across the world to replicate our model and we continue to be recognised by our peers in national awards for innovative service and delivery. There's something about performing a response mission integration activity that truly puts the individual at the centre that works in filling a very large gap in the cyber security response system. Sadly this is unique. For most Australians, the response system to cybercrime, scams and identity crime is absent. There appears little deterrence from law enforcement, and in some quarters, little interest. In this submission we will be providing case studies that highlight this point. We do so not to embarrass responders, but to highlight the complexities that confront our community when cyber security and response is not prioritised.

3. Structure

3.1 This submission draws heavily from the privileged position we have from engaging our community and listening to their needs and experiences each day. It is not a paper that talks about the absence of technical controls, although there are many, a large number of which could be readily addressed by organisations and individuals following guidance from the Australian Cyber Security Centre (ACSC) and the Australian Competition & Consumer Commission's (ACCC) ScamWatch. There are "easy" wins for technology companies and software vendors as well in deploying capabilities where security features are already enabled and not something a user needs to identify, learn and implement themselves. Cyber security for most is a concept that conjures up imagery of coders and programmers beavering away on machines in a manner that demonstrates a fluidity of language beyond the grasp of mere mortals. It is an industry that has perpetuated from an asymmetry of knowledge between the expert and the user, where concepts and workings of cyber security can be perceived to be out of reach for most. We hear this a lot in our community engagement, whether on the phones or during community awareness raising events. It is a perception and at times a culture that is not useful to bridge the gap in promoting and enacting safe cyber security practices. We’ve attended many school events where “experts” are telling kids not to use social media. This is no solution. Technology is not something we should be teaching younger generations to fear (or any generation for that matter). There are so many benefits to come from technology, but like any human invention there are risks.

3.2 Instead we will be focusing on what we think are changes that could be made that are the most scalable and impactful for Australia – business, government and the community. We will seek wherever possible to answer the questions posed in the document produced by Government entitled *Australia’s 2020 Cyber Security Strategy: A Call for Views*. We have been selective with these in terms of those we feel we are in the best position to answer because of our work.

3.3 Importantly we submit these ideas as IDCARE and not as being reflective of any one individual we have assisted or organisation that we gratefully receive financial contributions from.

4. Where are we now?

4.1 If we applied an energy efficiency star rating to Australia’s cyber security threat response system, we would be lucky to obtain 1.5 stars out of five. IDCARE knows this because we ask community members to reflect on their engagement and response experiences across the system each day – including asking community members to rate their experiences across the system to address their needs. The worst performers since 2014 have repeatedly been law enforcement, credit bureaus, ISPs and large foreign technology companies, as well as social media platforms and telecommunications carriers. This is a broad and consistent church of community discontent. Thematically a number of observations driving this discontent emerge and are summarised as follows:

- **Deterrence and the globalised threat:** There is little to no deterrence for criminals who exploit online channels, dominated by growing offshore threat environment and the non-applicability of traditional law enforcement responses;
- **Commodification:** Underpinning the vast majority of these crimes are personal attributes, including images, and account information that have been “commodified” via a vastly expanding information economy (ie. criminals are exploiting the value not placed on such information);
- **Exception to Business as Usual:** an incident or event and its management for many actors in the cyber security system is the exception to the rule. This means response experiences for individuals have high degrees of friction, are repetitive, ask consumers to communicate through the same channels that they have just been victimised on, and share the very same details that have just been stolen or misused to commit other crimes;
- **Literacy and comprehension:** the need for translation when the response system demands actions and information from consumers that is using language and terms quite foreign to community members;
- **Empathy and risk ownership:** organisational response is naturally skewed towards addressing a specific organisational risk and absent of understanding or acknowledgement of the broader

risks to the individual – their stop with one organisation is often one of many. It is too easy for no one organisation to take responsibility because it is a "system" issue – in other words, that community member's concern is someone else's problem.

4.2 There are positive indicators of some change. Pleasingly the major financial institutions are investing in scam, cyber security and identity crime response more than at any other time. We have seen community sentiment improve when it comes to reflecting on the response offered by Australia's major financial institutions – particularly over the last 24 months. We have also seen corresponding shifts with Government agencies where they have dedicated teams to victim response interface, such as the Commonwealth Department of Human Services. IDCARE knows that in the vast majority of cases, community members when interfacing these organisations will not be harmed. However, the same cannot be said of the vast majority of other interactions with other organisations in Government or industry.

4.3 We deliberately do not distinguish between these crime types because all are influenced and enabled by the online environment. We have found perhaps too much pre-occupation with some quarters on whether certain crimes are "technical" enough to warrant attention. The community could not care about how any one organisation chooses to define cybercrime, but we know all too well that this influences whether response agencies will devote precious resources to the community member's cause. This extends our thinking on the challenge of ownership. Government under the existing strategy has been pre-occupied with capturing reporting, almost at the expense of any meaningful action. Everyone knows cybercrime and cyber security threats are growing and highly impactful. Any one organisation across Government, industry or the community sector can raise awareness. But typically most efforts to intervene and disrupt reside with Government. Inviting community members to report for the sake of reporting is no longer good enough. We caution individual clients when they report to law enforcement with the caveat that (1) they probably won't hear back; and (2) don't expect an arrest. This is a sad state of affairs as the consequences for these Australians can be devastating, and in some cases, result in the tragic loss of life.

4.4 To quote just a handful of IDCARE clients that provided a representative and anonymised view of the community experiences with law enforcement in response to their cybercrime in the month of October 2019:

4.4.1 "*I went to the bank and told them the account details of the fraudulent account listed/recorded in the fake invoice changed by the cyber criminal. Bank said they will only look at my case if I provide a police report. Police sent me to cyber.gov.au. Cyber.gov.au came back saying they could not help.*"

4.4.2 "*They told me to ignore the calls from the debt collector, saying they were scammers, when in actual fact they turned out to be legitimate.*"

4.4.3 "*Pretty uninterested which was a surprise for me*."

4.4.4 "*Went to local police station. Was told to get a report from my Telco, and that they could/would not do anything further without it. Was given a fraud form to fill in and return with a copy of my*

Telco's statement, as well as a Stat. Dec. No advice, nor useful assistance provided."

4.4.5 "*Police were not transparent, they were difficult to get on to, did not explain what was going on and client was left to chase them up.*"

4.4.6 "*I was surprised the Police were not interested in the issue and when I rang them they only read to me from their website. I am frustrated and I will be contacting the Ombudsman, as the reaction of my Telco and the Police is totally unacceptable*."

4.5 The issue is a complex one for law enforcement and traditional methods of policing, coupled with a strategy to create an online reporting mechanism that does not appear to address the needs of its reporters, demands that the way forward requires a fundamental rethink on existing practice. Community expectations in relation to police and crime response are strong, but in the context of cybercrime the challenges are significant and from our view of client experiences rarely are expectations met. Community members to experience cybercrime often have direct engagement with the criminals, and such events are rarely "one-offs", but commonly result in multiple engagements and criminal exploitation even at the time of reporting to law enforcement. Crimes reported to police for the most part have occurred, an event has taken place, such as the burglary of a house and the theft of a car. Cybercrimes are different. Events, such as the unauthorised access of emails, the exploitation of compromised credentials, or the persistent communication with online scammers often continue throughout a community member's engagement with law enforcement.

4.6 For the most part criminals are based offshore, and the types of crimes committed would best be described as high volume – low value. Structurally Government struggles with responding to these threats. Specialist resources from enforcement must be prioritised, and often this prioritisation is influenced by the dollar value or impact of the alleged offending. High volume – low value events tend to "slip under the radar" when it comes to law enforcement and broader Government response prioritisation. Telephone scammers are a useful case in point. Since IDCARE's inception we have witnessed a rapid escalation of telephone scam activity. Work with some of Australia's telecommunications carriers and global technology companies has revealed that many of these scammers operate from the Indo-Pacific region with some groups numbering in excess of 5000 people, calling Australia seeking to obtain payment under the pretext of impersonating large Government and business. Only until very recently, IDCARE struggled to draw this growing threat to the attention of Government. To most in Government and law enforcement, the view we witnessed was one that interpreted such events to be merely a phone call from a scammer, and not a sophisticated and growing transnational crime threat. In response to this absence of interest, IDCARE would test scammer numbers, identify the carrier hosting the number, report it to the carrier and hope in good faith they would investigate and cease the number from continuing. Whilst this could accurately be viewed as a "whack-a-mole" approach, akin to domain takedowns for fraudulent website and phishing emails, it was at least something that our charity could do in the absence of any coordinated effort by those charged with enforcement.

5. Where we need to be

5.1 The Federal Minister for Communications & Arts' recent direction to telecommunications carriers to enhance their evidence of identity procedures as one means to reduce the growing prevalence of unauthorised mobile phone porting events is welcomed. IDCARE in partnership with the Australian National University and the University of the Sunshine Coast undertook research on this particular form of crime to motivate change that was otherwise lacking at an industry level. Much more work needs to be done. Telephone scams remain the most prevalent way cybercriminals steal personal information in order to commit further online crimes against the Australian community. The Government's strategy to utilise diplomatic and foreign law enforcement relationships must be bolstered and acknowledged as a key and enduring part of contemporary and future diplomacy. Economies from which many of the threats impacting our community are important for legitimate trade and commerce with Australia. Many of our large corporates rely on offshore call and data centres in these locations. These offer important opportunities for Government to work with their foreign counterparts to enhance response capacity in nation-states where criminals are specifically targeting Australians, seemingly with impunity.

5.2 We have since welcomed the joint work of the ACCC, the Australian Communications & Media Authority (ACMA), and the ACSC in exploring the exploitation of communications services and the opportunities for its disruption. We would like to see tangible and practical outcomes from this work, including:

5.2.1 A permanent Virtual Task Force be established consisting of members from law enforcement (State, Territory and Commonwealth), key national regulators, carriers, financial institutions, technology companies, the Department of Foreign Affairs & Trade, and IDCARE:

5.2.1a Reporting to COAG on how Australia's communications systems (telephony and online) are currently being exploited by transnational crime and the impacts to government, business and the community;

5.2.1b The development, implementation and reporting on outcomes from national prevention and awareness campaigns promulgated throughout participating industries and sectors (including established prevention forums);

5.2.1c The co-design of enhanced user / consumer controls to disrupt the activities of transnational crime, including regulatory amendments, directives and self-initiated actions and the reporting on their impacts;

5.2.1d The development of a virtual international network to enhance the establishment of prevention, investigation and disruption alliances (government and corporate), assistance requests, and information sharing dedicated solely to communications systems exploitation and its response (outside of current, but shared mechanisms of international engagement that are cumbersome and not aligned with the rapid response required of this context);

5.2.1e Leverage and enhance efforts of the ACSC to develop a virtual information and intelligence sharing network dedicated to telephone scams, phishing and smishing campaigns, unauthorised mobile porting, SIM swapping and any other relevant and impactful communications exploitation methods pursued by transnational crime.

5.2.1f Enhance the participation of Australia's diplomatic and corporate advocacy bodies and councils and their support of foreign Governments and corporates domiciled in regions that are proximate to the threats impacting Australia to work together to disrupt such threats.

5.2.1g Development of standards of response and the education of such standards across responders, including frontline policing, on how to address the needs of community members, key response advice, and data collection requirements.

5.3 This idea may seem somewhat grandiose for what is perceived by many in enforcement and Government to be a mere nuisance. But today we would be hard pressed to find an Australian who has not experienced an attempted telephone scam, phishing email, and increasingly now a fake SMS (Smishing) text. The exploitation of Australia's communications system will endure and presently there is no real deterrence or coordinated effort that seeks to address this threat on behalf of the community in a systematic and strategic way. If there is such efforts are not visible, and from IDCARE's perspective we are not seeing any tangible difference being made with respect to the volume and impact such measures are having on the community. Without such an approach, the exploitation of Australia's communications system will grow and the trust required by the community in their legitimate engagement with business and government eroded.

5.4 We have seen telecommunications continue to offer enabling services to transnational crime that impact our community. Spoofing or the disguising of originating phone numbers is growing in prevalence and victimisation rates. It is publicly known that brands such as Australia Post, major financial institutions, the Australian Taxation Office and the Department of Human Services (including MyGov), have all had their SMS communications origination numbers "spoofed". The consequence of these actions is that criminals are able to send impersonation text messages pretending to be these large brands across the community where the message itself once received enters the historical and legitimate communication chain between the recipient and that organisation. This is particularly effective for criminals and such events have considerable consequences for the demand for IDCARE services. This is but one area that would benefit from the focus of a Virtual Task Force.

6. The role of Government

6.1 There has been a notable stance taken by Government and law enforcement in relation to their prioritisation and response to cyber security threats since the first Strategy. Whilst much greater public attention has been drawn to State actors and their ability to interfere via online channels, for cybercrime more generally the focus has been almost entirely on prevention, awareness and reporting, often what may be perceived to be at the detriment of disruption. How many arrests have been made of cybercrimals impacting Australians from offshore when considering the events Australians experience? If cybercriminals are making $2.3 billion a year from Australian consumers, how much of this was recovered from proceeds of crime action? Who are the main threats and what legitimate parts of the Australian economy do they leverage to achieve their ends? How can the diverse levers of Government and the corporate sector be used to disrupt and build our community's resilience? These are the questions that go to the heart of Government's role. Any organisation can jump on to the front page of a newspaper to raise awareness about cybercrime and cyber security. The media has an insatiable appetite for these stories. But there remains only one part of the economy that can take action and answer the questions posed – that is Government.

6.2 This role challenges the status quo. Government is not traditionally geared to respond to threats that continue to unfold as they are reported, that morph and change constantly, and require a significant dependency on corporate and community reporting to remain abreast of such changes. It is no longer good enough for Government to say "report to us" and have a perception build within the community that nothing is happening. The community has become much more discerning and, in some pockets, skeptical of the role and value of merely reporting events to Government. Our observations of these mechanisms and their development has formed our view that the focus of Government has been on creating an environment where reports are captured and sent to the relevant agency, rather than the outcomes from such reporting from the community's perspective. There is little value to the system by just knowing we have a problem or by knowing that a report has gone from a central repository to an individual agency. The community expects much more than knowing that the report was received. Many IDCARE clients hold a view that people who commit crimes will be investigated and brought to justice. This is a considerable gap in Government's current role in combatting cybercrime.

6.3 A positive development by Government initiated under the previous strategy has been the implementation of State and Territory Joint Cyber Security Centres. IDCARE has supported this establishment and one of our expert analysts frequents weekly the Brisbane Joint Cyber Security Centre. These interactions have been very useful in sharing insights and trends on what's impacting the community, business and Government. The development of secure online sharing environments is also a positive step to allow for participation and awareness of organisational representatives not able to physically convene at these sites. Further enhancing the information flows from Government on new and emerging threats should remain a continued priority in building intelligence and response networks across industry and government. The following case study highlights this point.

Case Study on the Benefits from JCSC Collaborative Arrangements on the Community

In early June 2019 IDCARE's JCSC Brisbane liaison officer informed the ACSC of an alleged investment fraud company impacting Australians via adds on social media. An Alert was issued via Stay Smart Online within the week. Within one business day of the Alert being issued via Stay Smart Online (ACSC), four separate reports came in to IDCARE from members of the community who had seen the Stay Smart Online Alert and ceased their investment at the initial amount of $250. The average loss attributed to this alleged investment reported to IDCARE prior to Alert was $318,200 (AUD). These loss amounts represent the accumulated amount of money individual Australians were investing in this alleged scam, all of which were unrecovered and resulted in clients having to seek Centrelink (pension) support. Some had sold their property, all claim the investment decisions had permanently altered their family's financial security. This one Alert is likely to have prevented at least a million dollars going to *the alleged overseas scammers, but the real total is likely to be much higher when consideration is given of the estimated cost to the welfare system and the incomplete number of reports to IDCARE (we estimate we receive between five and ten percent of the total volume of what’s impacting the community).*

Despite the success of this case, there were problems. Both IDCARE and the ACSC lobbied ASIC to post the details of the alleged fraud on <moneysmart.gov.au> - this is a site that lists investments that are believed to be fraudulent (and the entities behind them). In this case, like many others IDCARE has dealt with on investment frauds, foreign regulators that perform equivalent functions to ASIC are publicly disclosing investment frauds that are not disclosed on <moneysmart.gov.au>. This is considered further in our Submission. As at end of October 2019, the alleged investment scam has yet to be published on ASIC’s <moneysmart.gov.au> site. We expect that many other Australians have fallen for this scam since.

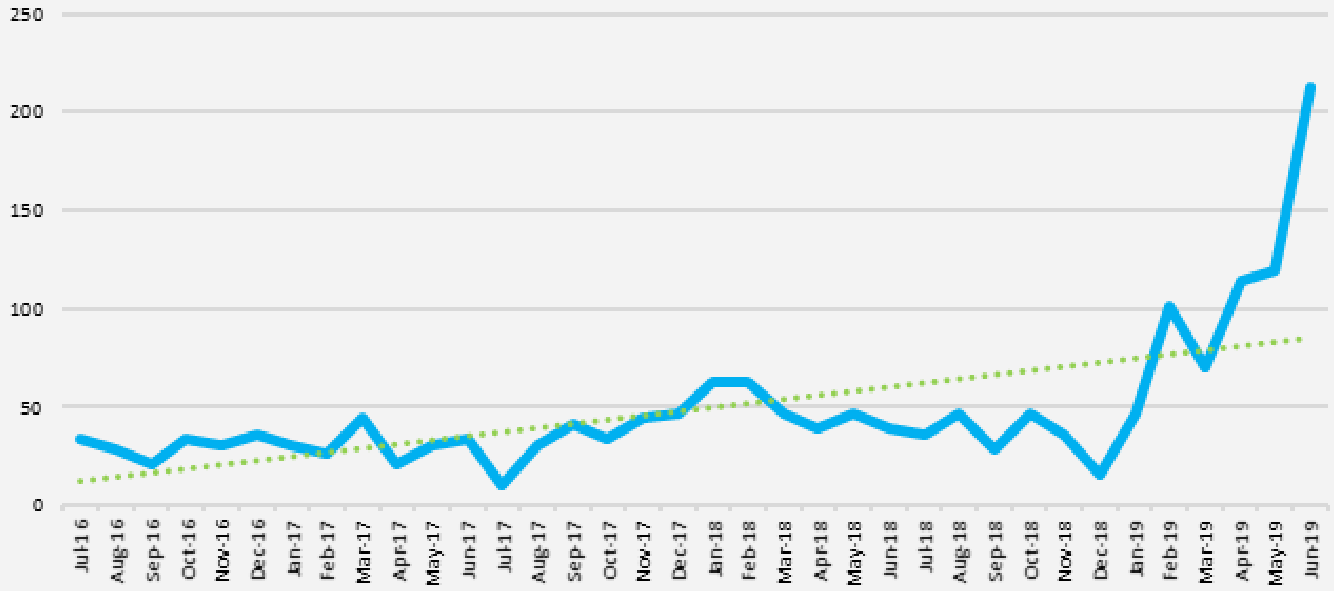
6.4 To further expand the presence of each Joint Cyber Security Centre in every State and Territory capital city and to establish more formalised joint industry and Government intelligence sharing, prevention, response and resilience arrangements, the new Strategy should look to template joint law enforcement, State/Territory Government, and industry task forces that overlay national and international efforts on the local environment. Each JCSC should be in a position to determine at any point in time what is impacting their relevant State or Territory location, the formulation of localised strategies to prevent, disrupt and respond to such threats, and aggregation / cascading of these with national and international efforts. Clearly flexibility is required as local representatives that come to the JCSC may do so on behalf of organisations that have national and international reach. IDCARE cannot afford to have representatives in each JCSC location, despite maintaining awareness of what cybercrimes are impacting every State and Territory. We would welcome efforts under the new strategy to explore this, including potentially having IDCARE cells within each JCSC to deal directly with impacted community members sitting alongside representatives from State and Territory Government and enforcement agencies to further augment our National Case Management Centre and improve the performance of the response system. These “resilience and response hubs” would look to expand the type of work and outcomes identified in the previous case study as well as act as key nodes and interface between government, business and what IDCARE is seeing impacting the community.

6.5 There are a number of additional pragmatic ways Government can enhance prevention, response and resilience efforts. These ideas have come from our capture of community response experiences and knowledge of how threats currently exploit the legitimate economy. To provide some granularity to these considerations, we break these ideas down into threat type and in some cases channel for consideration:

6.5.1 Investment Scams

6.5.1.1 Investment fraud scams are amongst the most impactful scams confronting the Australian community in terms of direct and irrecoverable financial losses and physical and mental health impacts. It is not uncommon for victims of investment scams to lose their entire life savings. They are commonly life changing events for individuals and their family. The age of most victims is in their sixties and older. Certainly there are elements of responsibility that most clients of IDCARE accept that rest on their shoulders for taking action and performing (or not) appropriate due diligence. The below graph provides a sense of the trajectory of victimisation resulting from investment scams impacting the Australian community over the last three years.

Investment Fraud Case Engagements
2016-17 to 2018-19 (3 years)



6.5.1.2 We believe the spike is largely attributed to a corresponding increase in usage by scammers of fraudulent endorsements by celebrities on social media advertisements of crypto-currencies. The same period also saw a jump in Bitcoin and other crypto-currency prices (almost tripling in value over the period from January 2019 to June 2019) and a steady and historically low cash rate, perhaps tempting investors away from keeping savings in interest bearing accounts towards other forms of investments. These externalities or market forces have made Australians more susceptible to investment fraud attempts as reflected in the above graphic.

6.5.1.3 We have found that moneysmart.gov.au maintained by ASIC is a useful community reference point for investment scams. However, the time it takes ASIC to post suspected investment scam information is too long and does not match the speed and agility of the adversary. The following case study highlights this point:.

Case Study on the Consequences of Alerting Inefficiencies

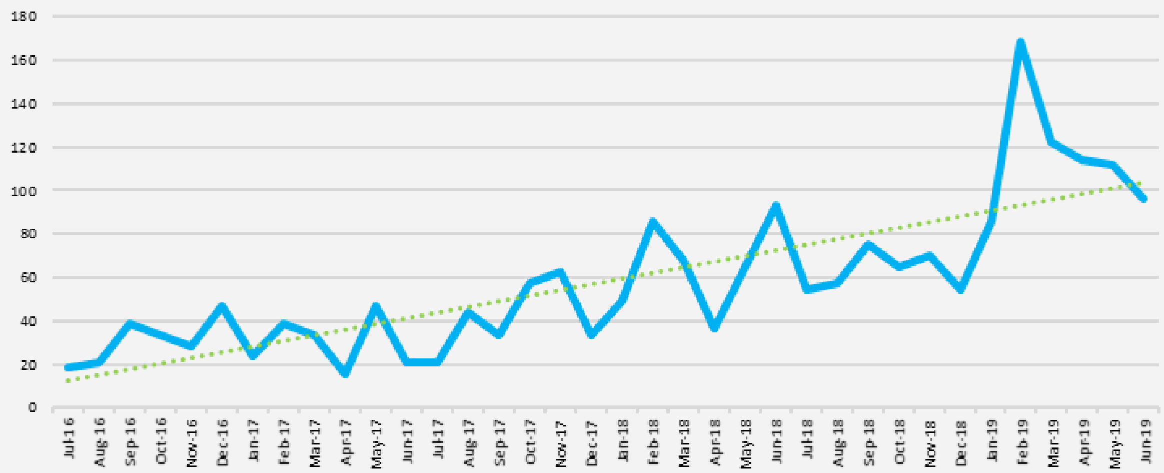
In December 2018 an elderly couple from Brisbane engaged IDCARE suspecting they had become involved in an online investment fraud involving crypto-currency trading. The name of the investment firm was not located on <moneysmart.gov.au>. Throughout January and February it was discovered that two foreign Government regulators of investment markets had posted consumer warnings about the investment dating back four years. The elderly couple lost in excess of $300,000 and are now more dependent on the welfare system. The couple accept they made mistakes and were the ones to invest, but their experience shouldn't detract from the fact that other overseas regulators called the investment scam out some years ago.

6.5.1.4 IDCARE would like to see ASIC create an international scam notification portal on moneysmart.gov.au that connects alerts relating to suspected international scams posted by their overseas counterparts. A cursory search of such regulators by IDCARE has identified 54 such websites and repositories as at October 2019 that contain information about suspected investment scams identified by overseas regulators. We would welcome meaningful engagement with ASIC on establishing this portal and a more formalised arrangement in connecting victims of investment fraud to IDCARE (at present ASIC refers community members without any formal arrangements with IDCARE).

6.5.2 Relationship Scams

6.5.2.1 Like investment frauds, relationship scams are certainly increasing in volume in terms of IDCARE clients reporting such activities. This scam type is heavily dependent on other actors detecting the scam on the client's behalf. In turn this influences the average detection time. This is a consistent theme across crime types - where we see a higher dependency on third parties to detect, the detection time is much higher when compared to self-detected events.

**Relationship Scam Case Engagements
2016-17 to 2018-19 (3 years)**



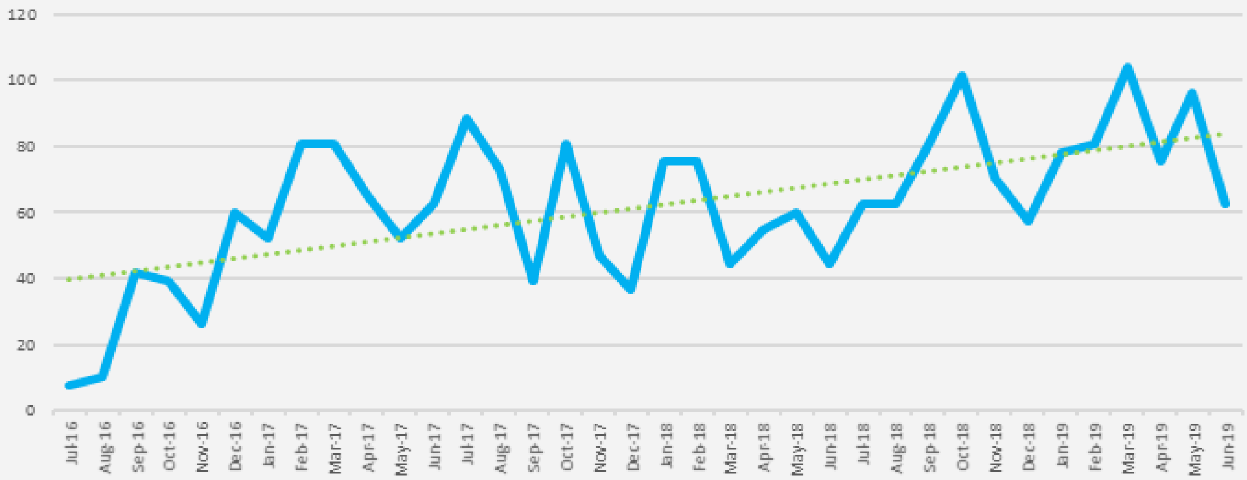
6.5.2.2 Key enablers of relationship scams are social media outlets and dating websites. These represent the most common channels individuals first connect with scammers. There are few warnings and little advice provided by these outlets for their users about scams generally. Response experiences are equally disturbing, with limited contact options available and typically North American centric advice on what consumers should do. Opportunities present for Government to be much more active here in its application of consumer protection measures and the regulation of such service providers to ensure they are operating safely – including extending the concept of "product safety" to the services offered that transnational crime relies upon to achieve their ends. IDCARE has made tentative steps with a number of these key enablers in looking to improve awareness, response and overall service safety, but often we are told that they would prefer this in the form of formal Government directives and regulation before they would act and/or their company operates beyond Australia's border and as such developing something bespoke for Australia is not a priority of theirs.

6.5.2.3 From our recent experiences many victims of relationship scams find themselves in positions where they are not just being defrauded of their own finances, but are acting as conduits to launder proceeds of crime on behalf of criminals (such as business email compromise and false invoicing fraud). In some extreme cases reported in the media, some individuals have found themselves involved in "drug muling" activity. An opportunity exists to further the work of the AUSTRAC initiated FINTEL alliance in proactively identifying Australians that may be caught up in relationship scams (or investment, employment and telephone scams) through following the money and reverse engineering how many other Australians are sending money to the same accounts. Project Sunbird as an initiative of the Western Australian Government is an excellent case in point. IDCARE would welcome this being performed at a national level via the FINTEL alliance with resourcing to appropriately fund aftercare for individuals and their family caught up in such scams. This shouldn't be viewed as "bolt on" and "in their own time" capability. These crimes are occurring in real time and intervention or the opportunity to work with community members to reach conclusions about their involvement requires a real time response. On occasion IDCARE has been asked by financial institutions and police to support their efforts to intervene at the penultimate stage of a scam – such as when the victim is literally in the bank branch looking to send funds or is about to board an international flight to visit their "loved one". Our intervention services need funding to enable the effective deployment of our specialist Identity & Cyber Security Counsellors at any time day or night. We have found that specific scam and cybercrime behavioural engagement strategies are more successful than others in de-escalating and empowering community members to withdraw from engagements with criminals. This is a capability we are hamstrung financially from deploying nationally, but the work performed to date demonstrates concept and a need for IDCARE outreach to improve. Such capabilities could reside in each of our proposed "Resilience & Response Hubs" within an expanded JCSC network.

6.5.3 Employment Scams

6.5.3.1 Employment scams, much like relationship scams, are key vectors that enable the laundering of criminal proceeds. Unlike investment scams, the majority of impacted customers are under 25 years and are typically students. During the last financial year (2018-2019) IDCARE witnessed a number of sophisticated business email compromise attacks impacting education providers specifically designed to recruit students for the purposes of laundering proceeds. Like other impactful scam types, employment scams do converge with other scam methods given the nature of its intended purposes – to launder funds on behalf of criminals committing other crimes.

Employment Scam Case Engagements
2016-17 to 2018-19 (3 years)



6.5.3.2 Like relationship and investment scam clients, employment scam clients require IDCARE services to work in partnership with financial institutions and law enforcement to provide a rapid intervention response service. Resourcing constraints at present do not permit IDCARE to meet the demand for this form of intervention and under the Strategy we are seeking support to expand these services to ensure that when Australians are in a moment requiring expert and specialist de-escalation care and support, IDCARE can provide this.

6.5.3.3 Akin to social media and dating websites for relationship scams, employment scams also prey upon legitimate social media outlets, in addition to job seeking websites. Since the last cyber security strategy IDCARE has even alerted Government that its own job support network has been targeted by transnational crime to recruit job seekers to launder criminal proceeds. We think there is scope under consumer laws (such as the *Competition and Consumer Act 2010 Cwth*) to explore the merits of adopting product safety regulatory frameworks to organisations that enable such scams to occur, but seem unresponsive to the known risks and impacts on the community. In these matters, the enablers of cybercrime, including scams and identity theft events, could be publicly identified as not addressing service safety risks to consumers where their products/services are used to enable fraudulent and deceptive conduct to other users of their service. Australian consumer law in its current form establishes that governments can impose mandatory safety standards or information standards, ban goods and services, and issue compulsory recall notices. The latter may not be so relevant, but the first two in our view have merit in exploring within a cybercrime and scam enabling context.

6.5.4 Telephone Scams

6.5.4.1 Telephone scams are prolific and have touched upon almost every Australian. As previously referenced, these events have struggled to gain priority given the high volume – low value nature of the offending. On occasions when IDCARE has raised this with Government cyber security stakeholders, the reception has not been positive, most arguing whether such events are even "cyber", "sophisticated enough to warrant attention" or "relevant". If Government wanted to make an impactful statement to the community in relation to cyber security and crime, we would encourage it to start with telephone scammers.

6.5.4.2 More than half of community members to experience telephone scams over the last five years have also experienced subsequent cyber (online) crimes. Some methods used by telephone scammers include convincing community members to provide remote access to their devices. In our view, there is an undeniable connection between telephone scams and cyber crime and security.

6.5.4.3 Offshore disruption from Government is almost completely absent. The use now of smishing or SMS-based phishing activity and spoofed originated numbers (that seek to impersonate business and government) are growing in the absence of any real deterrence. The proposed permanent Virtual Task Force on Communications Exploitation (see para 5.2) is one form that Government could take to initiate steps to build Australia's prevention, response and resilience to such activities. It would need to be careful that lobby groups and other interests don't diminish the integrity of what is set out to be achieved or its timeliness.

6.5.5 Email (Phishing) Attack Trends

6.5.5.1 Phishing attacks against the Australian community over the past twenty-four months have escalated in terms of reported cases and the financial returns for criminals. Like relationship and employment scam cases, the "bystander" (the family member or friend) plays much more of a detection role in phishing events than other cybercrimes. The average losses now for individuals to experience these attacks is much higher than before and the combined usage of SMS-text based (smishing) with spoofed numbers and fake websites are becoming popular for criminals. Phishing attack techniques to combine multiple forms of communication channels, emulate multi -factor authentication, and template / mirror legitimate business and government appearances and socially engineered actions are highly impactful to many Australians each year.

6.5.5.2 IDCARE's provisioning of independent harm assessments and response plans for organisations that are assessing the eligibility of notifiable breaches under the *Privacy Act 1988 Cwth* confirms that the deployment of multi-factor authentication and limiting of administrator access would have prevented the vast majority of breaches over the last 12 months. The ACSC's continued role in advocating key cyber security principles and advisories is a key contribution in this space that should be maintained in the new Strategy.

Case Study: Small Business and the Cyber Knowledge Asymmetry

A small business operator experienced a ransomware attack that disabled the company's ability to process customer orders, pay bills and generate invoices. The company suffered immediate cashflow risks and were unable to pay their staff over the coming fortnight. They had cyber insurance which was denied because their external IT service provider had not backed up their data offsite – they were deemed to be in breach of their policy. This was after the company had paid a forensics firm recommended to them by their insurer approximately $15,000 to decrypt their data. The ransom the criminals were asking for was $2,500. The ransom was deployed because the company's email account had been compromised following a spear-phishing attack where the CEO's email address had been "spoofed" and a link deploying the ransomware executed by the recipient. The business employed sixteen staff, that accumulatively were supporting 82 other family members. The business survived because the owner sold personal assets to re-inject capital until their systems were re-built. The business owner did not know about free online decryption tools, spoofing, or specific offsite back-up provisions in their policy. Whilst one can claim that ignorance is no excuse, the case highlights the knowledge asymmetry that the cyber security and threat environment can have on small business operators.

6.5.5.3 We continue to see Business Email Compromise (BEC) as a persistent threat to organisations large and small. Criminals are manipulating rules and filters, learning nuances in language and user social interactions, and advancing deceptive conduct towards false invoicing, payroll, and ransomware. For many small businesses the effects from these crimes can be devastating.

6.5.5.4 There is an ongoing role for Government to work with technology companies and email providers to explore what default settings could be enabled to enhance security standards on their products at the point of purchase / installation. There remains a significant knowledge asymmetry between providers of online products and the ability of consumers to secure against these persistent threats.

6.5.5.5 In addition, IDCARE believes that a review of the cyber insurance market is warranted in terms of its role in enhancing cyber resilience, the performance of these policies in terms of scope of offering, liability shift, and operation, as well as policy / claimant experience. This market continues to grow, and the experiences as captured in the previous case study are not uncommon.

7. The role of IDCARE in working alongside Government

7.1 When asked what the difference is between IDCARE and ScamWatch or IDCARE and Report Cyber (cyber.gov.au / ACORN) the answer is simple: ScamWatch and Report Cyber are reporting mechanisms;

IDCARE is a supporting mechanism. In addition to reporting, ScamWatch has considerable prevention and awareness capital, built over many years that resonates well as a brand recognised by the community at large. As a derivative of the ACSC and the community aware brand of StaySmartOnline, prevention and awareness activities are also performed by this mechanism. But they are not alone, and it is fair to say that the prevention and awareness space in Government is crowded and feedback in the provisioning of our support activities of the community reflects a confused view. We will address prevention, awareness, reporting and supporting themes and observations accordingly as well as opportunities for the future strategy to address points of confusion and any related inefficiencies that follow.

7.1.1 Reporting Mechanisms

7.1.1.1 IDCARE is aware of 28 separate Governmental reporting mechanisms relating to scams, cybercrime (including alleged image exploitation) and identity crimes. It is likely that almost all of these reporting mechanisms do not communicate with each other. Whilst one could argue that having many "front doors" to Government is of benefit to the community, this could only apply where the community is assured they don't need to knock on all the doors for information to be shared (including re-living and re-telling their experience so many times).

7.1.1.2 The way Government conceives reporting is not very useful. Community members are encouraged to report to ScamWatch, which could involve alleged crimes committed online or offline. Community members are also encouraged to report to "Report Cyber" or the ACSC if they experience cybercrimes, some of which could be classified as scams. In large part the community IDCARE engages couldn't really care how Government defines their responsibilities. They know they have experienced a crime, and they expect Government to respond. It's that binary. There is a value in what was initially set out to be achieved with the ACORN, now Report Cyber, in its holistic form. That is, a mechanism whereby members of the community shouldn't be burdened with working out which law enforcement agency has jurisdiction for their particular cybercrime event. This is a sensible policy foundation, but its execution and contemporary views of performance are not. What's been lost is the next step – understanding what the community member actually expects from reporting.

7.1.1.3 The community engagement satisfaction level with law enforcement since the commencement of ACORN and its continuation with Report Cyber has remained at harmful levels (averaging less than 3 out of ten in terms of addressing the needs of the community). Our qualitative data has identified three primary and consistent concerns from across the Australian community. The first relates to not achieving the law enforcement outcome they desired – namely an investigation is undertaken and justice served. The second most common theme relates to actually being engaged by law enforcement and not an automated response (in some cases that hasn't even occurred). The final most common complaint that underpins the very low satisfaction score pertains to law enforcement at the front counter referring community members to ACORN / Report Cyber when there has been no indication of cybercrime occurring or their response across the system demands a police report which ACORN / Report Cyber does not provide. The recently redeveloped Report Cyber makes such cases even more problematic because of the rules and decision-tree associated with actually completing reports – making some of these referrals back to Report Cyber an impossible task for community members to actually complete the form and report in any of the two environments.

7.1.1.4 There are a number of fundamental and at times competing issues with a capability like Report Cyber. First, the act of reporting a cybercrime online for many people is not a pleasant one. By virtue of what it is, most reporters of crimes experienced these online, and if personal information was compromised in some way as a result of this crime, then it is common for individuals to be asked during the response to provide the same details using the same channel – in effect re-living their experiences at a time when they are highly anxious and vulnerable. Those without intimate knowledge of its working could say that the option presents for members of the community to report offline at a police station. In our daily experience, this is a rare outcome and almost all attempts to do this results in the community member being directed back to Report Cyber / ACORN.

7.1.1.5 Connecting IDCARE's specialist telephone service as another channel to Report Cyber would help to address this concern, and potentially generate much more meaningful insights than the current and historical form, whilst exploring and working with impacted people on their broader needs. ScamWatch and Report Cyber already do this informally, but both do not contribute to IDCARE's resourcing for such services (contributing to the $1.4 m shortfall the Commonwealth presently creates for IDCARE in addressing the needs of Commonwealth referrals).

7.1.1.6 The second fundamental issue with Report Cyber / ACORN and related Government reporting mechanisms is an expectation that will not be met in more than nine times out of ten reports – that is Government pursuing those responsible. The reporting itself has become the outcome, rather than the result from the reporting. This has had very real consequences for the community and law enforcement. Through our own response system testing and client experience scores, and from programs such as SBS Insight, we are starting to capture a growing discontent and distrust in Government response. The flow-on effects of this are also becoming apparent in other quarters. Many formal and informal discussions with frontline policing around the country highlight that their confidence in investigating scams, cybercrime and identity theft needs building. Many don't feel skilled enough to investigate such matters or empowered enough to pursue criminals that commit such crimes across our community every day. There are a few notable exceptions. The New South Wales Police Cyber Crime Group is one such exception. They have an attitude that investigators of cybercrime need, and that is one born from a discontent of accepting the status quo and a continual pursuit of knowledge across a vastly changing discipline. IDCARE has not seen this in other parts of law enforcement, and we certainly have not seen this translate across many local areas and Police Stations. The following case study highlights an example this year where IDCARE anticipated that a community member's response and experience with law enforcement and Government more generally would likely be harmful.

Case Study - Reporting and Supporting Community Experience

In January this year John received two debit cards in the mail he didn't apply for. He immediately spoke with the banks concerned – banks he had never previously had any interactions with. One bank said they couldn't share details about the case because of privacy concerns. The other said that someone had used his Queensland Driver Licence and Medicare Card details to apply for the debit card and that the account appeared to have been used for money laundering (in his name) by criminals based offshore. He was advised to call IDCARE by the Department of Human Services having arranged for additional security measures on his Medicare account, including a new Medicare Card.

IDCARE worked with John to understand where else his identity may be being misused and how his driver licence and Medicare card information may have been compromised in the first case. John, like anyone else in this situation, was very anxious, guessing as to how this had happened, and what it meant for him and his family.

He reported the matter to his local police who referred him to the Australian Cybercrime Online Reporting Network. Knowing his licence was being misused, and residing in one of two States that allow for driver licence number changes, John requested from the Bank a letter to indicate that his licence had been misused to open an account. This is a rule imposed by the driver licence issuer on victims of identity theft in order to change a driver licence number. The Bank initially refused. IDCARE then advocated on behalf of John to convince the bank to write an email describing that his licence was presented to apply for an account and that this account was believed to be fraudulent. As part of their advocacy IDCARE advised the bank that by assisting John, they are actually reducing the risk across industry and government service providers that the criminals will continue to misuse his old licence.

His next step was to go to the local police station to request a police report number and a letter from the police indicating the same – that his licence was suspected of being misused to create a fraudulent account. The police initially refused, instead referring him back to ACORN. An IDCARE Case Manager then accompanied John to the same police station. The same advice was provided and when the police were informed that a letter was required from the police to the Queensland Department of Transport & Main Roads to request a licence number change, they again refused to cooperate. At the police station, on behalf of John, IDCARE called the Manager within the Queensland Department of Transport & Main Roads and ask that he speak with the local police to explain the process. The Sergeant at the Police Station agreed to receive the call and having been explained the process found within the police system a form that police complete and provide to people in John's position to request a licence change. John then took the banking email and signed Police form to the Queensland Department of Transport & Main Roads.

Six weeks later John got a new licence with a new number. His identity theft journey took around 35 non-consecutive hours, taking time off work, completing around ten different forms, making contact with Commonwealth, State, banking industry, telecommunications industry, credit reporting bureaus and IDCARE representatives, had reached a place where the offending and misuse of his identity stopped. But John, just like hundreds of thousands of Australians every year, will never reach a point where they know they are completely free from the risk that their identity one day will again be misused. His story is not the exception. His story is the rule on the journey members of our community take in responding to what is described as the fastest growing crime on earth. John was lucky to have found IDCARE. He still does not know to this day how criminals got his details. The criminals remain at large, and likely continue to offend. His journey across reporting and supporting mechanisms highlights how the current way of doing things needs a complete re-think. Without one, community discontent with Government in its response to cybercrime will grow with or without a strategy.

7.1.1.7 In recognising this issue, IDCARE has spent considerable time mapping the community’s journey across the Australian cyber security response system. If you use the precondition that personal and/or credential information has been compromised by a threat actor, such as via email phishing or a telephone remote access scam, the community member will spend on average 28.7 non-consecutive hours responding across a system that requires 67 response tasks to be performed, 45 of which are completely dependent on the community member to perform (Wyre, Lacey & Allen, forthcoming). The ironic part of this journey is that the community member in performing all of these tasks is actually doing so mostly to protect Government and business from enduring risks that they face and not so much the actual risks to the individual. Most community members are oblivious to these requirements of them and experience significant physiological and psychological distress during the actual response phase itself.

7.1.1.8 The renewed cyber security strategy needs to acknowledge the needs of individuals in their response and the requirement to improve the diversity of reporting channels, the resourcing of supporting efforts, and the maximisation of more networked approaches across organisational boundaries. IDCARE encourages Government under the new Strategy to develop a national plan to address the needs and response requirements of community members impacted by cyber security threats (including scams and identity theft). Our organisation would welcome the opportunity to contribute to this important initiative in addressing a key gap in our nation’s approach.

7.1.2 Prevention & Awareness Mechanisms

7.1.2.1 ScamWatch provides excellent prevention and awareness messaging for consumers. But the ACCC is not funded to continue this operation. The ACSC is quickly developing a highly useful alerting service on cyber security threats and fixes that is mostly targeted to business and government, albeit the consumer is included within its own nomenclature. The Stay Smart Online campaign, formerly managed via the Commonwealth Attorney-General’s Department, and now the ACSC, to date has largely focused on consumers with annual awareness weeks and awareness Guide development contributing to key national prevention collateral.

7.1.2.2 Prevention and awareness, despite the critical shortfall in deterrence and intervention, should not be lost as a key Government activity in the renewed Strategy. This Strategy provides an opportunity for Government to reconsider the roles and priorities of relevant Government stakeholders. Presently the divide in responsibilities between Commonwealth stakeholders, such as ScamWatch (the ACCC), ACSC, moneysmart.gov.au (ASIC), ThinkUKnow (AFP), and the eSafety Commissioner is artificial at best and mostly confusing for the community. And this is just one level of Government. States and Territories are rapidly developing their own capabilities. Whilst one could argue that there can never be enough prevention and awareness about cyber security issues and threats, the professionalisation of this discipline in some quarters has revealed to IDCARE intricate insights on the effectiveness of campaigns, their preventative value, and life-span of messaging uptake. Since the last Cyber Security Strategy

IDCARE has witnessed a dramatic growth in specialist prevention and awareness roles across many large corporates. The same cannot be said of Government agencies. Instead in the Government landscape we have seen a continued proliferation of agencies competing for scarce prevention and awareness media space and community cognition (ie. ability to absorb the messaging).

7.1.2.3 We ask our clients that have been exposed to scams, cybercrimes and identity theft where they have had direct communication from criminals in order to deceive and elicit a response what made them believe the deception and what made them disbelieve the deception (the reason for seeking assistance from IDCARE). These are critical questions, the insights of which could benefit from a much greater professionalisation of the prevention and awareness cadre.

7.1.2.4 Whilst we have heard repeated calls for the "slip, slop, slap" campaign for cyber security, IDCARE doesn't believe that with our knowledge of belief and disbelief in this content such a campaign would provide a holistic result if it were targeted at preventing cybercrime. We are constantly asked what's the one piece of advice we would give to build a person's resilience – our answer is often "it depends". Every scam and cybercrime threat type has its own nuance. We once advocated for people to ensure websites had padlocks and the domain name was identical to the domain of the real organisation. Both now both are very easily circumvented by criminals. This adds a further complexity to the prevention and awareness space, and supports the notion that this function needs a dedicated and well-researched effort that can translate into much more timely and focused messaging by a few, rather than all in an attempt to gain attention and add legitimacy to an agency or campaign.

7.1.2.5 We propose that Government invest much more into this professionalisation through supporting empirical research, connecting our services to those interested in monitoring the effectiveness of campaign messaging, advancing the good work of the ACCC and ACSC, but be much clearer on roles and responsibilities to avoid distortion of key messages. We would strongly support further rationalisation across Commonwealth agency responsibilities, for example, prevention and awareness efforts targeting individuals become the sole occupancy of ScamWatch; whereas business (of all sizes) and Government be the sole domain of the ACSC. Both require resources and demand the ongoing support of specialist prevention and awareness expertise. The current divisions of responsibilities are confusing, likely to be inefficient, and in some cases harmful to the community by adding critical and unneeded time to a response journey when time is of the essence.

7.1.3 Supporting Mechanisms

7.1.3.1 Each organisation in the response system has the potential to play a support role. Almost all of the roles performed are defined by the product, service or legislative boundary of the specific organisation. This is what is different about IDCARE. Our organisation engages a community member as a whole consumer. They are consumers of Government services at all levels (local, State/Territory and Commonwealth). They are consumers of financial institutions and telecommunications providers, sometimes more than one. They are residents of every community in the country, as well as Australians travelling abroad. When their device or account is compromised, the impacts and ripple effects permeate across organisational boundaries, levels of government and relationships. We take this approach of all our clients, irrespective of whether they are customers of one organisation or another. This holistic approach is one of the main reasons why IDCARE maintains a very high customer satisfaction score.

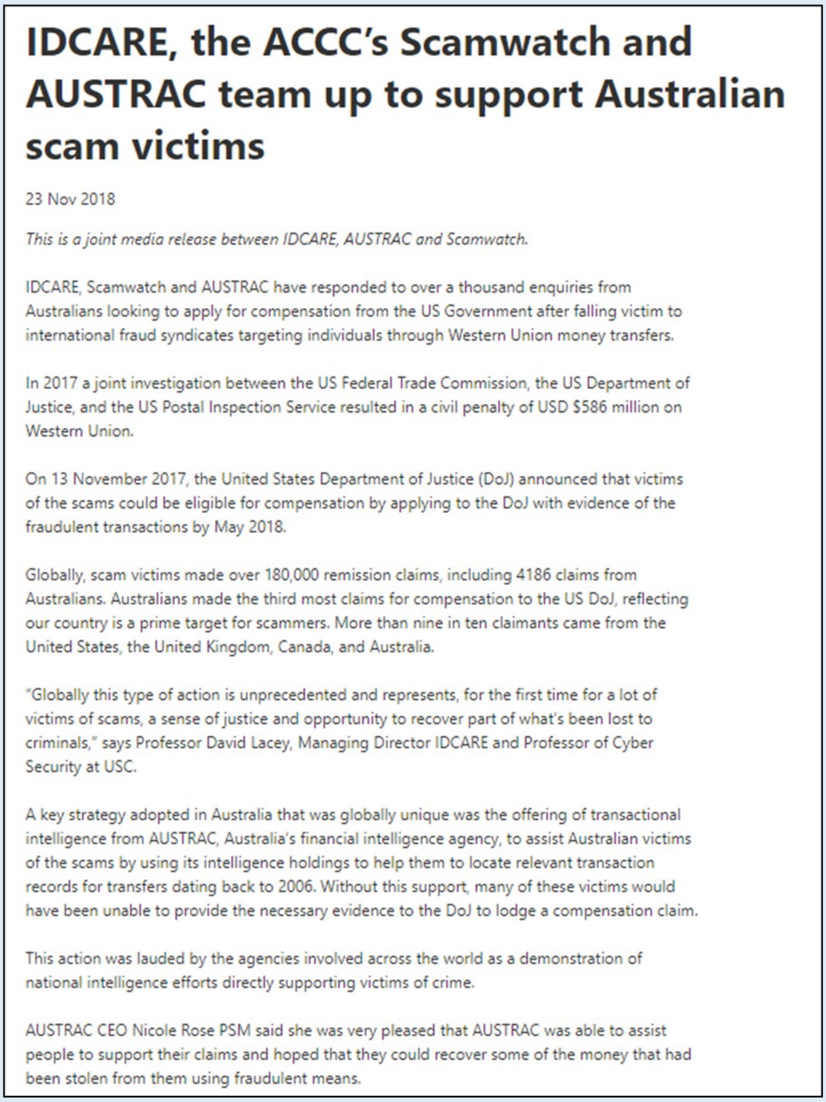
7.1.3.2 We are the only provider that has specialist Identity & Cyber Security Counsellors. During our feasibility study we found the greatest community need was to have counsellors, psychologists and social workers work with clients to understand their needs, build together response plans, and act as their "case manager" through their response (irrespective of the doors they knock on). We trained these behaviouralists in identity and cyber security, including the latest scams, technologies, and deceptive behaviours. They developed a very broad and deep understanding of Australia's response system. It's not a service that offers advice around lock your letterbox and change your password. It's a service that has a significant library of "response plans" that can tell a community member precisely what telecommunications carrier A requires a customer to do if they have had their Northern Territory driver licence and email account compromised. This Response Plan Library is updated every quarter to ensure IDCARE's pragmatic advice remains current and gives our community the most efficient (and least harmful) pathway to address their immediate concerns and any enduring risks.

7.1.3.3 But our service is at a critical juncture. We could quite easily double the caseload and extend further our operating hours. We could connect more directly to Government and business to enhance their insights on how our community (and their customers) are being impacted and how parts of our economy are performing in preventing or even enabling such crimes to continue in more real-time. We simply cannot sustain a model where large organisations shift their customers to IDCARE without contributing to the costs of delivering these specialist services. We need to call them out, which will embarrass a few, but we feel the community needs to know. We have already commenced this process by informing clients whether the organisation that refers them contributes to our costs. No doubt some will lose customers on this realisation, but we do not feel as an organisation that it is equitable that some demonstrate ethical leadership and others don't seem to realise or care that they are financially damaging our service and its ability to reach everyone that knocks on our door. In an ideal world "the system" should pay. But this is far from an ideal world. It is too easy for large Departments to say "well we didn't issue this identity document so that customers would use it to apply for a loan, so why should we feel responsible". The problem is, with this attitude, no one actually takes ownership. As a result we arrive at this situation.

7.1.3.4 We propose a model where Government explores mechanisms whereby it attains proceeds of crime, fines, or identification system "levies", to support organisations like our own. There are national mechanisms Government have initiated, such as the Document Verification Service and even AUSTRAC's funding model, along with Proceeds of Crime, where there are some opportunities to explore how "the system" (or a subset thereof) could contribute to services like

IDCARE. We understand that the Document Verification System generates revenue that can only be expended on efforts that align with its intended service. We would support Government(s) exploring the extension of such a service to include IDCARE if it were to mean that our critical support efforts continue to fill a key response gap in an equitably resourced manner. We would also encourage Government exploring models of fine and proceeds distribution beyond "crime prevention". In a recent example, the United States Federal Trade Commission and the United States Department of Justice settled a civil penalty with Western Union in excess of $250 million. The following case study highlighted our role in the matter and the opportunities that could be explored in looking for "system funding" solutions via AUSTRAC, ACCC, or ASIC regulatory penalty outcomes and their distribution to services such as IDCARE to ensure we can attend to the needs of the Australian community.

Case Study: United States Department of Justice & Federal Trade Commission Fine Settlement



IDCARE, the ACCC's Scamwatch and AUSTRAC team up to support Australian scam victims

23 Nov 2018

This is a joint media release between IDCARE, AUSTRAC and Scamwatch.

IDCARE, Scamwatch and AUSTRAC have responded to over a thousand enquiries from Australians looking to apply for compensation from the US Government after falling victim to international fraud syndicates targeting individuals through Western Union money transfers.

In 2017 a joint investigation between the US Federal Trade Commission, the US Department of Justice, and the US Postal Inspection Service resulted in a civil penalty of USD $586 million on Western Union.

On 13 November 2017, the United States Department of Justice (DoJ) announced that victims of the scams could be eligible for compensation by applying to the DoJ with evidence of the fraudulent transactions by May 2018.

Globally, scam victims made over 180,000 remission claims, including 4186 claims from Australians. Australians made the third most claims for compensation to the US DoJ, reflecting our country is a prime target for scammers. More than nine in ten claimants came from the United States, the United Kingdom, Canada, and Australia.

"Globally this type of action is unprecedented and represents, for the first time for a lot of victims of scams, a sense of justice and opportunity to recover part of what's been lost to criminals," says Professor David Lacey, Managing Director IDCARE and Professor of Cyber Security at USC.

A key strategy adopted in Australia that was globally unique was the offering of transactional intelligence from AUSTRAC, Australia's financial intelligence agency, to assist Australian victims of the scams by using its intelligence holdings to help them to locate relevant transaction records for transfers dating back to 2006. Without this support, many of these victims would have been unable to provide the necessary evidence to the DoJ to lodge a compensation claim.

This action was lauded by the agencies involved across the world as a demonstration of national intelligence efforts directly supporting victims of crime.

AUSTRAC CEO Nicole Rose PSM said she was very pleased that AUSTRAC was able to assist people to support their claims and hoped that they could recover some of the money that had been stolen from them using fraudulent means.

7.1.3.5 In the case study presented IDCARE worked with the US Federal Trade Commission to determine initially whether Australians would be eligible to claim a remission. When this was determined IDCARE rallied ScamWatch and AUSTRAC to join forces to look for two key inputs: (1) raise public awareness via the media of the opportunity to Australian scam victims; and (2) encourage AUSTRAC to "open its doors" and allow members of the community to extract from its intelligence holdings evidence of their funds being sent offshore via Western Union to the scammers to enable them to submit a claim. To their credit and leadership, both Commonwealth agencies agreed. It highlighted how Government and organisations like our own can work together in creative ways to support victims of cybercrimes, identity crimes and scams. Much more work and innovation between our organisations can be done. We hope the new Strategy recognises this potential and encourages Government to find ways to ensure resources and support for growing resources reflect this.

8. Concluding Remarks

8.1 A national strategy on cyber security is a positive contribution from Government. The approach taken to circulate a discussion paper and focus our thoughts and ideas against questions that we feel most relevant to our work is welcomed. We hope you find our ideas and thoughts of benefit to your own policy development. Whilst elements of our submission are critical of some, we hope that our honesty and directness in drawing your attention to what can be improved and what is working well will inspire further thinking on how the next Strategy can enhance Australia's position in a cyber security context. We acknowledge that this is a complex domain and that there are many more who share goodwill and a desire to be better than those who may be more interested in preserving their own budget or self-interests. The latter cuts against the grain of achieving a networked Strategy outcome to a networked environment. IDCARE stands ready to join others to advance our country's interests and overall resilience to cyber security threats and the benefits to our economy that flow from such wonderful human inventions.