IDCARE

Submission to the

Scams Mandatory Industry Codes

2024

Executive Summary

The proposed Scams Code Framework is a necessary development to improve how Australia responds to the ever-increasing numbers of scams and related crimes of deception impacting our community. There is little to no deterrence of international scam groups, so without foreign State intervention, alternative mechanisms and strategies are needed to both dissuade these groups and enhance the resilience of our community to their deceptive attempts. We all have a role in this. Whilst the Scam Code Framework identifies three specific industries, the operating model of these criminal groups and their criminal supply chains calls for new and innovative response approaches that are all-sector encompassing, including from government organisations.

The Australian Competition & Consumer Commission's own targeting scam reports identified in 2020 that the volume of scam impacts on our community over the preceding decade was unsurpassed in prior periods. It was colloquially known as the scam decade. However, since that report, reported scams impacting Australians has increased by more than 300% per annum according to subsequent ACCC public reporting. On any measure, we are failing and failing badly to address these very tangible impacts on our community where hundreds of millions, even billions of dollars, of hard-earned savings are being diverted from our economy into the accounts of organised crime. No other crime has such a penetrating impact on our community than crimes of deception. Most of us are reminded about them each day via phone messages and phishing emails. The current policy attention on the subject is welcome. The development of minimum standards to prevent, detect, and respond is essential. Too often we walk in the shoes of scam victims to find that the bigger evil is not the scammer, but how our country responds. Whilst we may be constrained to directly shape the thinking of these very sophisticated criminals, we can absolutely shape and influence how this country gives itself the best chance to prevent, detect and respond. That remains our organisation's focus – to directly support the victim, whilst shaping the performance of industries and sectors in their response.

Around one in two community members to engage IDCARE services are victims of crimes of deception. The very definition of this is of little to no importance for these Australians, but one that pre-occupies a lot of discussion across government and industry in looking at ways to better understand impacts and integrate capabilities to improve response. Regrettably, at present, demarcation of responsibilities across Government only adds to the confusion for many Australians and diminishes the effectiveness of our response. You just have to ask yourself what government portfolio has responsibility for a crime that results from the stealing of personal information, online, in order to deceive others into believing a scam. This simple, but very common scenario, cuts across at least four portfolios all vying to have a policy and budgetary stake, often at different policy tables. The current risk IDCARE sees of the policy landscape is that we will move from taking a very complex issue and response and find ourselves in an even more complex environment that only adds dysfunction and harm to our community. It is akin to the great Aussie house extension with no real long-term plan, no real courage to make decisions to reduce duplication, or improve coordination of disparate parts, where we find the toilet is now in the kitchen and wondered how we got there. This obviously goes beyond consideration of a Code, but does go in part to governance structures and responsibilities. It's something that needs some urgent attention as it contributes significantly to the response complexities experienced by many thousands of Australians and broader population expectations.

Notwithstanding the architectural policy and responsibility challenges, we believe a Code is necessary, but one that needs to offer a little more precision and fidelity in some areas, and genuinely places the community member at the centre of our response. We shouldn't shy away from this and ignore the clear stake and advantage victims offer in better understanding, protecting and responding. We haven't found this in the current draft Code and our work reaffirms that this approach offers enormous potential for our country, for regulated entities, and most importantly, for individual victims.

Not all areas of the Code we feel equipped to contribute thoughts and perspectives towards, so in this submission we have only focused on the key areas where our engagement with communities and lessons from offering a unique service to such people has the most relevance.

We sincerely welcome the opportunity to provide comment. There is a lot to be done and we do believe the Commonwealth, in particular, is at an important policy cross-road on how it can better organise itself across crimes of deception, including cyber, to make practical and real positive change in this context. Our submission focuses on the following areas:

- Our work and understanding;
- Prevention, awareness and response support for individuals impacted by scams; and
- Additional considerations for enhancing the Industry Code's objective to disrupt scam activity.

Our work and understanding

IDCARE was established in 2013 as a joint industry-government specialist response service dedicated to providing practical, behavioural, and technical support for victims of deception. During that time the Commonwealth, States and Territories, agreed upon a National Identity Security Strategy, which acknowledged the need for improved victim support. IDCARE was recognised by the then Commonwealth Minister for Justice as Australia's national response to this need in launching our service. It was to operate as a joint government and industry not-for-profit and during the first five years of operations struggled enormously with its resourcing and sustainability. IDCARE has no annual appropriation from Government and like many ombudsman schemes, does not generate levies from referred organisations to sustain operations. Put simply, IDCARE despite the criticality of its work and being the preferred go to service for many governments and industry members, has no guaranteed on-going funding. Most of our revenue is achieved through providing services procured by some governments and select industry partners. At best it is sporadic and is far from ideal, particularly given demand for our specialist services increases on average 20%-30% per annum. We've come perilously close at times over the last few years of having to deny our services to many tens of thousands of victims as the funding and our charitable capacity exhausts itself. We've been asked on more than one occasion what we would say to people referred to us from Government when government ceases to fund the services that it requires of IDCARE. We've responded under significant time constraints to build infrastructure for specialist services only for them to not be resourced or occupied because of funding limitations. We've had to respond to State governments looking to duplicate our service only for community members from these States doubling in demand for IDCARE services since their commencement. These decisions test our resolve and at times faith in some of the decisions being made and whether they are being made in the interests of Australians or more for political expediency and bureaucratic portfolio pushing. In amongst all of this, we have a crime that remains undeterred, reaching unprecedented levels, and causing enormous pain to many thousands of Australians and their families each year. It is a fair conclusion that our operating and funding model as a joint industry-government national capability needs to be reconsidered. There is enormous value in our work and unrivalled expertise in this context in working directly with Australians each day that confront some of the worst experiences of their life. But there are alternatives to our current model, such as government-business enterprise structures and ombudsman models, that could preserve the public confidence we have and independence of operations, but also support enhanced visibility and accountabilities. But none of that is possible without greater funding assurance and recognition that IDCARE continues to provide unparalleled excellence in client care and support when it comes to crimes of deception.

In the early years, there appeared to be no real appetite from Government to actually invest in IDCARE, despite the growth in these crimes, the launching of the service, and the absence of any alternative for the community. Achieving a base level of funding support was gradually achieved as privacy, cybercrime, and scams all emerged

as real and visible impacts for our community. Australians are increasingly recognising and requiring more of government and industry to address this problem – a problem that they are reminded about on almost a daily basis via emails, phone calls and SMS texting from organised crime. The need for specialist care and response services for the community could no longer be ignored. The demand for IDCARE services, in large part through the connection of individuals from large corporates and government agencies, grew exponentially to now receive in excess of 300,000 contacts per annum equating to around 100,000 victims engaging each year.

Our services for the community are not charged. A free community service remains an important design feature and one that ensures our work is accessible to all Australians, irrespective of their personal wealth and circumstances. Having responded to more than half a million Australians to have experienced crimes of deception, we have remained committed to innovating and leading the way in specialist response support. For example, in the last two years, with the support of Westpac, IDCARE has engaged over two hundred communities across Australia, mostly in regional and remote areas of all States and territories, to hear directly from community members about their own experiences, needs and challenges. Our team have delivered response and resilience clinics in the most remote locations, and sadly, crimes of deception are just as prevalent there as they are in our cities. We've worked with leaders in cyberpsychology and deception research to refine our practice, and now have dedicated cyberpsychology clinics that provide community members most harmed clinical and technical interventions to enhance their recovery and resilience. This is a world-first that we have pioneered and are proud to say has come out of Australia in partnership with Australian researchers. Our size and agility have provided an enormous advantage to innovate. It has been one of the key factors to our success and ongoing client satisfaction with our work. Our future operating model needs to embrace this as we continue to meet the challenges of today and prepare for tomorrow.

Importantly, the core of our work is to provide community members with a central and expert place to go that is independent and confidential to encourage sharing of concerns and issues in order to best assess risks and developed personalised response plans. We do this by constantly testing how government agencies and the private sector respond to risks presented to the individual from crimes of deception, including cybercrimes, data breaches, scams and identity credential compromise. This is necessary because of both rapid change and the essential requirement to be able to provide Australians with the most accurate and contemporary way forward to addressing their risks and concerns. The last thing we need to do is provide the wrong advice and put in place measures that will have little to no effect in reducing their harm. IDCARE's library of response actions is significant and continues to change. Our experts know that if any combination of attributes are shared with scammers, or where they have engaged victims via particular channels, or have required scam victims to perform certain actions, what the real risks are to that person and what Australia's response system actually affords at any one point in time. It doesn't matter whether it is a Tasmanian licence, a Queensland birth certificate, a MyGov ID, or a Macquarie Group account number. Nor does it matter whether it was a breach of data from a ransomware attack, a response to a relationship scammer, or clicking on a link via an Australia Post impersonation text message using an iPhone. IDCARE traverses all levels of Government, all industries and all crimes of deception and we pride ourselves as being the true one-stop-shop for all Australians. Both sides of politics have acknowledged the critical work of IDCARE for the Australian community.[1]

We know intimately what organisations are performing well and what organisations are contributing to the harm for Australian victims. We learnt early on not to trust what others would say their organisation would do

[1] Australian Parliament House *Hansard 25 October 2021* (House of Representatives, Commonwealth of Australia 2021) 12:41 minute mark.

given a particular scenario, and that we had to continuously test things for ourselves and learn from the community members own experiences. Government is just as much of a help and hindrance as the private sector for victims. We've seen Government agencies refer victims to 30-day freedom of information processes when trying to understand what information a criminal has used about them to commit a crime in their name in order for them to take their own immediate protective measures. We've seen some cryptocurrency exchanges tell scam victims that they will only investigate if the police tell them to investigate, knowing full well that the volume of complaints to police far exceed their own capacity to respond. During large data breaches we've seen the temptation from both sectors to try and influence the independence of our advice and its advice. That's not surprising given the often conflicting positions such organisations find themselves in looking at reducing or curbing community concern and demand for their own services despite the real risks to the individual. We saw during the first year of COVID Australia's response system collapse where requests for support from victims were not being answered in some parts of the response system or some were being told not to expect a response for a couple of months.

What's apparent to our work is the critical need in providing information feedback loops to government and industry based on the community's experiences and risks of actual harm. As a result of our unique approach to individuals experiencing crimes of deception and related compromise of personal information, we occupy a niche which has enabled leading-edge research resulting in improved outcomes for individuals. For example, IDCARE identified the need for buy-now-pay-later (BNPL) providers to put in place prevention controls for community members who had experienced personal information compromises after identifying a 551% overall increase in BNPL account establishments in the 5 years prior to 2022. This assisted to inform Government of the need to consider how to shape the behaviour of that industry in building its resilience to criminal exploitation in the name of Australian scam victims. Our insights have previously shaped privacy credit codes for victims of credit related misuse in experiencing more streamlined ways of protecting their credit files. We take this role very seriously through acting as a mouthpiece for the voiceless victims and to share anonymised experiences and trends to affect positive change. To that end, we look at the draft Code from the perspective of the victim and from our intimate knowledge of the response system and its performance. We hope our submission is informative for Government and we remain open to discussing further our experiences over the last decade and thoughts to achieve the best outcomes for all Australians.

Prevention, awareness and response support for individuals impacted by scams

The draft Code takes a very practical approach to prevention which is welcomed. Our ongoing research work with academia on the cyberpsychology of deception has gone a long way to understand why crimes of deception occur, what makes people vulnerable and how effective prevention measures are at stopping these attempted crimes in their tracks. They go much deeper than to rely on the temptation for 'pop-psychology' reporting from consultants based on phone surveys that are typically unreliable and lack academic rigor. Our research overwhelmingly supports the view that prevention messaging if not achieving sufficient absorption within a person's subconscious is largely a waste of time and money. Previously IDCARE has reported on the merits of "just-in-time" interventions that seek to break a person from their scam compliant state that leverages information about high risk behaviours and transactions. It acknowledges the nuance between warning customers that they may be engaged in a scam and the potential liability that organisations may confront if they deny such access or transactions to individuals. This is an area that needs more consideration, particularly if an outcome of the Code's operation is the enhanced sharing of scam intelligence, and with it, personal attributes.

For example, if financial institution A shares information about a scam account with telecommunications carrier B, and that information contains personally identifiable information about a scam victim or their account that results in them being denied access to a product or service or change of account because of such sharing, the resultant action may present considerable legal and liability questions for the parties concerned. It will also

result in further harm to the victim. IDCARE is aware of a number of related examples where community members have been denied access to products and services across government and industry because their personal information, such as identity credentials, have been flagged as being associated with a cybercrime, identity theft or other crime of deception without their knowledge. It is a wicked problem, because at times an organisation may not be sure whether such information attributes relate to a victim or a perpetrator. They may in fact not be confident they have even the right contact information to validate which one it is.

We see obligations for External Dispute Resolution services also requiring further consideration from a victim's perspective. We don't believe that this obligation will work for victims in a way perhaps the Code foresees. A better model is to have this centralised and provide community members with one point that cuts across sectors and industries, rather than leave it for individual schemes relative to their specific terms of reference. A SIM-swap, as an example, may well present an opportunity for escalation to the TIO, but in most of these events we also see hacked bank accounts, social media accounts and email accounts. Are we expecting consumers to escalate to three or four External Dispute Resolution services? This is part of the challenge for victims in terms of the dysfunctional pathways of the response system and the Code requires some more thinking from the perspective of the victim in relation to this.

Reporting, notification and exchanging information of scams

An alternative proposition would be to have a community member who engages IDCARE following a scam event consent to their information being shared with financial institutions and other key targets of organised crime and where such sharing requires minimum detection and prevention actions to be taken by the recipient organisation. The problem in not doing so was highlighted in one community member's case where they provided consent for their information to be shared by IDCARE to an organisation only for a criminal to subsequently access their account and for them to lose around $30,000 in account value when the criminal targeted the organisation that had received the information but did nothing to act on it. In another more recent example, we've had victims of data breaches have flags instigated on their personal information without their knowledge and then for future legitimate transactions to be denied because of the flag, denying the person access to finance.

Designing prevention systems based on personal information exchange is fraught where the victim is not aware of such an exchange or does not consent to it. It's equally fraught where there are no enforceable minimum standards of response on receipt of such information and this is unknown to the individual concerned. The Code shouldn't shy away from the potential good this prevention measure has, but it does need much more fidelity in terms of (1) what the minimum actions are to be taken on receipt of such information by exchanging organisations (such as a retrospective sweep of applications in the person's name since the estimated time of exposure and the flagging of future applications or account changes as potentially high risk events requiring extra validation), and (2) most critically, feedback to that individual of the results to validate or otherwise what has been found or delayed because of a high risk assessment.

The latter design feature has the potential to be a game changer for Australia. When one looks at the Code and our broader response to crimes of deception, we have typically boxed the role of a victim to be a reporter only. We ask community members to fill out several forms from government where the outcome of doing so is government knowing something as opposed to the individual victim being protected and the system becoming more resilient. We're too small a country to have more than one reporting mechanism and more than one central supporting capability for victims. The 'no wrong doors approach' at a superficial level is a terrific idea. In the last 12 months both Scamwatch and ReportCyber have embedded options for victims to be contacted by specialist IDCARE case managers even where their awareness of IDCARE to start with was low. But a 'no wrong

door approach' fails where the victim either doesn't get to the right door in a timely way or goes to a door that is meaningless and just another data collection experience that benefits others.

What's behind that door needs to integrate specialist care and support with meaningful individual and system protection and response actions. There is no need to duplicate or create even more of this in a country of only 27 million people. The opposite needs to happen. We need to streamline, rationalise and think critically about what real difference is being made when asking community members to fill out forms. Put simply, how will filling out a government form help a victim who has just lost their life savings? We need to challenge ourselves as to whether we truly have their interests in mind, because if we do, then the potential is enormous in not just remediating their concerns and needs, but in providing real protection to our economy, detection of previously unseen crimes, and prevention of future ones by an unrelenting threat. As a country we want to be in a position where someone's misfortune results in better protection for them, but also for others. The technologies are there and our sense at IDCARE is that there is enormous goodwill for change across industry and government.

IDCARE has experienced great success with obtaining the consent of victims and sharing details with financial institutions that has resulted in millions of dollars in prevention outcomes. But the missing piece is the feedback loop to the victim. It's so obvious and yet so rare coming from both industry and government. The apprehension may come because an individual organisation may not want to have these conversations with people. At times we see this and act as that independent conduit. We have seen this help both the victim and the relevant institution, but this needs investment and for such processes to become much more automated and industrialised. We'd like to see this embraced by the Code and better articulated.

Practically this means that the Code needs to address the response standards for receiving information, the need for victims to know and consent, and most critically, the need for information identified by receiving organisations to be shared back with victims. For every scam victim to come to IDCARE, there is on average around two other crimes committed in their name. These become visible to victims only after they have done the heavy lift in understanding where else scammers have exploited their details. Point-in-time government reporting measures don't typically see this. Australians are spending days, weeks and in some cases months and years, responding to these crimes. Much of this work is repetitive, often re-traumatising victims, extremely bureaucratic and incredibly frustrating. We think the Code has potential here, but at present misses the mark without much greater details.

Additional considerations

Government holds significant information that, if shared with consumers and industry, would make a very tangible difference to the impact of scams on the Australian population. This has great potential and has previously been trialled by agencies, such as AUSTRAC and the ACCC with IDCARE in various ways, such as assisting victims of scams provide evidence to the United States Government of the use of Western Union services in order to claim a remission resulting from a deferred prosecution agreement. It was a terrific example of Government using its unique information holdings to assist scam victims through engaging with IDCARE to support community claimants (victims of scams). Work like these initiatives give opportunities not just to assist victims, but also proactively detect community members currently being compliant to the demands of scammers where money is being transferred to known scammer accounts offshore. At present this is not shared with regulated entities and many Australians remain oblivious to their scam victimisation. Government can make a real difference here beyond promulgating what it requires of regulated private sector entities.

In terms of broader governance in the context of improved information sharing and participation from government, there is some sense that this will be difficult to achieve where the government entity concerned is also the regulator. This may go some way to explaining the absence of a more participatory approach from the likes of some agencies, such as AUSTRAC, to sharing direct information with regulated entities and in assisting

victims in a more enduring way. The same challenge may present for the National Anti-Scam Centre where on the one hand it supports information sharing, and on the other as a body within the ACCC, is part of the regulatory apparatus. This positioning, including the future positioning of a national victim response capability, requires further consideration and the scam code along with other discussions across portfolios presents an opportune time to have these. We encourage Ministers and Secretaries to engage IDCARE in these discussions and have found in recent contexts, such as the national strategy for identity resilience, to be lacking in broader consultation of a such a critical issue for our country and community.

Consultation is key, because the scam code is silent on what the likely impacts will be for capabilities such as IDCARE's. With the onus on enhancing regulated entity response efforts for scam victims, it is an obvious outcome that this will mean considerable increases in demand for our service. From 2021 to 2023, and in the absence of a scam code, demand for IDCARE services from the Australian community grew more than 100% (i.e. it more than doubled). The portion of funding from Government for the delivery of victim support services to the Commonwealth concludes early next year. The same is planned for referrals from law enforcement, both leaving an estimated service delivery gap based on current usage demands of around $7 million per annum. We are transparent with this in our engagement with government, but we feel that with the introduction of a scam code, the gap will grow further between what is required of IDCARE and the resourcing available to meet this requirement. It is necessary to continue to engage with Government and our stakeholders across industry to fully understand what this will mean over the immediate term.

Concluding remarks

The Scam Code is a significant step forward in commencing the journey of redressing the unrelenting impacts of scams on our community. In our submission we have identified areas that we feel require more work to provide better outcomes for the Australian community and victims of these crimes. We welcome the opportunity to contribute further to the discussion given our unique role, and encourage government to engage IDCARE further in conversations about how to advance the work in supporting scam victims and providing more streamlined ways to effect a much more positive journey for victims of these crimes that achieves prevention and response outcomes for the system. We cannot impress enough on the Government the point-in-time opportunity this policy area presents to better coordinate and bring together key privacy, cyber security, identity and scam portfolios to achieve much improved prevention, detection and response outcomes for Australia. None of us should tolerate the status quo and we congratulate the Government for taking steps, such as the Code, that recognises this.