

Submission to The Treasury: *Scams Prevention Framework Exposure Draft*

September 2024

IDCARE acknowledges the traditional custodians of the land on which we operate across Australia and New Zealand.

IDCARE pays respects to the Australian First Nations Elders past, present and future and acknowledges Māori as tangata whenua and Treaty of Waitangi partners in Aotearoa New Zealand.

These community members hold the memories, the traditions, the culture and the hope of their people who we seek to support through our work.

© 2024 IDCARE. Reproduction without express written permission is prohibited. Written requests should be directed to media@idcare.org

Connect with IDCARE at www.idcare.org

Introduction and overview

IDCARE welcomes the draft Treasury Laws Amendment Bill 2024: Scams Prevention Framework (**Scams Prevention Framework**) as a necessary development to better protect the Australian community from harmful scams and related crimes of deception. Every day IDCARE sees the extreme harms caused by scams which may have been prevented or disrupted with better responses and mechanisms by industry and government.

The proposed Scams Prevention Framework provides a strong opportunity to advance Australia's resilience to scams, but this needs to be carefully considered in light of what is likely to offer the best chance of success and a conscious regard for individual rights and protections. In its current draft form, the Framework does not provide adequate control to individuals over their own information or adequate protections, nor does it sufficiently safeguard victims of scams against further harm being caused by the system. Our assessment of the Framework against the backdrop of many tens of thousands of scam cases extended IDCARE specialist services each year, points to opportunities for further refinement before meaningful differences will be made to the overall scam victimisation confronting Australians.

In the four weeks prior to this submission, IDCARE directly supported 8,034 community members confronted with crimes enabled via online deception. These criminals made \$56.5 million in just the last month that is no longer in the accounts of community members and being spent in local communities to support local economies. Some of these crimes resulted from the direct scamming of government agencies and industry staff and systems in the name of Australians. The complexities and nuances to many of these crimes are largely absent in the current exposure draft Bill and explanatory materials. This absence goes a long way to our assessment that without further refinement, there will be little difference made to the volume of offending and the overall community resilience to scams.

IDCARE's key thematic recommendations relate to:

- **Definitional construct needs:** the exposure draft limits the real risks to scam victims and artificially constrains common scam exploitation measures due to its current definition.
- **Specificity on prevention, detection and response measures:** where the most ground will be made is in defining and applying specific standards in prevention, detecting and responding to scam risks. Acknowledging that industry specific detailed regulation will be contained in the sector-specific codes, our strong view is that greater specificity is required in the Framework legislation. Without this, there is little prospect that the costs outlaid by regulated entities will result in a dividend that makes the Australian community more resilient to these crimes. It is poised to become just a process to report to Government without meaningful change.
- **Safeguards to prevent harm to victims of scams are absent:** we recommend actionable scam intelligence should have clear and transparent safeguards and the Principles should include greater detail. Individuals should retain some control over how their information is used, should be notified when protective measures are put in place, and be able to have protective measures removed on request. The current situation is resulting in serious harm to scam victims from actual system responses and not just the scammers themselves.

Summary of Recommendations

Scam definition:

1. **Scam definition breadth:** *Scam* is too narrowly defined and does not reflect the complexity of a person’s experience with fraud and misuse, nor the hardship created. The definition should be broadened to encompass fraudulent misuse that takes place without the actions of the identity owner, nor does it reflect the reality that following the initial scam engagement, scammers typically continue to exploit that individual by targeting institutions directly (such as banks and government agencies). Some institutions targeted include those which the individual has never had a relationship.
 - (a) The definition of **Scam** (cl 58AG) should be expanded to include *or directly or indirectly attempt to engage with a regulated service through impersonating an SPF consumer*.
 - (b) The definition of **SPF consumer** (cl 58AH) should be expanded to include *whether the SPF consumer is being impersonated or not and where the SPF consumer has a pre-existing relationship with the regulated service or not*.

Response standards:

2. **Minimum prevention and response measures:** The Scams Prevention Framework legislation should set out minimum standards which must be inserted into every sector-specific code, to ensure there is clear guidance is regarding what is considered reasonable and the minimum standards that will be expected of regulated entities.

IDCARE recommends that a new provision be inserted in Division 3 – Sector-specific codes for the Scams Prevention Framework, which sets out *minimum prevention and response measures for regulated services*, as follows:

- (1) Prevention measures are extended to all SPF consumers that believe they are at risk of scam exploitation within one business day following customer identification and receipt of request (either directly from the SPF consumer or their advocate).
- (2) The reasonableness of response measures should include:
 - (a) altering the SPF consumer via an agreed channel of engagement any proposed changes to their accounts or applications for new services prior to advancing such changes;
 - (b) altering the SPF consumer via an agreed channel of engagement any prior changes from the determined “at risk” period (for example, a date upon which the SPF consumer believes the scammer obtained information that could enable further criminal exploitation) within one business day of detecting such risks.

Suspicious transactions:

3. **Suspicious transactions in the AML/CTF Act:** Scam-related transactions for entities regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) should be included as suspicious matters under Division 2 of *that Act*, for the avoidance of doubt.

4. **Government response measures:** The Scams Prevention Framework should include obligations on Government to advance and apply minimum response standards in preventing, detecting, investigation and responding to scams.
5. **AUSTRAC monitoring of suspicious transactions:** AUSTRAC should be able to receive suspicious matter reports relating to scam destination accounts and not be constrained in its ability to allow the Commonwealth to proactively identify other Australians who may be scammed and sending money to the same accounts but unaware they are doing so.

Information privacy and control:

6. **Incorporate privacy-by-design in the Scam Prevention Framework:** the Framework should include privacy-by-design principles, ensuring that information privacy is embedded into the Framework's architecture from the outset. For example, the Framework should:
 - explicitly emphasise the protection of personal information
 - align with the APP principles
 - address how data minimisation and proportionality will be maintained
 - require entities involved in scam prevention to inform individuals about how their data is collected, used, and shared, and
 - provide transparency on how personal data may be shared with third parties in the absence of SPF consumer consent, such as law enforcement agencies or industry partners.
7. **Individual control and consent mechanisms:** the Framework should mandate clear mechanisms for notification, consent and control. Individuals should be notified when protective measures are put in place, and they should have the opportunity to remove protective measures, within stated timeframes.
8. **Actionable scam intelligence safeguards:** Actionable scam intelligence should have clear and transparent safeguards to prevent further harms to victims of scams, this includes providing assurance that the scammer attributes shared are not real victim information used by scammers (a common strategy of scammers).
9. **Regulatory data sharing:** Privacy Impact Assessments should be required and Guidelines should ensure that SPF consumers do not have their privacy impugned because of information sharing, including, but not limited to, requiring publication of Privacy Impact Assessments anonymisation and de-identification of reports which contain information relating to scam victims.

Dispute resolution:

10. **Internal dispute resolution:** internal dispute resolution mechanisms should be subject to regular review by the entity's respective regulator to ensure they are fit for purpose.
11. **External dispute resolution:** external dispute resolution systems should be as easily navigable for consumers and reduce the need to report to several different entities.
12. **Government dispute resolution:** mechanisms for dispute resolution services for consumers with grievances about government decisions and actions should be detailed.

About IDCARE

IDCARE provides the Australian community with specialist case management and response services to victims of crimes of deception, including scams, identity theft, cybercrimes and post-data breach notified person support. Our national service was launched a decade ago as a unique joint public-private and not-for-profit. The blending of specialist case management, cyber-psychological and technical support interventions is a world-first.

The vast majority of our specialist support services are directed to victims of online crimes of deception, typically known as scams and cybercrimes. In most cases these individuals experience serious harms, financial and non-financial. Many of these harms are compounded by a response system that traumatises victims, that places organisational protections over individual victim needs, is oriented towards a reporting-outcome rather than a recovery and resilience outcome and does little to provide assurance that victims can move forward in their lives with little risk of further exploitation.

The demand for our services has grown more than 200% in the last four years alone, underlying our value and relevance to the community. But there is a constant tension between supporting more than 2,000 referring organisations of community members to IDCARE, many across Government, and balancing our finite specialist resourcing. For example, our funding support from the Commonwealth to enable IDCARE to respond to ReportCyber referrals of individuals ceases in January 2025. This means the ability for victims to receive specialist support from IDCARE will not be resourced, impacting around 2,715 community members a month, many of whom are victims of scams and other forms of online deception. This highlights the perilous nature of our work in supporting the Australian community and the challenges this presents in maintaining a specialist resource base consisting of cyber-psychologists, technicians, case managers, analysts and support staff. At a time when scams and cybercrimes are occupying positions of policy priority, this predicament is not ideal for the community we serve and the highly specialist staff and volunteers who turn their skills towards caring for victims through their work at IDCARE.

IDCARE scam reports

Current public reporting from the ScamWatch, ReportCyber, and financial institutions reference a decline in financial losses through scams, while IDCARE direct data shows financial losses increasing. This disparity in reporting can be explained by the differences in client cohorts between IDCARE, ScamWatch, and ReportCyber. These differences include elements such as imbalanced representations of age groups, breadth of cybercrime remit, representation of victims experiencing harm, and scale of financial losses. These disparities across cohorts can result in significant discrepancies in data, such as observing financial loss as increasing or decreasing.

For example, ScamWatch reports a \$167M decrease in reported losses between January to July 2023 and January to July 2024. About \$100M (60%) of this was due to a decline in reported financial losses from investment scams. The exact cause of this reduction is unclear, however IDCARE data does not reflect this trend. IDCARE has seen investment scam losses stay the same, if not increase, in the same time periods. In the Jan-Jul 2024 period, IDCARE saw \$150M in losses despite having half the number of investment scam cases as ScamWatch (who reported \$100M in investment scam losses across their cohort). On any

measure, there is much work to be done and by no stretch has Australia addressed the scam threats to our community.

IDCARE has responded to approximately 88,500 cases in the past 12 months (1 October 2023 to 30 September 2024). Targeted industries and sectors over this period by scammers, either through targeting consumers directly or subsequently targeting industries and sectors through scamming their staff and systems with the details of scam victims are presented in Table 1.

Table 1: Targeted Scam Industries and Sectors (1 Oct 23 – 30 Sep 24)

Targeted Scam Industry / Sector	Proportion
Banking Industry	46%
Social Media	18%
Commonwealth Government	15%
Telecommunications Industry	6%
Buy Now Pay Later Industry	1%
Superannuation Industry	1%

Table 2 shows the proportion of cases relating to proposed regulated industries, broken down by scam engagement and scam misuse, illustrating that almost one third of scams reported to IDCARE are engaged through social media, while almost half of all scam misuse was facilitated through the banking sector (bank industry misuse includes a range of outcomes from sending funds to scam account, to a scammer opening a bank account in a victim’s name after a scam event); note that there is overlap between cases, as a single case may be affected by more than one industry.

Table 2: Proportion of cases relating to proposed regulated industries (1 Oct 23 – 30 Sep 24)

	Banking	Telcos	Social Media + Messaging Apps
% of scam cases where the <i>misuse</i> * was industry facilitated or hosted	47%	2%	2%
% of scam cases where the <i>engagement</i> * was industry impersonated or facilitated	6%	6%	28%

Misuse* refers to situations where the scammer targeted products and services. *Engagement* refers to enabling channels relied upon by scammers.

In circumstances where engagement with a scam was through a website, we record the type of deception used, as shown in Table 3. IDCARE data illustrates that more than a third of scam cases initiated via a website engagement were through a legitimate website which contained malicious ads, products or services. In comparison only 20 percent were through scam websites impersonating legitimate sites. This data brings attention to the need for legitimate site operators to monitor and remove malicious content and suggests that the

proposed industry of *paid search engine advertising* may not be sufficient to disrupt scam website engagement. Consideration should be given to broadening the sector code to include all paid advertising, whether it be through a search engine or a legitimate website.

Table 3: Website scam engagement deception type (1 Oct 23 – 30 Sep 24)

	% of scam cases initiated via website engagement
Legitimate website contained malicious ads/ products/ services/ people	35%
Fake website	28%
Genuine service (ABN, police check, travel visa) engaged through a scam 3rd party website which deceived the victim into paying money to the scammer	19%
Impersonation of legitimate website	19%

Definition of scam

The proposed scam definition is too narrow to adequately protect SPF consumers. Primarily, the examples of exclusionary provisions to be contained in the SPF rules indicate the definition of scam is not intended to cover further offending by the scammers following their engagement with scam victims. In a very large percentage of scam cases, the target of their deception shifts from the individual to the institution, such as financial institutions and government agencies. Such cases are typically not often reported as scams by targeted institutions and the current Framework lacks in its awareness of these very connected criminal activities.

Under the current definition of scam, the proposed Framework will not address this very real and extended risk to the community whereby compromised victim information is used to target other entities by scammers. IDCARE has found that a common instance of this event involves the harvesting of a victim’s credentials via a scam, followed by the fraudulent opening of a bank account in the victim’s name. Of our clients involved in scams, 14% experienced such co-occurring misuse and a further 30% experienced the scamming of industry and government in the name of victims who were unaware of how threat actors first got their information.

To orient compliance on the last phase of the criminal value-chain where the consumer engages the scammer is often not the last time the scammer exploits that individual. The definition as drafted ignores the complexities and enduring risks that commonly unfold and are likely to not be captured in current government or industry reporting mechanisms. The absence of this understanding is evident in the current code and most likely speaks to Government reporting on scams and cybercrimes being a “point in time” reporting measure where what then unfolds for scam victims are not captured or fully understood. This is a major difference with IDCARE’s case management approach where often the subsequent post-initial scam exploitation is captured. To address this major deficiency, IDCARE proposes the following amendment:

Recommendation – Scam definition

(1) Scam definition breadth: The definition of a *Scam* should be broadened to encompass fraudulent misuse that takes place without the actions of the identity owner, to reflect the reality that following the initial scam engagement, scammers typically continue to exploit that individual by targeting institutions directly (such as banks and government agencies), including institutions with which the individual has never had a relationship, and that risks to individuals endure long after the victims' initial engagement with the scammer.

(1)(a) amendment to clause 58AG

Current Exposure Draft

CI 58AG Meaning of scam

(1) A scam is a direct or indirect attempt to engage an SPF consumer of a regulated service that...

Recommended Amendment to Exposure Draft

CI 58AG Meaning of scam

(1) A scam is a direct or indirect attempt to engage an SPF consumer of a regulated service *or directly or indirectly attempt to engage with a regulated service through impersonating an SPF consumer* that...

[with an addition to sub-cl 58AG(2)]:

(2) *(e) deceptively impersonates or attempts to deceptively impersonate the SPF consumer into facilitating an action by the regulated service.*

The extension of the proposed definition will cover at least a third of all case scenarios reported to IDCARE. Hence this scenario is a major deficiency in the current exposure Bill and the overall mechanics of the reforms proposed.

If the recommended amendments to the definition are accepted, then there are flow-on implications for the meaning of an SPF consumer which as currently drafted assumes that the consumer has a relationship with the regulated entity. In many of these subsequent flow-on effects from the scam engagement, the victim may have no pre-existing relationship with the regulated service. These include instances where the scammer creates a new relationship with the regulated service on behalf of the victim.

This common scenario is not contemplated in clause 58AH of the Exposure Draft and a recommended change is provided as follows:

Recommendation – Scam definition

(1)(b) amendment to clause 58AH

Current Exposure Draft

CI 58AH Meaning of SPF consumer

(1) An SPF consumer, of a regulated service, is:

[...]

who is a person to whom the regulated service is or may be provided or purportedly provided.

Recommended Amendment to Exposure Draft

CI 58AH Meaning of SPF consumer

(1) An SPF consumer, of a regulated service, is:

[...]

who is a person to whom the regulated service is or may be provided or purportedly provided, *whether the SPF consumer is being impersonated or not and where the SPF consumer has a pre-existing relationship with the regulated service or not.*

These proposed definitional adjustments will allow the SPF to more accurately reflect the scam exposure to the Australian community across regulated services. The implications of not making these changes would be an artificial barrier for victims to address the more likely risks they will confront. This type of ongoing exploitation can be incredibly difficult for individuals to correct and prevent, and we have had clients who report false accounts and cards being initiated many months after they first detected the scam and have taken response measures, such as replacing government-issued identity documents. In some extreme cases, community members have opted to change their name and move interstate in the expectation that this will prevent ongoing misuse (when it doesn't).

Response standards

The draft Framework does not include a definition of 'reasonable steps', but rather foreshadow the creation of "sector-specific codes" (cl 58CA). This is appropriate to enable the Codes to be tailored to the diversity of entities that will be regulated. Nevertheless the Framework legislation should ensure that there are clear minimum standards that will be expected to be contained in each industry code. In our experience there is typically a mismatch between what consumers consider reasonable and what the entities they are dealing with consider reasonable.

The Framework should include minimum standards that can be translated into clear guidance in the specific industry and sector. We address two specific examples of these in the following subsections, namely:

- (i) Timeframes and reasonableness; and
- (ii) Suspicious transactions and Government inclusion.

Timeframes and reasonableness

The Scams Prevention Framework should explicitly require the sector-specific Codes to include meaningful timeframes, as well as definitions of reasonableness that fit with industry contexts. Over the previous 12 months, IDCARE clients experiencing scams reported that it took an average of 17 days to detect they had been scammed, it took clients six days to detect misuse after it had occurred. Timeliness of response is critical and it is common for scam victims to literally experience secondary crimes committed before their eyes and be powerless to stop it in the moment.

For example, an IDCARE client reported that they had received a “Sorry to see you go” text message from their telecommunications provider; their phone then switched to SOS only and service was lost. An email confirmed that the phone number had been ported to another provider. Then, her email address, connected to the telecommunication account, was hacked and access was denied. This all happened in a matter of minutes, while the client was watching. They tried to contact their service provider immediately via telephone but were unable to make contact with support as it was out of business hours, they then tried their social media service but again the relevant support team was only available via an online form and not responsive as a ‘live’ communication.

In the absence of minimum standards there will continue to be considerable variability in what consumers experience as response measures applied across the proposed regulated industries. In one recent case a member of the community alerted their financial institution to a potential risk that their account may be accessed by scammers targeting the institution in their name following a scam, only for \$30,000 to be transferred out of their account two weeks after being alerted to the risk. The financial institution at the time of initial notification of risk refused to provide details to the consumer about what protections that could expect to be put in place and by when.

IDCARE recommends the following be minimum standards to be inserted into the Scams Prevention Framework with an obligation to apply in every sector-specific code:

Recommendation – Response standards

(2) Explicit minimum prevention and response measures in a new provision in *Division 3 – Sector-specific codes for the Scams Prevention Framework*

CI 58CAA Minimum prevention and response measures for regulated services

- (1) Prevention measures are extended to all SPF consumers that believe they are at risk of scam exploitation within one business day following customer identification and receipt of request (either directly from the SPF consumer or their advocate).
- (2) The reasonableness of response measures should include:
 - (a) altering the SPF consumer via an agreed channel of engagement any proposed changes to their accounts or applications for new services prior to advancing such changes;
 - (b) altering the SPF consumer via an agreed channel of engagement any prior changes from the determined “at risk” period (for example, a date upon

which the SPF consumer believes the scammer obtained information that could enable further criminal exploitation) within one business day of detecting such risks.

Suspicious transactions and Government inclusion

For the avoidance of doubt, scam-related transactions for entities regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) should be included as suspicious matters under Division 2 of that Act. The current proposed Framework does not include obligations on Government to advance and apply minimum response standards in preventing, detecting, investigation and responding to scams. As was revealed by IDCARE client reports, the Commonwealth is among the top three most targeted sectors by scammers. Not including the Government as a sector with scam obligations will preclude the Framework from achieving the economy wide or so-called ‘ecosystem’ approach to enhancing Australia’s resilience to such crimes foreshadowed in the Exploratory Draft and Explanatory Memorandum. This inclusion would also require further reflection of where consumers with complaints would go to resolve their disputes (such as the Commonwealth Ombudsman).

As a very practical measure, ensuring that AUSTRAC is able to receive suspicious matter reports relating to scam destination accounts will allow the Commonwealth to proactively identify other Australians who may be scammed and sending money to the same accounts but unaware they are doing so. This is a critical measure currently absent in the proposed SPF and is a very practical and meaningful way the Commonwealth can demonstrate a stronger return on investment for the considerable burden placed on regulated entities to report against AML/CTF Act requirements by proactively identifying and disrupting scams targeting the Australian population. This should be an obvious and documented response from the Commonwealth and not one left to chance behind closed doors and at the discretion of policy makers. It is also a very obvious performance measure to report upon in any such code – that is community members to find out they are involved in a scam by Government.

Recommendations – Suspicious transactions and Government inclusion

- (3) Suspicious transactions in the AML/CTF Act:** Scam-related transactions for entities regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) should be included as suspicious matters under Division 2 of *that* Act, for the avoidance of doubt.
- (4) Government response measures:** The Scams Prevention Framework should include obligations on Government to advance and apply minimum response standards in preventing, detecting, investigation and responding to scams.
- (5) AUSTRAC monitoring of suspicious transactions:** AUSTRAC should be able to receive suspicious matter reports relating to scam destination accounts will allow the Commonwealth to proactively identify other Australians who may be scammed and sending money to the same accounts but unaware they are doing so.

Information privacy and control

The proposed Scam Framework's Principles and the information sharing provisions in *Division 5 -Subdivision C* fail to acknowledge the importance of information privacy and do not sufficiently address the requirements outlined by the Australian Privacy Principles (**APPs**). This omission poses a significant risk to the privacy rights of individuals, as it fails to consider the balance between scams disruption and safeguarding personal information. IDCARE has seen firsthand how scam responses can cause further real harms to scam victims when individuals are not notified of these measures and have no control over them.

While there are safeguards for entities in not having to publish their policies, there is no requirement for regulated entities to ensure that prevention and disruption measures are disclosed to SPF consumers affected by their actions. As one example of the consequences on consumers where their information is shared without prior consent and in the absence of transparent prevention and response standards, IDCARE clients frequently report that their identity information has been flagged with a Credit Reporting Body without their knowledge or consent, and they have consequently been unable to access credit or verify identity documents - even after making several requests for the flag to be removed (once discovered). For clients who are already experiencing financial hardships these blocks on verification and credit cause extreme stress and further harms.

To avoid causing further harm to scam victims and ensure that SPF consumers maintain their rights to privacy and control over their personal information, the following critical points should be addressed:

1. **Adequate emphasis on information privacy:** the Framework does not adequately emphasise the protection of personal information that could be collected, shared, or processed as part of scam prevention measures. The APPs mandate that individuals have a right to control how their personal information is collected, used, and disclosed. Any Framework that collects data for scam prevention must align with these privacy principles to prevent further harm, potential misuse or overreach.
2. **Individual control and consent mechanisms:** the Information Sharing provision allows the Regulators to disclose information without notifying the individual about the disclosure or of the use of information, and the Principles do not include mechanisms for obtaining user consent. Under the APPs, individuals have the right to consent to the collection and use of their personal information and to know when their information is being processed. For example, where an individual has their account flagged for scam risk they should, where practicable and reasonable, have the opportunity to remove protective measures. Further, these protective measures should be removed within a defined timeframe.
3. **Actionable scam intelligence safeguards:** Actionable scam intelligence should have clear and transparent safeguards to prevent further harms to victims of scams, this includes providing assurance that the scammer attributes shared are not real victim information used by scammers (a common strategy of scammers). As one example, a client had her home unexpectedly searched by police because her identity documents had been used in further scams. While actionable intelligence is important it is equally important that SPF consumers do not have their privacy violated in the process. This concept should be pursued with caution, ensuring that victim's personal information is not shared without proper safeguards and ongoing consent.

4. Minimise potential risks of data overreach: In combatting scams, there is a risk that entities could over-collect or retain personal data beyond what is necessary. The current Framework does not address how data minimisation and proportionality will be maintained, which are key requirements under the APPs.
5. Provide clarity on non-Regulator data sharing and third-party involvement: the Framework fails to provide transparency on how personal data may be shared with third parties in the absence of SPF consumer consent, such as law enforcement agencies or industry partners. IDCARE has previously received reports from clients who have been engaged by law enforcement for suspected involvement in scam activities. In 2023, a client contacted IDCARE reporting that his MyGov account had been accessed and that a fraudulent tax return had been lodged in his name. He contacted the ATO and advised them of the fraud but did not take further action. Later, he noticed that several new bank accounts had been created in his name. Eventually this client was forced to close some of his legitimate accounts as his bank had become suspicious. This misuse culminated in law enforcement raiding the client’s house. The APPs require that individuals are informed about who their data is shared with and for what purpose. Without clearer privacy guidelines for data sharing, the sector-codes could infringe individuals' privacy rights and enable ongoing and further harms to scam victims.
6. Provide guidelines on Regulator data sharing: Interoperability of entity reporting will likely be integral to the success of the Scams Prevention Framework, it is understandable that regulated entities are expected to share information. It is promising to see that the information sharing provision is one which attracts civil penalty. However, it is important that reporting guidelines are established to ensure that consumers do not have their privacy, in any way, impugned because of information sharing between organisations. As a potential solution to mitigate this risk, guidelines may be established to ensure that reports which contain information relating to scam victims and consumers are appropriately anonymised and de-identified.

To protect individuals' privacy rights while effectively preventing scams, the right to information privacy and control should be explicitly incorporated into the Scam Prevention Framework legislation. By aligning with the Australian Privacy Principles, the Framework can ensure that personal data is collected, used, and shared responsibly, with individuals retaining control over their personal information.

Recommendations - Information privacy and control

- (6) Incorporate privacy-by-design in the Scam Prevention Framework:** the Framework should include privacy-by-design principles, ensuring that information privacy is embedded into the Framework’s architecture from the outset. For example, the Framework should:
- explicitly emphasise the protection of personal information,
 - align with the APP principles,
 - address how data minimisation and proportionality will be maintained,
 - require entities involved in scam prevention to inform individuals about how their data is collected, used, and shared

- provide transparency on how personal data may be shared with third parties in the absence of SPF consumer consent, such as law enforcement agencies or industry partners.

- (7) **Individual control and consent mechanisms:** the Framework should mandate clear mechanisms for notification, consent and control. Individuals should be notified when protective measures are put in place, and they should have the opportunity to remove protective measures, within stated timeframes.
- (8) **Actionable scam intelligence safeguards:** Actionable scam intelligence should have clear and transparent safeguards to prevent further harms to victims of scams, this includes providing assurance that the scammer attributes shared are not real victim information used by scammers (a common strategy of scammers).
- (9) **Regulatory data sharing:** Privacy Impact Assessments should be required and Guidelines should ensure that SPF consumers do not have their privacy impugned because of information sharing, including, but not limited to, requiring publication of privacy Impact Assessments anonymisation and de-identification of reports which contain information relating to scam victims.

Dispute resolution

The proposed Framework also touches on internal dispute resolution mechanisms for complaints and external dispute resolution schemes.

Internal dispute resolution mechanisms should be subject to regular review by the respective regulator. Many entities in the proposed regulated sectors currently have access to contact channels to report scams, however, IDCARE clients have nonetheless faced consistent structural barriers. For example, IDCARE clients have reported that they were not notified that their phone number was being ported or that a sim-swap was occurring. Other IDCARE clients expressed concerns that their banks failed to respond in a reasonable timeframe to their concerns. These concerns are particularly pronounced for consumers of social media, common feedback for this industry reflects a concerning inability to directly engage with the entity.

In our previous submission on the Scam Code, IDCARE flagged that external dispute resolution (**EDR**) mechanisms should be implemented with the consumer in mind. A common concern for consumers is a need to report to each individual organisation, for example where an individual needs to report to their telecommunication provider in the event of sim-swap, they will then likely need to engage with their bank and other institutions to rectify the misuse and prevent further harm. These systems should be as easily navigable for consumers and reduce the need to report to several different entities.

Recommendations – Dispute resolution

- (10) **Internal dispute resolution:** Internal dispute resolution mechanisms should be subject to regular review by the entity’s respective regulator to ensure they are fit for purpose.

- (11) **External dispute resolution:** External dispute resolution systems should be as easily navigable for consumers and reduce the need to report to several different entities.
- (12) **Government dispute resolution:** mechanisms for dispute resolution services for consumers with grievances about government decisions and actions should be detailed.

Concluding remarks

The past 12 months have seen a significant number of scams reported to IDCARE, with half of these cases involving industries proposed for regulation under the Scam Prevention Framework. However, the current draft of the SPF is too narrow to fully address the complex and enduring threats posed by scams, particularly the ongoing misuse of compromised victim information. As our data demonstrates, scammers often shift their focus from individuals to institutions, yet this is not captured by the proposed Framework. Without expanding the definition of scams and including robust mechanisms to address the aftermath of the initial scam, the Framework will fail to protect a significant portion of scam victims.

Additionally, the Framework must include clear, enforceable minimum standards that are obligatory for all sector-specific codes, including for response timeframes, reasonable actions, and suspicious transaction monitoring to ensure consistency in how scams are handled. Moreover, information privacy and control must be prioritised within the Framework to prevent further harm to victims and ensure alignment with the Australian Privacy Principles. This includes explicit mechanisms for SPF consumers to be notified about the measures and respond, actionable scam intelligence safeguards, and enhanced transparency and guidelines for data sharing both between regulators and from entities to their parties.

While a Scams Prevention Framework is a necessary step, the current Exposure Draft requires amendments. By broadening the definition of scams, instituting minimum standards for response, and prioritising information privacy, the Framework can more effectively address the full scope of scam risks and provide better protection for community members. Without such change there is a real prospect the current draft Framework will result in higher regulatory costs with an absence of meaningful resilience outcomes, at the sacrifice of individual privacy rights. None of these are insurmountable issues and the opportunity to have a Framework that seeks to advance positive outcomes for the Australian community's overall scam resilience is to be commended.