AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Proposed Scams Code Framework

ACCC Submission in Response to the Treasury's Scams – Mandatory Industry Codes Consultation Paper

5 February 2024

Introduction

The Australian Competition and Consumer Commission (**ACCC**) welcomes the opportunity to comment on the Mandatory Industry Codes framework (the **Framework**) proposed in the consultation paper released by the Treasury on 30 November 2023 (**Consultation Paper**).

The ACCC has called for the introduction of consistent, mandatory, and enforceable eco-system wide obligations to reduce the harm to Australians caused by scams. The development of obligations that are enforced will provide an effective mechanism to prevent scammers connecting with Australians and taking their money or personal information, supplementing, and supporting the cooperative efforts under the National Anti-Scam Centre. As such, the progress represented by the Consultation Paper initiatives is welcomed.

The ACCC recognises a whole of ecosystem approach will necessarily involve some regulatory complexity. A multi-regulator model recognising existing structures and legislative arrangements provides practical advantages in sectors that currently have licensing arrangements (banks and telecommunications) and existing regulatory oversight. However, for the Framework to work effectively, further legislative change is required to facilitate efficient information sharing between regulators and to provide for workable delegations between the system-wide regulator (the ACCC) and the sector-specific regulators. Without these additional steps, the multi-regulator model may lead to silos, duplication, and undue burden on regulated entities.

This submission focusses on how the Framework can be further enhanced to protect Australians more effectively and provide workable regulatory oversight without undue burden on industry.

The ACCC and the National Anti-Scam Centre

The ACCC is an independent Commonwealth statutory agency that promotes competition, fair trading, and product safety for the benefit of consumers, businesses, and the Australian community. The primary responsibilities of the ACCC are to enforce compliance with the competition, consumer protection, fair trading, and product safety provisions of the *Competition and Consumer Act 2010* (**CCA**), regulate national infrastructure, and undertake market studies.

In 2023, the government allocated $58 million over 3 years to establish the National Anti-Scam Centre within the ACCC to make Australia a harder target for scammers. The National Anti-Scam Centre commenced on 1 July 2023 with a focus on three key capabilities:

- **Collecting and sharing data and intelligence** across the scam ecosystem to enable the early identification of scam trends. This intelligence, shared with law enforcement, government departments and agencies, consumer groups, and the private sector, will inform education and disruption efforts, focusing on early intervention to reduce or prevent losses to scams.
- **Coordinating scams prevention, disruption, and awareness activities** by drawing on expertise across government, law enforcement, industry, and consumer organisations to lead a nationally coordinated, timely, anti-scam strategy.
- **Helping consumers spot and avoid scams** by working with the National Anti-Scam Centre partners across the scams ecosystem to support consistent messaging and provide better education resources to help consumers protect themselves and others.

Through our capabilities, and by coordinating engagement across all states and territories, the National Anti-Scam Centre provides leadership in making Australia the world's hardest target for scammers. We are already seeing early signs of success since the establishment

of the National Anti-Scam Centre. For example, Australians reported total losses of $83.63 million in the October to December 2023 quarter, down 42.03% for the same quarter in 2022 and down 24.93% from the July to September 2023 quarter. However, whilst greater cooperation goes a long way to addressing scams, the Framework is important and necessary to support this work. In particular, the Framework will help ensure consistency and avoid weak links where businesses choose not to cooperate or sufficiently invest in scam detection and prevention.

Consumers must be at the heart of this Framework given the significant harm resulting from scams. Consistency in the application of protections set out in the codes across sectors will be crucial to ensuring all Australians are safeguarded, and well supported through dispute resolution processes where scammers infiltrate these safeguards. ACCC Scamwatch data in Table 1 demonstrates the wide variety of contact methods scammers use to target victims, highlighting current gaps which mandatory, enforceable codes must help close.

Table 1. Top 5 contact methods by financial loss (2023)

Contact type	Financial loss	% change in losses from 2022	No. of reports	% change in reports from 2022
Phone	$117.2m	16.9% decrease	55,420	13.2% decrease
Social networking	$94.7m	18.1% increase	17,544	30.7% increase
Email	$80.3m	3.9% increase	85.944	64.8% increase
Internet	$70.2m	5.6% decrease	17,566	28.3% increase
Mobile apps	$65.1m	9.1% decrease	8,101	19.5% decrease
SMS	$27.1m	4.9% decrease	109,623	37.3% increase

Scammers are becoming more sophisticated in their contact methods, often using digital or web-based technologies to target victims. As highlighted in Table 1 above, 2023 Scamwatch reports reflect an increase in contact made through social media, email, SMS and internet, meanwhile phone and mobile application contacts have declined.

The range of contact methods highlights the need for a multi-regulator model and for the ACCC as the system-wide regulator acting as a safety net to capture entities not explicitly covered by a code. It also provides an opportunity for digital platforms, particularly messaging and social media platforms, to take consistent and effective action to reduce the increasing losses to scams on their services.

ACCC's approach to the consultation and submission

The ACCC, through the National Anti-Scam Centre, has engaged extensively with Treasury, regulators, consumer organisations and industry about the Code framework since the release of the Consultation paper. This includes bilateral meetings and participation in the following Treasury stakeholder roundtables:

- Telecommunications sector (15 January)
- Banking sector (18 January)
- Digital communications platforms (23 January)
- Consumer groups (19 January)

The National Anti-Scam Centre has also participated in the multi-regulator workshops and has actively promoted the Treasury consumer survey to its stakeholders and scam reporters.

The ACCC has not expressed views on all questions in the Consultation Paper. We note many of these matters have been discussed with Treasury and stakeholders at various forums during the consultation period. Instead, we provide some key recommendations to assist Treasury in designing a Framework that will provide material benefit to Australians impacted by scams. The ACCC will continue to engage and offer our scams expertise as the Framework is further developed.

Summary

The ACCC has called for and endorses the introduction of mandatory and enforceable scams codes to promote consistent measures across sectors to address scams, and provide clear roles and responsibilities for the Government, regulators, and the private sector.

Key points the ACCC highlights in this submission include:

1. The Framework must be **consumer focused**. Even with the best efforts by industry and government, some consumers will inevitably be impacted by scams.
    - The Framework should provide simple and clear pathways for consumers to seek assistance from a business or businesses used in a scam with mandatory internal dispute resolution (**IDR**) and a **simple, single pathway for external dispute resolution** (**EDR**).
    - By their nature, scams involve deception. The approach to consumer reporting and redress needs to consider **trauma informed approaches to victims** that ensure they get the support they need and are not re-traumatised through the dispute resolution or other processes.
    - The Framework would also benefit from clear articulation that where there is a breach of the obligations, **compensation or redress** will apply. Businesses should be incentivised to resolve consumer complaints about scams quickly and to make the investment necessary to ensure prevention and disruption efforts are effective.
2. The ACCC recognises the practical benefits of proposed **multi-regulator model,** noting legislative change will be required to facilitate effective and timely **information sharing** between regulators. Delegation powers that are effective and workable will also be required. In particular, the model will be enhanced if the ACCC also has the power to delegate its powers to Australian Securities and Investments Commission (**ASIC**) and/or the Australian Communications and Media Authority (**ACMA**) on a case-by-case basis for breaches of the overarching obligations. Current delegation powers are ineffective and should not be relied upon for this Framework. Absent these enhancements, we are concerned the model will lead to silos and duplication which will undermine the whole of ecosystem approach and burden industry.
3. The obligations in the overarching legislation and the codes must provide **meaningful enhancements to scam protections, consistent obligations across sectors, and must be enforceable**. The Framework should enable the National Anti-Scam Centre to require any business to **take down scam content** or block scammers exploiting legitimate services. This would provide a mechanism to take swift action even where a business falls outside the Framework and prevent scams exploiting gaps in the whole of eco-system approach.

4. The Framework should be refined to ensure that it **enables effective disruption initiatives** across the eco-system to prevent harm. This would be enhanced by a **workable definition of 'scam'** that will not require businesses to undertake lengthy investigations to determine if conduct is a scam before taking prompt action and offering dispute resolution.

The Framework should be designed to minimise victimisation and loss

The National Anti-Scam Centre's analysis of Scamwatch[1] reports from 1 January to 31 December 2023 shows that Australians made over **301,000 scam reports**, representing a 26% increase compared to 2022. Understanding from these reports how scammers target their victims and secure money from Australian consumers and businesses will assist to develop an effective anti-scam Framework.

Over 108,000 reports related to phishing scams; 39,000 related to false billing scams; and 21,000 to online shopping scams.

Financial loss

In 2023, total reported losses to Scamwatch was **$481 million** representing a 5% decrease[2] from the $568 million reported lost in 2022. These figures reflect Scamwatch data only, with actual losses likely to be higher given the many consumers who do not lodge a report for various reasons, including feelings of shame, unawareness of reporting options or processes or belief the agency reported to would not be able to assist. Most of these losses occurred in 5 key scam types:

- investment scams ($293.5m)
- romance scams ($34.4m)
- false billing ($27.9m)
- phishing ($26.1m) and
- job scams ($24.6m).

Over 2,400 reports were made by small and micro businesses with $17.3 million reported lost.

How scammers target Australians

Scams can occur through direct communication from a scammer via phone call; SMS; over the top and messaging services; social networking; email; webchat and forums. They may arise from in-person contact. They will generally involve multiple contact methods.

Scammers may set up websites, social media presence, use telephone numbers, email and messaging services to target victims. They may also pose as businesses or services that have websites, apps and online marketplaces. They may advertise and appear in search results and on review platforms. They also impersonate known businesses, government, charities, and individuals.

[1] Scamwatch is a key, but not the only source of scam reporting data. Consumers also report to their bank, ReportCyber and a range of other institutions and organisations. Enhancing information sharing between these sources of data is a key project of the NASC.

[2] Note the removal of a significant outlier in Scamwatch report data.

Payment methods

In 2023 the most reported payment method was bank transfer with $214.8 million reported lost. This represents an increase of 2%. This was closely followed by cryptocurrency with $160.9 million reported loss (an increase of 0.2%).

Personal information loss

In 2023, around 58,000 Australians reported to Scamwatch that they lost personal information in a scam (this compares to about 29,000 who reported financial loss). This includes identity credentials such as driver licence or passport; bank account or credit card information; account details or passwords for banking; social media or government services like MyGov.

The use of personal information obtained in a scam can lead to ongoing harm including potential for full identify takeover and financial loss.

Emotional and social harm

Scammers use a range of tactics that can include social engineering, grooming, blackmail, and threats. Some scams, such as romance scams, can occur over months or years where victims are tricked into thinking they are in a real relationship.

Reports to Scamwatch highlight the significant emotional and social harm caused by scams. Many Australians report losing their entire lifesavings; their superannuation; their home and their families. The consequences of this can lead to mental health crises. The ACCC has been made aware of Australians who have died by suicide as a direct result of a scam.

1. The Framework must be consumer focussed

Scammers use services provided by legitimate businesses and quickly adapt to target less regulated sectors and/or new technologies, making it difficult to predict all sectors that may either need to respond to specific scams or need to be brought under the Framework in future. For this reason, the ACCC supports the development of general obligations to ensure the Framework can be enforced by the system-wide regulator, irrespective of whether an entity is specific regulated under a code.

A whole of ecosystem EDR scheme would better support consumers and provide clarity for businesses

The role of the National Anti-Scam Centre has demonstrated the importance of having a single source for consumers to engage with. The ACCC considers the establishment of a whole of ecosystem EDR scheme, catering to all sectors covered by the Framework, would better support consumers and provide clarity for businesses. Under such a model, consumers who are unsatisfied with the IDR process of their service provider would need to engage with only one EDR scheme.

Adopting a single EDR scheme would avoid the need for consumers to make several reports and/or make complaints to separate EDR schemes to seek a resolution. It would also avoid any disputes about which EDR scheme applies which could leave the consumer without resolution.

Further, as discussed above, the impact of scams extends beyond just financial losses, with many victims experiencing severe emotional distress and/or a significant administrative burden including impacts of identity compromise and credit default listings.

Compensation should be available to victims of scams where obligations in the codes have not been met. Embedding adequate compensation for consumers in any EDR scheme is important both for consumer protection, as well as incentivising industry to make appropriate investments in their systems and processes to detect and address scams. An EDR scheme should have powers to award compensation to victims for:

- direct financial loss that occurred as a result of the scam
- significant inconvenience and time taken to resolve the matter
- interference with the complainant's expectation of enjoyment or peace of mind
- fees for re-issue of identity documents, or re-opening of any accounts.

Restitution for broader consequences flowing from scams should also be offered under EDR, for example restoring victims' credit ratings with credit reference agencies.

Reporting and redress should adopt a trauma informed approach

The Framework should provide simple and clear pathways for consumers to seek assistance from a business or businesses used in a scam. The Framework needs to recognise that in most scams multiple intermediaries may be involved, and the information asymmetry will be greater than in most consumer to business interactions. For example, a consumer is unlikely to understand fully how the scam has occurred or which intermediaries have been involved. The consumer in most cases will not have the skills or technology to obtain the information relevant to identifying where to seek redress or proving that a business did not comply with an obligation. For example, currently many scam victims ask their bank to provide information about the recipient bank and bank account, but this is often not provided to the victim. Obligations for IDR and EDR should recognise this information asymmetry and provide a simple, single pathway.

In almost all instances of a scam a criminal offence will have been committed by the scammer. The Framework needs to recognise that victims of these crimes will not only be navigating processes under this Framework but may in some cases also need to make a report to law enforcement and may be involved in investigative processes with police authorities in Australia or even overseas. The approach to consumer reporting and redress needs to consider trauma informed approaches to victims that ensure they get the support they need and are not re-traumatised through the dispute resolution or other processes that require them to report the scam repeatedly.

The Framework would benefit from clarity about when compensation or redress may apply. Businesses should be incentivised to resolve consumer complaints about scams quickly and not use the Framework as a mechanism to refer consumers across the eco-system. It is our view that at a minimum, compensation should apply where a consumer suffers loss and the requirements of the Framework have not been met.

The impact of scams on victims extends beyond just financial losses. Depending on the scam, victims may experience severe emotional distress and/or a significant administrative burden. Support and complaints handling should be carefully designed to specifically recognise and mitigate these harms and remove any stigma associated with reporting their experience. There can be many reasons scam victims do not make a report or seek any assistance

- due to the shame or guilt they may feel
- not knowing reporting was an option
- not thinking that agency reported to would be able to do anything or that the report would assist broader anti-scam work

- not knowing where to report the issue.[3]

The Framework must ensure complaints and redress avenues are well publicised, easily accessible, easy to navigate and designed to genuinely assist victims. Further, the Framework should ensure victims are encouraged to report to a single source, and that there are systems in place to share information across the National Anti-Scam Centre, regulators and industry so victims do not need to make duplicate reports. When effective, timely information sharing processes are implemented for industry and regulators under the Framework (as outlined in Part 2 below), the ACCC would strongly support consumers pursuing and reporting to the proposed whole of ecosystem EDR body. This would further facilitate the National Anti-Scam Centre continuing its monitoring role through Scamwatch, given reports would be provided routinely through information sharing processes.

2. Designing an effective multi-regulator enforcement model

The ACCC recognises the need for the proposed multi-regulator enforcement model. However, there are several key elements required for this model to be workable for regulators and to provide certainty for businesses.

The proposed multi-regulator model

At a high-level, the model will be enabled by:

- Articulation of scam priorities by each regulator, informed by the National Anti-Scam Centre data.
- An effective information sharing regime between regulators and EDR scheme(s).
- Effective powers of delegation between regulators.
- Cooperation and consistency in messaging from the ACCC, ASIC or ACMA to regulated entities;
- Key regulators utilising one scam reporting mechanism and consumer information source (Scamwatch) and not creating more pathways, duplication or confusion for consumers

Without these enablers, the overlap of roles and responsibilities of each regulator that is necessary to create a whole of ecosystem framework has the potential to result in considerable duplication in investigative work for regulators. Dealing with enquiries from multiple regulators can also be burdensome for regulated entities, complainants, witnesses, and other interested parties.

Compliance and enforcement powers and remedies

We consider enforcement tools, remedies, and penalties should be consistent across the Framework, and regulated entities should not be exposed to greater or different information gathering tools (with differing consequences for non-compliance) or different penalties, subject to whether a matter is dealt with by a sector specific regulator or referred to the ACCC.

That said, noting the size of some of the businesses within the ecosystem, a highest common denominator approach is recommended – that is, the strongest compliance powers should be available equally across all regulators. Further, material penalties are

[3] Voce I & Morgan A 2023. Cybercrime in Australia 2023. Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

required to act as a deterrent for non-compliance. Any applicable penalties must be sufficient to avoid the perception they are merely 'the cost of doing business'.

Penalties for non-compliance with digital communications platform code

The maximum penalty for breach of a civil penalty provision under the *Broadcasting Services Act 1992* (**BSA**) is 2000 penalty units[4] (currently $626,000). This is much lower than the maximum penalties available for non-compliance under the CCA, where the maximum penalty is the greater of:

- $50 million;
- three times the value of the benefit obtained, or
- 30 per cent of the corporations adjusted turnover during the breach.

Many of the businesses likely to be covered by the digital communications platform code, and many of the businesses in respect of which the ACCC has raised concerns about scams, are large, global digital platforms. The penalties currently available under the BSA are insufficient to encourage compliance by multi-billion dollar digital firms. Accordingly, to effect general deterrence penalties for non-compliance with the digital platform communications code should attract the maximum penalties available under the CCA.

The ability to delegate powers to sector-specific regulators

As the system-wide regulator, the ACCC should have the ability to act in relation to the sector-specific obligations (in addition to the sector-specific regulator). This would lead to more efficient outcomes where an investigation uncovers multiple breaches of the Core Obligations. This overarching role would position the ACCC as a 'safety net' to catch and take action against businesses not otherwise explicitly covered by a code.

Sector-specific regulators will often have advantages over the ACCC given their role in granting and overseeing licencing arrangements. Establishing an efficient process for the ACCC to delegate its enforcement and related powers to sector-specific regulators, where they may be investigating broader conduct by businesses in the sectors they have responsibility for, would significantly enhance the Framework. Legislative powers of delegation can be supported by introducing standing Memorandums of Understanding between the ACCC and ASIC and/or the ACMA.

Effective information sharing is critical to an effective multi-regulator enforcement model

Streamlined information sharing processes are essential under the multi-regulator model for regulators, the National Anti-Scam Centre, and industry participants. Firstly, a clear framework to facilitate information sharing between regulators is essential to promote timely enforcement action and to avoid regulators working in silos. Unless existing barriers to information sharing are identified and removed, regulators will be delayed in taking action and at risk of duplicating efforts.

Regulators will need to share information including:

- scam reports by victims and non-victims to identify harms and compliance targets
- information which is provided to regulators voluntarily by industry participants
- information which is provided to regulators under their compulsory powers

The Framework anticipates information sharing across various participants in the scams eco-system and the design for how these provisions operate and interact will be critical to

[4] Section 205F.

how effectively the ACCC and other regulators are able to monitor and enforce the code(s) and legislative obligations. We understand the proposed framework anticipates information sharing in the following ways – sharing between:

- the business and one or more regulator(s)
- a regulator and another regulator(s)
- a regulator and one or more covered businesses.
- the business detecting the scams activity with other businesses covered by the same or a different industry code.

The ACCC is concerned to ensure information sharing by businesses with one or more regulator, and by a regulator with one or more business or one or more regulator, is as efficient as possible and results in the lowest possible burden. This could be achieved by designing information sharing provisions so that businesses share information relating to their principles obligations with the ACCC and sector-specific obligations with the relevant sector specific regulator, but supported by an information sharing provision in the legislation or each Code that explicitly provides for that information to be shared with the other co-regulators.

The ACCC has existing information sharing powers under the CCA that could be amended to enable it to share information with the other proposed co-regulators. At present, these provisions are transactionally focussed and would not facilitate the kind of regular and timely information sharing the multi-regulator model would require. Safe information sharing between industry and regulators to achieve enforcement is key.

Effective information sharing is critical to support industry and the National Anti-Scam Centre to disrupt scams

Efficient information sharing within and across sectors and the National Anti-Scam Centre is equally important to ensure scams can be quickly identified and addressed by businesses.

The design of the information sharing framework should reflect the level of risk associated with inadvertent disclosure of the information and the sensitivity levels of the information held. We understand highly sensitive personal information may need to be shared between industry participants across industries to identify and combat scams. Appropriate safeguards should therefore be built into the Framework to ensure information sharing (and use) is limited to what is necessary and no more.

Businesses often raise privacy concerns in sharing scam related information between industry participants and with regulators. One benefit of enshrining the information sharing regime in legislation or the code is that the sharing of personal information could then occur under the exception in Australian Privacy Principle 6.2 which permits sharing information where secondary use or disclosure is required or authorised by or under an Australian law.

For many years the ACCC, and now the National Anti-Scam Centre, has shared information with industry and regulators from reports made to Scamwatch. In most instances this relies on obtaining the specific consent of the scam reporter before sharing the full report with law enforcement or with the business whose services were used in the scam (i.e. the bank or digital platform). The National Anti-Scam Centre also shares scammer identifiers (phone number website, email of scammer, social media profile) etc. with regulators and the private sector. While the National Anti-Scam Centre has these systems in place it is not aware of any other regulator or private sector entity that is sharing scam information to this extent. The Framework should enable more sharing of scammer intelligence and identifiers across the eco-system. This includes removing the requirement for a scam to first be 'verified'

before information sharing can take place to enable regulators and industry to investigate and determine whether something is in fact a scam.

The ACCC also considers APIs could be set up to allow automated sharing with the National Anti-Scam Centre, law enforcement, and other regulators to minimise duplicate and manual handling of information, thus reducing the burden on industry. The National Anti-Scam Centre is currently working towards facilitating information sharing across the eco-system including by leveraging and integrating with existing platforms with the private sector such as the Australian Financial Crimes Exchange. But for this to be successful, private sector entities and regulators such as the ACMA will need to be enabled to share information with the ACCC. Currently the ACMA and the private sector are not sharing information with the ACCC due to privacy constraints.

Penalties for non-compliance with the Framework

The consultation paper also discusses the role of the ACCC in enforcing the principles-based obligations, and identifies existing CCA penalties for non-compliance, but does not explicitly provide for financial redress, except via IDR and EDR schemes. This may limit potential redress to only those cases where a business has breached an obligation in the Framework and/or in a code and investigated by a regulator.

Where enforcement action is taken, remedies are currently available under Part IVB of the CCA. Under the general provisions of the CCA, a court may order a business that has breached the CCA to provide redress (generally via a court-enforceable undertaking) directly to consumers or businesses harmed by the conduct – even where those consumers or businesses have not previously identified or complained about the conduct. The Framework should ensure the same CCA redress provisions apply to scams. Where a business is found to have breached a provision relating to scams, a business may be ordered to provide redress directly to consumers. This should also include a proactive obligation on the business to identify all consumers who were affected by a scam because of the breach.

Alignment with other digital-specific frameworks on dispute resolution

In the government's response to the ACCC's September 2022 Digital Platforms Services Inquiry (**DPSI**) report on regulatory reform, the government noted that it would undertake further work to develop internal and external dispute resolution requirements for digital platforms (including requesting industry to develop voluntary IDR standards by July 2024). The ACCC suggests that the government consider further opportunities for alignment between these future requirements and the dispute resolution requirements as part of the scams framework.

In particular, the ACCC recommended in the September 2022 DPSI report that mandatory IDR standards for digital platforms should ensure accessibility, timeliness, accountability, the ability to escalate to a human representative, and transparency. These standards should apply for any IDR scheme covering scams on digital communications platforms.

Further, there is currently no mention of compensation under either the industry-wide obligations or the digital communication platform-specific obligations. The ACCC notes that, unlike for the telecommunications and banking sectors, there is no existing EDR scheme for digital platform services to facilitate compensation. However, it would be preferable for the scams framework to expressly set an expectation that digital communication service providers should consider whether their consumers should be compensated for scam losses which have occurred as a result of the provider failing to meet its obligations under the

framework (for example, by failing to act within a reasonable time after being notified of a scam on the platform).[5]

Process for code development

In the development of any sector-specific codes in consultation with industry, timeframes should be specified to ensure accountability. While codes are generally easier to amend than primary legislation, there is still often a long period between code reviews of up to 5 years, with implementation of changes then taking an addition 1-2 years. Businesses are also likely to be critical if codes are reviewed or amended too frequently, as this reduces regulatory certainty. As such, it is important to be cognisant of these constraints when considering the extent to which flexibility is needed to respond to future technological and other developments.

In relation to the digital communication platform code, to ensure more timely development we recommend this code be developed by the ACMA rather than by industry. For example, the process for development and registration of 'class 1 content' industry codes under the Online Safety Act 2021 has been relatively long. The Act commenced in January 2022, with the first industry not coming into effect until almost 2 years later in December 2023. For the 2 industry codes which the eSafety Commissioner declined to register and is in the process of drafting industry standards to cover the relevant services.[6] This experience suggests it would be preferable for the regulator to develop the codes itself rather than relying on cooperation and coordination from industry.

3. Overarching principles-based obligations must provide meaningful enhancements

For the Framework to be most effective, it must be mandatory and enforceable with the full suite of CCA remedies and powers available. Applying a strong set of obligations on key sectors across the ecosystem in the CCA is likely to result in more effective and timely outcomes for consumers.

The ACCC supports the development of sector-specific codes and standards, and has identified additional areas for further consideration.

Additional obligations for digital platforms

A significant number of high loss scams originate on digital platforms, as outlined in Table 1 above. In addition to the obligations set out in the Consultation Paper, the ACCC recommends digital platforms be subject to the specific obligations in the overarching legislation to ensure alignment with international regimes on scams and with the ACCC's recommendations in its fifth interim report of the DPSI on regulatory reform:

- **Verification of financial advertisers:** As part of verifying the identity and legitimacy or business users and advertisers, service providers should verify that any prospective advertiser of financial products and services holds an appropriate licence from the ASIC.[7]
- **Communication with parties whose content has been blocked or removed:** Where content is removed on the basis that it is a scam or suspected scam, service

[5] ACCC, Regulatory Reform Report p 84. See also Digital Services Act (EU) arts 14(5) and 15(2)(f), which require platforms to notify affected users about redress possibilities.

[6] https://www.esafety.gov.au/industry/codes

[7] ACCC, Regulatory Reform Report p 85; Financial Services and Markets Act 2000 (UK) s 21; Online Safety Bill (UK) ss 38-40.

providers provide the person who shared the content with a statement of reasons and provide information about dispute resolution options.[8]

- **Protection against misuse:** Service providers should suspend users that frequently share scam content or frequently submit notices that are manifestly unfounded.[9]
- **Policies and enforcement processes:** Service providers should ensure that their relevant policies (e.g. terms of use and enforcement processes) address scam content.[10]
- **Transparency reporting:** In addition to responding to information requests from ACMA or the ACCC, service providers should publish regular reports on actions taken to address scams, as well as data regarding notice-and-action measures (e.g. the number of notices submitted, the time required to respond to notices, respective actions taken, and whether such actions were performed on the basis of automated means).[11] The ACMA should be empowered to specify mandatory information for inclusion in public reports.[12]

Designing effective codes

The ACCC considers that a mandatory code should do more than re-state existing law. It should establish a higher standard of practice beyond what is already required by the CCA. A reasonable degree of specificity is important for both business clarity and to ensure enforceability of the Framework. Conversely, a code that is overly prescriptive may also have the unwanted effect of entrenching minimum standards as the norm and inhibiting businesses from implementing best practice. A balanced approach, bearing in mind the objectives of the code, is therefore required.

To strengthen the obligations, we consider clear and enforceable timeframes for all required actions should be specified. We note, for example, that the United Kingdom's Contingent Reimbursement Model Code establishes minimum standards underpinned by explicit timeframes.

In addition to the obligations proposed, the ACCC recommends that businesses should be required to implement appropriate internal governance mechanisms to enable effective scam prevention and response (for example, appointed responsibility, escalation requirements, board / senior manager visibility and internal reporting). Similarly, the ACCC recommends the addition of obligations on record-keeping to specify the data to be held to facilitate requests for access for enforcement purposes.

'Know Your Customer' obligations required for all sectors

The Framework should require businesses to implement Know Your Customer and robust verification requirements to prevent scammers exploiting their systems. This should also include clear obligations to remove scammers and scam content with enforcement consequences should they fail to do so.

---

8 Digital Services Act (EU) art 15.

9 Digital Services Act (EU) art 21.

10 Digital Services Act (EU) art 12; Online Safety Bill (UK) ss 10(5)-(8), 27(5)-(8), 38(2).

11 ACCC, Regulatory Reform Report p 86; Digital Services Act (EU) art 13; Online Safety Bill (UK) s 78; Online Criminal Harms Act 2023 (Singapore) s 19, Third Schedule paragraph 8. See also the Reducing Scam Calls and Scam SMs Industry Code at cl 6, requiring Australian telecommunications providers to provide quarterly reports to the ACMA about blocked scam calls and SMs.

12 ACCC, Regulatory Reform Report p 86; Online Safety Bill (UK) s 78, Schedule 8.

Anti-scams strategy obligation

While we note some regulators have a role in the approval of relevant company policies (the Australian Energy Regular approving providers' customer hardship policies as an example), it is not feasible or appropriate for regulators under the Framework to assist individual regulated entities to create a compliant anti-scam strategy given the size of the regulated population and their regulatory role as outlined in the Framework. Such an approach would be too resource intensive to be sustainable and requires detailed knowledge of the internal business systems and processes.

We note the ACCC does not provide such assistance in respect of other codes prescribed under the CCA, including where the businesses that must comply are small businesses and may be liable for significant financial penalties where a code is breached. As such, the onus for creating (and maintaining) an anti-scam strategy should be on the regulated entities.

We recommend that under the Framework, the National Anti-Scam Centre develop and publish guidance on compliance strategies to clarify expectations for regulated entities. Relatedly, the National Anti-Scam Centre would expect businesses subject to the codes to take responsibility for distributing scam alerts and direct consumer communications, noting that the most effective communications are targeted to points in time most relevant for the recipient i.e. in transaction process.

Further, the ACCC recommends the consumer-facing aspects of a business' anti-scam strategy should be accessible to the public. This would allow external parties, such as consumer advocacy groups, to see whether businesses' processes are adequate. The public elements of the strategy should help consumers understand:

- the broad anti-scam initiatives which the business has committed,
- the practical implications of the strategy for a consumer's interactions with that business. For example:
    - how the business will alert consumers to scams,
    - how a consumer can report a suspected scam, and
    - actions the business will commit to after a consumer reports a suspected scam.
- the business' obligations and the consumer's rights where a consumer has fallen victim to a scam,
- consumer avenues for redress where a business has not met its obligations or commitments, and
- if the consumer is unsatisfied with the business' response to a scam, information on the relevant external dispute resolution scheme.

4. The Framework should support effective disruption initiatives by all businesses to prevent harm and be adaptable

To fully protect Australians from scams, the overarching obligations should apply to businesses generally, including those not covered by specific industry codes.

Alternatively, to address harm from specific scams, there should be a general power in the CCA to require a business to take down scam content or block or prevent a scammer using a service. Where a request is made, a business must comply unless it can establish on reasonable grounds that the content or conduct was not a scam or scammer. If it fails to do

so, it could be subject to enforcement action under the CCA. Non-compliance with such a request could also trigger liability for consumer losses associated with the scam.

We believe the sectors identified for initial inclusion in the Framework are a good starting point. However, we note scammers currently use services supplied by other sectors not captured under the initial phase of the Framework. For example:

- **Background technologies**: Scammers rely on a range of legitimate services to deceive victims and maintain their anonymity. These include internet service providers, web hosting providers, and virtual private networks. Many scams direct victims to websites, which depend on the services of web hosting providers, however the willingness of hosting providers to voluntarily take down offending websites is highly variable and inconsistent.
- **Remote desktop applications (**such as AnyDesk**) and Encrypted Messaging Services** (such as Telegram and Signal) are a key enabling factor for many scams. Many of these entities are not domiciled in Australia and often do not recognise Australian authorities but, are highly relevant to scams.
- **Non-bank financial services:** Scammers use a range of non-bank institutions to obtain and hide the source of their victims' funds. These include cryptocurrency exchanges, cryptocurrency wallet providers, online remittance services, online marketplaces, gift cards, and web application distribution platforms (such as the Google Play Store and Apple Store).

The Framework will need to evolve quickly to cover the whole eco-system. Scamwatch data highlights that, as currently drafted, there may be areas of the ecosystem that will not be covered and where significant harm occurs. For example:

- cryptocurrency – payments via cryptocurrency exchanges are not covered
- online shopping scams – marketplaces and online stores are not part of the scheme
- other stores – supermarkets and stores are outside the framework. Consider the rise of gift card scams and the actions taken by supermarkets to address it.
- scam websites – general scam websites would fall outside the scheme. There are no obligations on website hosts or registrars to take action to address scams.
- superannuation – a failure by a superannuation firm to verify a customer might lead to harm from a scam
- remote access software providers would fall outside the scope.

Proposed scam definition requires further consideration

The ACCC considers the proposed definition of 'scam' is unworkable. It is too narrow and may have an unintended consequence of excluding conduct that is commonly considered a scam. To provide clarity for consumers and businesses, the ACCC recommends a broad definition of 'scam' be included in the overarching obligations with capacity for further clarification in the industry specific codes. Any further clarification that is needed to reflect the different sectors could be addressed in the sector specific codes.

The ACCC considers the definition needs to ensure that matters the public generally recognise as scams are captured. In many jurisdictions scams are essentially fraud offences, for example the conduct is usually captured by criminal offences relating to fraud against the individual. It may not always be possible to identify a clear demarcation between scams and cybercrimes, such as hacking or identity theft. At the time a scam occurs, a victim will not have enough information to know or understand whether it is a scam or the type of scam.

The Framework should specify the types of matters not covered by the obligations such as fraud against the Commonwealth or employee fraud. It could also clarify that it is not intended to capture conduct where there is no connection or engagement with or from a victim, for example hacking and data breaches. However, caution should be applied because victims will not have the information required to make this determination and matters may need to be fully investigated before it can be determined whether the obligations applied.

The ACCC also cautions against the use of terms such as 'authorised' and 'unauthorised' fraud or scams. The consultation paper refers to "authorised fraud" and it is the ACCC' view that consumers involved in scams do not authorise a fraud. Using the term 'authorised' to describe a scam transaction suggests that a consumer who is deceived into a transaction has fully consented to the transaction or has knowledge that the transaction they are about to make is fraudulent, when that is not the case. Further, in many instances a consumer may authorise a particular action that leads to other 'unauthorised' actions. For example, a consumer may be tricked into authorising one payment to a scammer but not the subsequent payments made independently by the scammer using the consumer's credentials.

While banks may have information available to determine whether a payment was authorised by a customer, a telecommunications provider is not going to know whether a phone number reported is being used to convince someone to authorise a payment. Even a bank who investigations a 'hacking' of an account ('unauthorised fraud' in bank terms) will not always have information to make a conclusive decision that a scam had not preceded the hacking. If a victim provided information to a scammer which subsequently led to an account takeover on a digital platform that led to account access through a bank many months later, the Scams Code Framework should offer the same protections to the consumer. The initial scam may in fact be relevant to considering the role of an intermediary in another sector.

The proposed definition in the Consultation Paper requires 'intent' and would result in some activities that are considered scams falling outside the framework (for example, many threat based scams). We foresee that an unintended consequence of the proposed definition will be businesses devoting time and resources to verifying the intention of scammers, rather than taking quick action.

The ACCC suggests a more workable definition such as:

> ***'Scam' means any conduct which a reasonable person would believe was intended to deceive a person to obtain a benefit or cause a loss, financial or otherwise, by deception or other means.***

The ACCC recommends that the proposed definition be worded such that businesses are enabled to act (through disruption activity, information sharing, etc.) when they have reasonable grounds to suspect a scam, rather than needing to secure clear evidence of intent or verify a scam. The sector specific codes could then provide more clarity about how a sector identifies scams. For example, while the definition could be improved, the *Reducing Scam Calls and SMS Code* contains a definition of scam call and scam SMS as follows:

'*Scam Call' means any voice telephony call which has been generated for the purpose of dishonestly obtaining a benefit, or causing a loss, by deception or other means.*

'Scam SM' means any SM where:

> *a) the SM contains a link or a telephone number; and*

b) the purpose, or apparent purpose, of the SM is to mislead or deceive a recipient of the SM into using the link or telephone number; and

c) the recipient would be likely to suffer detriment as a result of using the link or telephone number.

Section 4.1 of the Scam Calls Code provides a list of characteristics to assist the industry to identify scam calls. This approach could also be followed in the banking and digital platforms codes.

The definition is going to be important for regulated business to determine in what circumstances it must take particular action including to disrupt or block a scam. When considered as preventative measure the definition should not require a business to investigate each and every customer transaction to understand the intent of the scammer noting this is highly complex for telecommunications providers who may only have call patterns to rely on. The definition needs to enable businesses to make quick and reasonable decisions about whether conduct appears to be a scam so that they can take swift action.

Further, it is important that any definition of 'scam' does not negate the nexus with state fraud offences. It is also important that the criminal characterisation of scams is recognised to prevent the trivialisation of scams which are often perpetration by organised crime.