



# Scams Prevention Framework

**ACCC Submission in Response to Treasury's Scams Prevention Framework – Exposure Draft**

4 October 2024

# Introduction

The Australian Competition and Consumer Commission (**ACCC**) welcomes the publication of the Exposure Draft of the Scams Prevention Framework Bill. The Exposure Draft proposes to insert a new Part IVF into the *Competition and Consumer Act 2010* (Cth) (the **Primary Legislation**), which establishes the Scams Prevention Framework (the **Framework**). We recognise the contributions across government, industry and consumer representatives to reach this important milestone.

We strongly support the introduction of mandatory industry codes to protect Australians from scams.<sup>1</sup> The ACCC considers consumer-focused, mandatory and enforceable codes are an essential component in making Australia a harder target for scammers.

The ACCC also supports the decision that the Australian Financial Complaints Authority (**AFCA**) will be the sole external dispute resolution body for scam-related complaints for the three initially designated sectors. This is in line with the 'no wrong door' approach that provides scam victims with a simple, single pathway to seek redress and recover. We appreciate that the Minister will have the power to designate additional external dispute resolution scheme bodies in the future. However, to maintain clear redress pathways for consumers and simplicity for regulated entities, we suggest that the threshold for doing so be high. Given the nature of scam complaints and importance of expeditious resolutions for victims, we note and support the Government's plans to ensure adequate resourcing for AFCA; this increase in funding will be critical to the scheme's success.

The ACCC will have a key role as the Scam Prevention Framework general regulator and will monitor compliance with and enforce the Scams Prevention Framework. This submission therefore focuses on opportunities to strengthen the legislation to protect Australians to the greatest extent possible. It also provides suggestions for greater clarity and certainty in implementation, for regulators and regulated entities designated under the Scams Prevention Framework.

The ACCC has not sought to address all of Treasury's questions set out in its 'Summary of reforms' document. Instead, we have focused our views and recommendations on those matters with most relevance to our role as the Scams Prevention Framework general regulator.

## 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 CCA, regulate national infrastructure and undertake market studies.

The ACCC runs the National Anti-Scam Centre; a virtual centre that sits within the ACCC and brings together experts from government, law enforcement and the private sector, to disrupt scams before they reach consumers. The National Anti-Scam Centre analyses and acts on trends from shared data and raises consumer awareness about how to spot and avoid scams.

The National Anti-Scam Centre commenced on 1 July 2023 and its work is underpinned by key priorities including prevention, identification and disruption, consumer education and

---

<sup>1</sup> As outlined in our February 2024 response to Treasury's consultation paper on the proposed mandatory Scams Code Framework, the ACCC has called for and strongly supports the introduction of consistent, mandatory and enforceable ecosystem wide obligations to reduce the harm scams cause for Australians. Our submission is available here: <https://treasury.gov.au/consultation/c2023-464732>

awareness and support (redress and recovery for victims). The National Anti-Scam Centre establishes new, dynamic partnerships between government and industry participants from the banking and finance, telecommunications and digital platforms sectors. The National Anti-Scam Centre facilitates partners sharing insights and opportunities to target scam activity and mitigate the harms to diverse and vulnerable communities. The ACCC is also building the technology infrastructure to support high-frequency, secure data sharing with a range of data sharing partners. This work will be critical in supporting and facilitating the information sharing requirements under the Scams Prevention Framework.

In the National Anti-Scam Centre's May 2024 Quarterly Update, it reported a decrease in scam losses across all its data sources, continuing the trend observed during the second half of 2023.<sup>2</sup> The increased collaboration led by the National Anti-Scam Centre is already having an impact on scam activity, but the Scams Prevention Framework will be critical to cutting off scammers before they can reach Australians and requiring significant uplift in the efforts of some sectors of industry to have the right measures in place to achieve this.

### **ACCC approach to consultation on the Scams Prevention Framework**

The ACCC, through the National Anti-Scam Centre, has regularly engaged with Treasury and other areas of government to progress the Scams Prevention Framework.

Throughout the consultation period, the ACCC attended numerous consumer representative group and industry stakeholder roundtables to understand matters of concern to those most likely to be included in the Framework.

The National Anti-Scam Centre also meets regularly with representatives from each of the first three proposed designated sectors on a bilateral basis and through the National Anti-Scam Centre's Advisory Board, Emerging Trends and Response Working Group, Data Integration and Technology Working Group, Communications and Awareness Working Group and our recent Investment Scam Fusion Cell.

The ACCC's engagement with Treasury on the Scams Prevention Framework has drawn on the ACCC and National Anti-Scam Centre's scam expertise, having been responsible for running the Scamwatch service for over 15 years and our broad enforcement and compliance experience.

### **Summary of this submission**

Key points the ACCC makes in this submission include:

1. **The definition of a 'scam'** – the ACCC sees opportunities to enhance the definition of a 'scam' to provide greater certainty for regulated entities about their obligations and to better protect Australians by capturing the full range of scam activity. In particular, we advocate for a definition incorporating objectivity<sup>3</sup> to promote appropriate, timely disruptive action in relation to actual scams and suspected scams. It is important that any definition does not require a conclusion as to whether activity that likely constitutes a scam is in fact a scam. Such a definition could both delay and limit the scope of action and response necessary to effectively combat scams.
2. **The operation of the Scams Prevention Framework**
  - **Regulatory Powers Act (Standard Provisions) Act 2014 (Cth) (the Regulatory Powers Act) and structure of Part IVF** – a straightforward mechanism enabling the ACCC and other Scams Prevention Framework regulators to use their existing investigation and enforcement tools under the Framework

---

<sup>2</sup> National Anti-Scam Centre in action – Quarterly update May 2024, p 3.

<sup>3</sup> Such as inserting an objective test as to whether conduct is likely to constitute a scam.

would promote more efficient regulation and be familiar to regulated entities. We acknowledge the *Regulatory Powers Act* provisions in the Primary Legislation may assist future Scams Prevention Framework regulators without existing appropriate investigation and enforcement tools. The Primary Legislation could include the Regulatory Powers Act provisions for future possible regulators but specifically allow the ACCC, the Australian Securities and Investments Commission (**ASIC**) and the Australian Communications and Media Authority (**ACMA**) to apply their existing legislation. This would also be simpler and provide greater certainty than waiting for the Minister to make a declaration on alternative powers.

- **Need for explicit requirements for regulated entities to take proactive scam detection and disruption steps** – the Exposure Draft and Explanatory Materials make clear the Government’s intention to impose an obligation on regulated entities to take positive, pre-emptive steps to reduce the volume of scams and prevent scammers engaging with Australians. The ACCC considers there are opportunities to clarify and strengthen civil penalty provisions in the Primary Legislation by clearly setting out specific steps regulated entities must take to meet their obligations under the Scams Prevention Framework.
  - **Need for clear and consistent technical data standards applied to entities sharing information under the Scams Prevention Framework** – the ACCC needs to be able to require regulated entities, or ACCC-approved third-party agents of regulated entities, to meet certain requirements for data sharing. This is to ensure effective information sharing which is critical to support industry and the National Anti-Scam Centre in its work to disrupt scams. The ACCC will include its expectations about how regulated entities will be required to share information with the National Anti-Scam Centre in the Notifiable Instruments provided for in the Primary Legislation. The ACCC considers that the time-period prescribed for reports under the Scams Code Framework could all be covered by the Notifiable Instruments, rather than in the Scams Prevention Framework Rules, so matters relating to reports are covered in the one instrument.
3. **Consistency across Sector Codes** – obligations on regulated entities must be consistent across sectors, and between Primary Legislation and Sector Codes, to ensure adequate protection of Australians irrespective of the scam type or contact method. The ACCC considers this could be achieved by ensuring that the detailed requirements set out in Sector Codes are consistent. Model provisions could be developed to be used in all Sector Codes, unless there a compelling reason as to why a model provision is not appropriate for a designated sector.
  4. The ACCC has also proposed sector-specific obligations for subordinate legislation to help guide industry, using the banking sector-specific code as an example.

## 1. The definition of a ‘scam’

A critical definition in the Scams Prevention Framework is the definition of ‘scam’, which sets out the scope of conduct to be regulated under the Framework. As expressed in our February 2024 submission, it is critical the definition of ‘scam’ be broad enough to cover the wide range of matters currently understood to be a scam and activity that may arise in future.

The Explanatory Materials make clear the policy intention is not to introduce a requirement for regulators (or other persons) to form a view as to the subjective mindset of a scammer.<sup>4</sup> As such, the ACCC recommends the definition of 'scam' be enhanced by explicitly inserting an element of objectivity. This would reduce uncertainty for regulated entities when determining whether certain activity detected on their service, or based on other information available to a regulated entity, is an activity of a type requiring prompt action. This would also avoid regulated entities devoting time and resources determining the precise nature of the scam activity before disrupting and responding to the activity. The ACCC foresees challenges enforcing the Framework if an objective element is not included in the definition of 'scam'.

Relatedly, the ACCC supports the position that detailed information about the scope of the definition should be dealt with in the Primary Legislation and not deferred to Sector Codes or the Scams Prevention Framework Rules. We consider it important that the obligations of regulated entities be as consistent as possible across different sectors. (We cover the need for consistency across Sector Codes in more detail at Part 3 of this submission).

The ACCC recommends that the definition be reworded so regulated entities are required to act (through disruption activity, information sharing etc.) where it would be reasonable to conclude that an attempt to engage a consumer of a regulated service is a scam, rather than needing to secure clear evidence of intent or to verify a scam.

### **Carve outs**

We note proposed section 58AG permits the Scams Prevention Framework Rules to carve out particular types of scams for the purpose of the Scams Prevention Framework. The ACCC supports the Government's intention for the definition of 'scam' in the Primary Legislation to be deliberately broad to capture the wide range of activities scammers engage in, and their ability to adapt or evolve behaviours over time.<sup>5</sup> We have a strong preference for the definition to remain broad, even if it may overlap with certain conduct in other provisions of the CCA,<sup>6</sup> rather than risking certain types of scam activity not being adequately covered. As such, the terms of any proposed carve outs will be critical, to avoid narrowing the Primary Legislation definition in a way that creates unintended gaps in the coverage of the Scams Prevention Framework.

## **2. Operation of the Scams Prevention Framework**

Guidance for both industry and consumers will be crucial to help people understand the operation and scope of the Scams Prevention Framework. Guidance will need to explain key elements including how the Framework interacts with other relevant pieces of legislation, when the Scams Prevention Framework Rules will be made and in force, information sharing arrangements and the ability of regulators to use their pre-existing enforcement powers.

The ACCC recognises that it will be a matter for Government to balance the need for clarity and certainty in the Primary Legislation itself, with the need for flexibility and adaptability of the Framework in expanding on the Primary Legislation obligations in Sector Codes and industry guidance. For example, as discussed further below, the definition of 'reasonable steps' may be open to significantly varying interpretations and would be clearer for all entities under the Framework if the definition was included in the Primary Legislation.

---

<sup>4</sup> The Explanatory Materials state 'the use of 'deceptive' and 'deceptively' do not create fault elements requiring the establishment of the state of mind of the scammer (para 1.65).

<sup>5</sup> Explanatory Materials paragraph 1.64.

<sup>6</sup> Sections 18 and 29 of the CCA.

We recognise the ACCC as Scams Prevention Framework general regulator will have a key role in developing this guidance. We will develop this guidance with sector regulators, and other relevant parts of government, and in consultation with industry. However, regulated entities will also need to develop accessible guidance for consumers on their new rights under the Framework, particularly in relation to internal dispute resolution processes.

### **Civil penalty provisions**

The civil penalty provisions contained in the Framework could be clarified and strengthened to better protect consumers. The mere requirement for a senior officer to certify at least annually that governance policies, procedures, metrics and targets for combatting scams are compliant does not provide adequate protection to Scams Prevention Framework consumers. This principle could be enhanced by including more affirmative measures for regulated entities such as having robust processes, monitoring trends through active data collection and other activities to prevent scams.

Similarly, in relation to the 'respond' principle, regulated entities that fail to make 'publicly accessible' information about the steps taken to protect consumers are liable for significant civil penalties. We recommend setting out more precise parameters as to what is required to be published and where it is required to be published. We understand the Explanatory Materials indicate a regulated entity may meet this obligation 'by creating a page on its website providing dynamic information about 'latest scams and alerts' to its consumers and the steps it has taken to manage the risk of that scam activity to its consumers'.

The legislation would benefit from being more prescriptive so regulated entities can better comply with this principle (and for the ACCC to effectively enforce the principle). We recognise this must be balanced against not requiring regulated entities to publish detailed information about their scam protection measures to avoid scammers identifying and exploiting this material. A specific carve out to exclude certain information that may assist scammers would help to address this issue.

### **Investigative and enforcement tools**

The operation of the Scams Prevention Framework could also be improved through introduction of specific provisions enabling designated regulators to access their own investigative and enforcement tools. Instead, regulators under the Framework, in the absence of a declaration that alternative powers apply, must rely on parts of the Regulatory Powers Act as the default power for monitoring and investigation. The Scams Prevention Framework also introduces specific regulatory tools that are already available in the CCA including infringement notices, injunctions and enforceable undertakings.

Given the ACCC is proposed to be the Scams Prevention Framework general regulator and uses its existing CCA regulatory tools, we consider it would be more efficient and effective to access those powers rather than rely on the Regulatory Powers Act provisions or the specific regulatory tools that have been introduced in the Exposure Draft. We anticipate the proposed hybrid approach would create some administrative burden and complexity (which in turn would hinder and slow our investigative and enforcement processes).

### **Effective information sharing across the scams eco-system**

The ACCC welcomes the developments the Scams Prevention Framework represents towards removing barriers to information sharing between Scams Prevention Framework regulators, regulated entities and other relevant entities and in turn avoiding duplicative efforts in combatting scams.

Efficient information sharing processes are essential under the multi-regulator model across the ecosystem (including between Scams Prevention Framework regulators and regulated

entities, entities in other sectors that are not designated under the Scams Prevention Framework, law enforcement agencies and other relevant government agencies) and will support action to disrupt scams. The Framework could be enhanced by including clear references to the *Privacy Act 1988* (Cth) (the **Privacy Act**). This would ensure that personal information could be disclosed under the Scams Prevention Framework to facilitate the protection of consumers from scams.

We also expect the ACCC, as the Scams Prevention Framework general regulator, will need to share personal information with regulated and other entities to enable them to disrupt a scam (or similar scams) and take action to minimise harm relating to the scam. We acknowledge the proposed power (in subsection 58BU(1)) for the ACCC to disclose information about a scam with a range of entities is quite broad. However, the ACCC is concerned that paragraph 58BU(3)(b) appears to limit the ACCC's ability to disrupt similar scamming actions. It may be necessary for the ACCC to be able to disclose personal information in such circumstances so that appropriate action can be taken in response to the scam activity.

Further, given scams may have an international dimension (for example, where the scammer is located overseas), it will be important for all Scams Prevention Framework regulators to be able to share information about scams (including personal information) with relevant overseas regulators and law enforcement entities. We also note that as the Bill is currently drafted, the ACCC will have the ability to share information with an unregulated entity, however it will not have the ability to compel an unregulated entity to take disruption action in response to the information shared.

### **Information asymmetries in relation to internal dispute resolution processes**

There is a potential information asymmetry risk for consumers when engaging with regulated entities in internal dispute resolution processes. For example, a regulated entity responding to a complaint from a consumer may provide limited or no detail about the steps the regulated entity has taken to investigate the consumer's complaint. A consumer could simply be told that the regulated entity has reviewed the matter and there is no further action required or refer the consumer to another entity (regulated or not) for assistance. In the absence of meaningful transparency from regulated entities in internal dispute resolution matters, consumers could turn to third parties to assist with money recovery. These third parties can offer consumers a legitimate service but there is considerable evidence that scammers also mimic money recovery services to re-engage victims.

A potential solution to this could be requiring, in Sector Codes, regulated entities to provide consumers with certain standard, accessible and intelligible information in response to an internal dispute resolution complaint. This would allow the consumer to consider their next steps, and whether external dispute resolution may be appropriate, in a suitably informed manner. If a consumer can determine that a regulated entity has taken meaningful steps to assist with their complaint, including engaging with the National Anti-Scam Centre to leverage actionable scam intelligence from across the ecosystem, this may avoid consumers commencing potentially unnecessary external dispute resolution proceedings.

### **Timing and scope**

The ACCC notes the Explanatory Materials state 'the commencement of the Scams Prevention Framework does not in itself impose an obligation on entities until a designation is made with respect to a regulated sector, and that instrument is in force'.<sup>7</sup> Regulated entities and Scams Prevention Sector Code regulators must be given certainty as to the implementation period (when regulated entities operating in the sector will be subject to a

---

<sup>7</sup> Paragraph 1.31 of the Explanatory Materials.

legal requirement to comply with the Scams Prevention Framework). We understand the Treasury is planning to consult on appropriate transition periods and we welcome the opportunity to contribute to that consultation process.

### 3. Consistency across Sector Codes

Consistency across Sector Codes and between the Primary Legislation and Sector Codes is crucial to adequately protecting consumers across all regulated sectors. We acknowledge the practical steps taken by regulated entities to comply with the 'detect', 'disrupt', 'respond' and 'report' principles will look different depending on the service(s) they offer. It is, however, important for the ACCC and Sector Code regulators to monitor compliance with and enforce obligations consistently across all regulated sectors.

#### **Delegations**

The ACCC is supportive of the delegation mechanism provided for in the Scams Prevention Framework, enabling the ACCC to delegate its section 155 document and information gathering powers to sector regulators to investigate and take enforcement action for breaches of Sector Codes. This was a key recommendation in our February 2024 submission, and an outcome which we expect will lead to significant efficiencies. As required by the Scams Prevention Framework, the ACCC is already considering how to support delegations through standing Memorandums of Understanding between ASIC and ACMA.

#### **Deferral of details to Scams Prevention Framework Sector Codes**

We note key obligations including the 'detect', 'disrupt', 'respond', and 'report' principles defer tailored, sector-specific details to Scams Prevention Framework Sector Codes. This is not the ACCC's preferred approach to the extent that it involves the deferral of details about 'reasonable steps'; 'relevant resources'; 'classes of Scams Prevention Framework consumers that have a higher risk of being targeted by a scam'; and the obligations that must be met in relation to an internal dispute mechanism for the sector. In particular, 'reasonable steps' may be open to significantly varying interpretations, and it is not clear how prescriptive Sector Codes will be.

The ACCC appreciates the Explanatory Materials do provide some guidance by, for example, setting out the kinds of actions 'taking reasonable steps' may include.<sup>8</sup> However, we consider the Scams Prevention Framework provisions would be strengthened through inserting more specific details into the Primary Legislation itself. The insertion of important elements set out in the Explanatory Materials in relation to 'reasonable steps' such as removal of content associated with scam activity, blocking phone numbers, accounts or content associated with scam activity and introducing holds to payments and confirmation of payee (for banking services) into the legislation (by way of non-exhaustive examples) would vastly assist regulated entities to comply.

The ACCC strongly supports more prescriptive provisions being set out in the Primary Legislation to ensure regulated entities clearly understand their obligations.

### 4. Sector-specific code obligations – banking sector example

Treasury has invited feedback on obligations that would be suitable for sector-specific codes. As outlined throughout this submission, the ACCC considers it is essential for Sector

---

<sup>8</sup> Paragraph 1.174 of the Explanatory Materials.



Codes to be consistent to adequately protect consumers irrespective of services or platforms they use.

By way of illustration, in this section we set out examples of the types of non-exhaustive obligations which may be incorporated into the banking Sector Code (and which should be adapted to suit the telecommunications, digital platforms and other future Sector Codes for consistency). The obligations outlined extend beyond those covered in the voluntary banking sector initiative, the Scam-Safe Accord. Whilst those initiatives contain important measures, more is needed.

### **Mandated implementation of anti-impersonation scam customer-specific keywords**

Crucially, regulated entities under the banking Sector Code must require customers to create a unique keyword which precedes all communications with their bank. We consider this would help combat both text and voice call scams targeting a mass number of consumers as each consumer has a unique keyword. We acknowledge customer experience considerations will also be important and may require, for example, the availability of prompts for customers (given the likelihood legitimate customers may forget their keyword).

### **Requiring customer confirmation before sending funds to suspicious accounts**

Banking customers must be required to confirm a transaction before funds are transferred to known suspicious accounts. Regulated entities should be required to take positive steps to obtain a customer's consent to transfer, and the transfer must not be processed without this approval.

### **Receiving banks must monitor incoming funds and freeze certain transactions**

Regulated entities under the banking sector-specific code who are the receiving institution in a transaction must monitor the source of funds, and whether incoming funds are suspicious for the recipient account. If a transaction is determined to be suspicious (i.e. where it would be reasonable to conclude that the attempt involves deception; and would, if successful, cause loss or harm including obtaining personal information of, or a benefit (such as a financial benefit) from, the Scams Prevention consumer or the Scam Prevention Framework consumer's associates under the Scams Prevention Framework), the regulated entity must freeze the funds for at least eight business hours, or until the Scams Prevention Framework consumer confirms the payment is legitimate.

Relatedly, consumers should be able to initiate a freeze on their account or a specific transaction if they hold concerns their account is compromised or there has been a suspicious transaction.

Banks must be required to provide an immediately accessible process for their customers to report losses (or potential losses) from a scam or account compromise. This should include a dedicated fraud-specific phone number (prioritised over general enquiries).

### **Identity verification including two-factor authentication processes should be improved**

The ACCC sees opportunities to significantly uplift current two-factor authentication processes. Regulated entities under the banking Sector Code should be required to provide the reason, including specific details where possible, for an authentication and block auto-population of a one-time code into a banking app. For example, information about who a new payee is ('add new payee John Smith') and details of the payment ('authorise transaction of \$10,000 to payee John Smith'). As raised earlier, a customer's unique keyword could also alternatively be used for two-factor authentication, requiring customers to actively engage in these steps.

**Anti-money muling obligations**

Regulated entities under a banking Sector Code must be required to compare the physical appearance of applicants with the identification documents provided when conducting a high-risk activity such as opening an account. Given the need to be mindful of any access needs for vulnerable groups when designing these measures, we suggest this can occur in-person or via sufficiently high-quality video, for example.

**Mandatory staff training and other anti-scam measures**

Regulated entities under a banking Sector Code must ensure any customer-facing staff members are sufficiently, regularly trained on the potential signs of a scam. Staff should be empowered to refuse to perform transactions they reasonably suspect are scam payments.

A mandatory sender ID registry is needed, ensuring all communications between a regulated entity and its customers must also use a consistent 'senderID' for text message communications and only use phone numbers clearly identified on their public facing websites, bank cards or in-mobile applications.