



Scams – Mandatory Industry Codes

Consultation paper

November 2023

© Commonwealth of Australia 2023

This publication is available for your use under a [Creative Commons Attribution 3.0 Australia](https://creativecommons.org/licenses/by/3.0/au/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, signatures and where otherwise stated. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.



Use of Treasury material under a [Creative Commons Attribution 3.0 Australia](https://creativecommons.org/licenses/by/3.0/au/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used ‘as supplied’.

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics — then Treasury prefers the following attribution:

Source: The Australian Government the Treasury.

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on The Australian Government the Treasury data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet website (see <https://www.pmc.gov.au/honours-and-symbols/commonwealth-coat-arms>).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

In the spirit of reconciliation, the Treasury acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Contents

- Consultation Process.....3**
- Request for feedback and comments3
- Proposed Scams Code Framework.....4**
- Introduction.....4
- Current approaches to addressing scams.....4
- Objectives and key principles6
- Key guiding principles6
- Key features of the proposed Scams Code Framework8
- Definitions9
- Principles-based obligations11
- Anti-scam strategy.....13
- Information sharing and reporting requirements.....14
- Consumer reports, complaints handling and dispute resolution.....15
- Sector-specific codes and standards.....17
- Approach to oversight, enforcement and non-compliance22
- Penalties for non-compliance.....23
- Appendix A – List of stakeholder questions.....24**
- Attachment A – International developments28**

Consultation Process

Request for feedback and comments

This consultation is being co-led by the Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA).

Interested stakeholders are invited to comment on the issues raised in this paper by 29 January 2024. Submissions may be lodged electronically or by post; however, electronic lodgement is preferred via the Australian Treasury website. For accessibility reasons, please submit responses in a Word, RTF or PDF format.

Submissions will be shared with other Commonwealth agencies where necessary for the purposes of progressing policy work on scams. All information (including name details) contained in submissions may be made publicly available on the Australian Treasury website unless you indicate that you would like all or part of your submission to remain in confidence. Automatically generated confidentiality statements in emails are not sufficient for this purpose.

If you would like only part of your submission to remain confidential, please provide this information clearly marked as such in a separate attachment. Legal requirements, such as those imposed by the *Freedom of Information Act 1982*, may affect the confidentiality of your submission.

Closing date for submissions: 29 January 2024

Mail	Scams Taskforce Market Conduct and Digital Division The Treasury Langton Crescent PARKES ACT 2600
-------------	---

Enquiries Enquiries can be initially directed to scampolicy@treasury.gov.au.

The reforms outlined in this paper have not received Government approval and are not yet law. As a consequence, this paper is merely a guide as to how reforms might operate.

Proposed Scams Code Framework

Introduction

Scams are a growing threat to Australian consumers and businesses, with financial losses to scams of at least \$3.1 billion in 2022 (an 80 per cent increase on losses recorded in 2021).¹ In 2022, 65 per cent of Australians were exposed to a scam attempt.²

Scammers are becoming more technologically advanced and coordinated, enabling them to evolve and find new vulnerabilities to target, new ways to deceive consumers, and new methods to avoid detection.

Current anti-scam measures vary across the ecosystem of sectors and businesses that are targeted by scammers (scams ecosystem). While some sectors (like telecommunications) have industry codes to reduce scams, other sectors in the scams ecosystem have no specific, enforceable anti-scam requirements.

While many businesses have been responding to the increasing threat of scams to Australian consumers, the Government remains concerned that these efforts are often siloed within particular businesses or sectors, or that take-up of broader measures has been irregular across each sector.

There is currently no overarching regulatory framework that sets clear roles and responsibilities for the Government, regulators, and the private sector in addressing scams. The Government has committed to introducing new mandatory industry codes to outline the responsibilities of the private sector in relation to scam activity, with a focus on banks, telecommunications providers and digital platforms.

On 30 November 2023, the Assistant Treasurer, the Hon Stephen Jones MP, and the Minister for Communications, the Hon Michelle Rowland MP, announced consultation on a proposed Scams Code Framework ('the Framework') to deliver the Government's commitment.

This consultation paper has been informed by initial targeted consultations with regulators, industry representatives, consumer groups and people impacted by scams. The paper invites stakeholders to provide feedback on the proposed features of the Framework to inform Government decisions.

Current approaches to addressing scams

The Government has recently introduced several initiatives targeted at reducing scam activity and its impacts, including:

- the establishment of the National Anti-Scam Centre (NASC) led by the Australian Competition and Consumer Commission (ACCC) on 1 July 2023, which is an initiative to coordinate efforts to prevent scams by improving intelligence sharing across Government and the private sector and raising public awareness about scams
- work by the Australian Securities and Investments Commission (ASIC) to identify and take down investment scam websites, which has already taken down 2,500 websites since July 2023³

¹ ACCC (2023), [Targeting scams: report of the ACCC on scams activity](#), ACCC, accessed 21 November 2023.

² Australian Bureau of Statistics (ABS) (22 February 2023), [13.2 million Australians exposed to scams](#), [media release], ABS, accessed 2 November 2023.

³ ASIC (2 November 2023), [ASIC's new website takedown capability knocks out over 2,500 investment scam and phishing websites](#), [media release], ABS, accessed 2 November 2023.

- work underway by the Australian Communications and Media Authority (ACMA) to establish Australia’s first SMS sender ID registry, to help prevent scammers imitating trusted industry or Government brand names – such as ATO or myGov – in text message headers
- funding of specialist support services for victims of identity theft.

Currently, telecommunications providers are the only sector specifically regulated in relation to scams. Telecommunications providers are subject to the *Reducing Scam Calls and Scam Short Messages (SMS) Code*, an industry-developed code registered and enforced by the ACMA, which requires telecommunications providers to take reasonable steps to prevent and block scam calls and text messages. Telecommunications providers are also subject to other anti-scam rules made by the ACMA requiring use of multifactor identity verification to protect services from scammer compromise and fraud.

Telecommunications providers have reported that approximately 1.4 billion scam calls and 257 million scam SMS have been blocked under the code to 30 June 2023.⁴ Consumer reports of scam calls have also decreased by 56 per cent from 2021 to 2022.⁵ However, in 2022, scam calls resulted in the highest reported losses to Scamwatch (increasing by 40.6 per cent to \$141 million from 2021), demonstrating that scams are becoming more sophisticated and opportunities remain for the sector to enhance disruption.⁶

While regulators like the ACCC, the Office of the Australian Information Commissioner (OAIC) and ASIC can take some action to protect consumers⁷ from the impact of scams through their role as consumer protection, privacy and financial system regulators, there are no specific requirements on banks and digital platforms to address scams.⁸ Recent reviews have identified gaps in the banking and digital platforms sectors’ approaches to prevent and disrupt scams, and support consumers who have been scammed.

- In its September 2022 Digital Platform Services Inquiry (DPSI) interim report, the ACCC identified that digital platforms do not take sufficient and consistent steps to protect consumers from online harms, such as scams. The ACCC recommended that the Government introduce targeted measures mandating that digital platforms prevent and remove scams from their services, including by providing a notice-and-action mechanism, verifying the identity and legitimacy of certain users and advertisements, and publicly reporting on scam mitigation efforts.⁹
- In 2023, ASIC found the overall approach to scams strategies and governance in Australia’s major banks was variable and less mature than expected, with gaps and inconsistencies in scam detection, response, and victim support.¹⁰

⁴ ACMA (n.d), [Action on scams, spam and telemarketing: April to June 2023](#), ACMA website, accessed 2 November 2023.

⁵ ACCC (2023), [Targeting scams: report of the ACCC on scams activity](#), ACCC, accessed 2 November 2023.

⁶ Ibid.

⁷ For the purposes of this paper, a consumer refers to a customer or user of a service or platform that is offered by a regulated business subject to the Framework (i.e. banking, or telecommunications service or digital platform). This could include individuals or businesses.

⁸ While banks have an AML/CTF requirement which includes having systems and controls in place to report suspicious matters, which includes scams, this does not set out broad obligations or requirements in relation to preventing, detecting and responding to scams.

⁹ ACCC (2022), [Digital Platform Services Inquiry Interim Report No. 5- Regulatory reform](#), ACCC, accessed 2 November 2023.

¹⁰ ASIC (2023), [Scam prevention, detection and response by the four major banks](#), ASIC, accessed 2 November 2023.

On 24 November 2023, the Australian Banking Association Ltd (ABA) launched an industry-led ‘Scam-Safe Accord’ that outlines the anti-scam measures that will be implemented across the banking sector to disrupt, detect and respond to scams.¹¹ Measures include a new confirmation of payee system, warnings and delays to protect customers, expansion of intelligence sharing across the sector, and limiting payments to high-risk exit channels, among other initiatives.

While existing Government and industry initiatives will have an impact on scam activity, the Government considers that more needs to be done to consistently uplift practices within key sectors in the ecosystem – banks, telecommunications providers and digital platforms – and reduce opportunities for scammers to exploit gaps and weaknesses within and across sectors to steal from and harm consumers.

Objectives and key principles

The primary objective of the Framework is to set clear roles and responsibilities for the Government, regulators, and the private sector in combatting scams. This includes ensuring that key sectors in the scams ecosystem have measures in place to prevent, detect, disrupt, and respond to scams, including sharing scam intelligence across and between sectors.

Where a business does not meet its obligations under the Framework, where applicable, Internal and/or External Dispute Resolution mechanisms would ensure consumers have access to appropriate redress, and regulators would be given new enforcement and penalty powers.

The Framework and other scams-related activity (such as through the NASC) will not eradicate all scams. However, the intended outcome is to make Australia a harder target for scam activity, and less attractive to scammers, therefore reducing scam losses and impacts.

Key guiding principles

The proposed Framework is underpinned by three key principles, addressing the gaps in the current approach.

Principle 1: A whole-of-ecosystem approach to address scams

Scammers exploit loopholes – inaction from a sector or parts of a sector in the scams ecosystem risks scammers exploiting that gap, contacting potential victims, and increasing the risk of more Australians losing money to a scam.

Every business in the scams ecosystem has a role to play in combatting scams. Therefore, a strong, whole-of-ecosystem regulatory framework is needed to ensure that those best placed in the system deal with the scams threat. This requires a coordinated effort between Government, regulators, and the private sector to:

- prevent scammers from contacting consumers through key communications channels provided by telecommunications providers (disrupting scam calls and SMS) and digital platforms (blocking and removing scam content, communications and advertisements)
- educate consumers to recognise and report scams to the relevant business or Scamwatch
- prevent and take timely steps to recover payments made to scammers such as through bank transfers where possible

¹¹ <https://www.ausbanking.org.au/new-scam-safe-accord/>.

- provide clear pathways of support and complaints handling for those who have been affected by scams
- strengthening links between cyber and identity resilience to prevent scams

A whole-of-ecosystem approach will lift the bar for businesses in key sectors to take a consistently proactive approach to stopping scams.

Principle 2: The Framework must be flexible and responsive

Scammers quickly adapt and are likely to shift their focus and activity to less regulated parts of the scams ecosystem. Scammers are also likely to target developments in technologies and markets to create new types of scams and harms. The Framework will need to be flexible and responsive to future changes in the scams ecosystem.

Principle 3: The Framework will complement and leverage existing interrelated regimes, systems and initiatives

While there is currently no specific, ecosystem-wide regulatory framework on combatting scams, there are numerous interrelated frameworks and reforms that will have an impact on scam activity. The Framework will complement and leverage these existing interrelated regulatory regimes and reform processes, to reduce overlap and regulatory burden on industry. This includes but is not limited to:

- work being progressed on the Australian Cyber Security Strategy 2023-2030
- the National Strategy for Identity Resilience released in June 2023 and associated initiatives being progressed
- reforms to Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF)
- reforms to the Government's digital identity accreditation framework
- reforms to strengthen Australia's privacy framework, to guard against identity fraud, scams and the risk to businesses of failing to manage personal information appropriately¹²
- the existing Australian Code of Practice on misinformation and disinformation, and proposed legislation to give ACMA powers to enforce industry codes addressing misinformation and disinformation
- the ACCC's ongoing work and reporting as part of the Digital Platforms Services Inquiry, and related ongoing work across portfolios.

Information from stakeholders on other intersecting frameworks, reviews or reforms that may have a role in their efforts to combat scams, and which should be considered in policy development, are welcome.

Beyond existing Government initiatives, the Framework will also consider the voluntary work being progressed by different parts of industry to address scams, such as the anti-scam initiatives being delivered by the banking sector. The Government may consider lifting effective voluntary scams initiatives into legislation by establishing them as either ecosystem-wide obligations or sector-specific obligations within the Framework, where appropriate.

¹² [Government Response to the Privacy Act Review](#).

Key features of the proposed Scams Code Framework

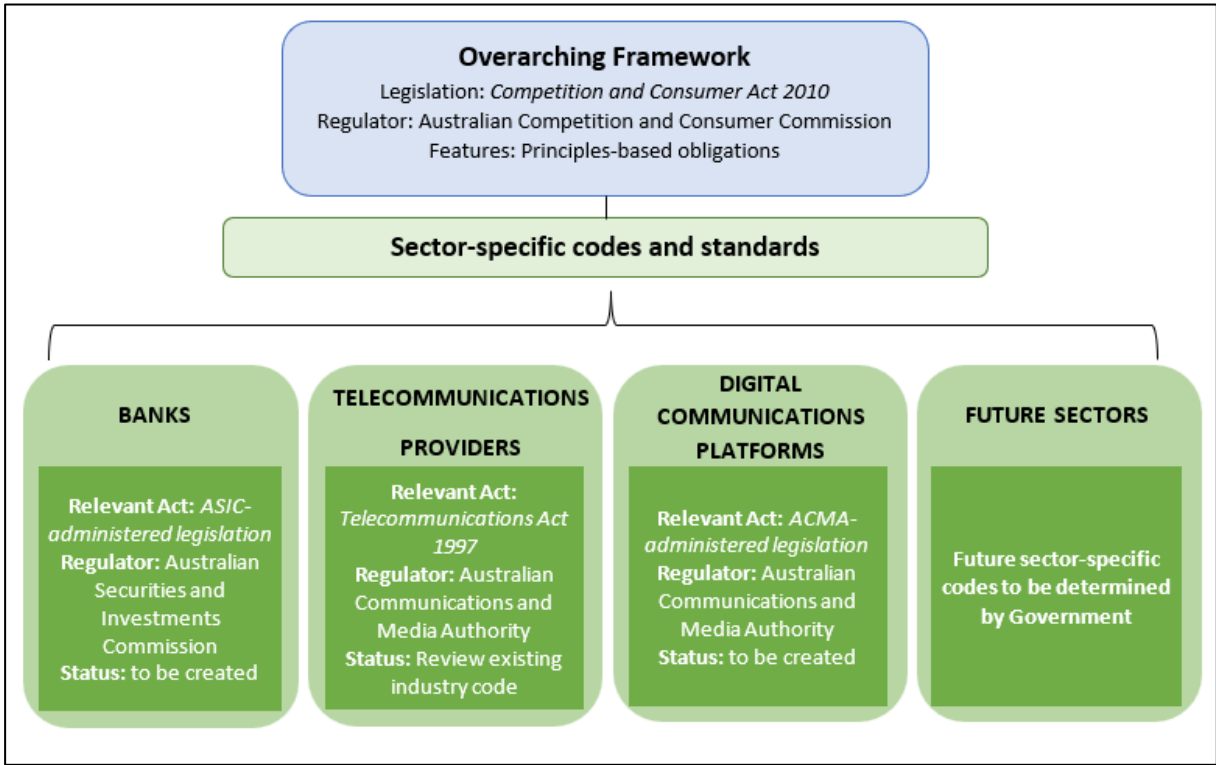
The implementation of the Framework is subject to future Government decisions, and legislative design and development. References to amending existing legal frameworks are demonstrative of policy intent only. The focus of this paper is to seek feedback on the proposed key features and obligations that would form part of the Framework.

The Framework would be established by introducing a new overarching regime in primary law – for example, in the *Competition and Consumer Act 2010 (CCA)*. The CCA would set mandatory obligations for businesses in designated sectors within the scams ecosystem to take action to address scams delivered over their services. Mechanisms would also be established under sector-specific legislation, enabling Government or regulators to develop codes and standards for designated sectors that put additional, tailored obligations on businesses to prevent, detect, disrupt and respond to scams.

The initial sectors covered by the Framework would be those most targeted by scammers – banks, telecommunications providers and digital communications platforms – with scope for further sectors to be designated in future by the relevant Minister. These could include the superannuation sector, digital currency exchanges (cryptocurrency), other payment providers, and transaction-based digital platforms like online marketplaces.

Figure 1 sets out the proposed key features of the Framework, which are discussed in further detail below. It does not include legislation that could be potentially impacted through consequential amendments.

Figure 1. Proposed Scams Code Framework



Questions on the proposed Framework:

1. Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?
2. Is the structure of the Framework workable – can it be implemented in an efficient manner? Are there other options for how a Framework could be structured that would provide a more efficient outcome?
3. Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?
4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?
5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?
6. What future sectors should be designated and brought under the Framework?
7. What impacts should the Government consider in deciding a final structure of the Framework?

Definitions

It is intended that the primary law would include a definition of scams, and the initial sectors designated within the Framework. Where possible, it is intended that definitions under the Framework would leverage existing definitions in other legislation. This paper seeks views from stakeholders on formalising a definition of a ‘scam’ under the Framework and views on a proposed definition.

The Government’s proposed definition of each sector would determine the scope of the Framework and the initial set of businesses that would be required to comply with obligations. This paper seeks views on the types of businesses that would be captured and their ability to meet the proposed obligations for their sector, and any unintended consequences that might occur as a result of the proposed definitions.

Definition of a scam

Including a definition of ‘scam’ in the primary law will help set a clear and consistent scope for the type of harms that businesses regulated under the Framework are expected to address on their services. The definition is not intended to replace or supersede the scope of anti-scam functions set out under other legislation or Government initiatives.

There is currently no agreed formal definition of a scam in Australian legislation. Currently, regulators generally address scams as a category of fraud. It is proposed that the definition of a ‘scam’ under the Framework would be consistent with the definition of fraud as defined under the Commonwealth Fraud Control Policy, which aligns with the definition under the *Criminal Code Act 1995* (Cth). Sector-specific codes could provide further guidance on the meaning of ‘scams’ based on specific fraudulent practices observed in each sector e.g., the definition of a scam call under the telecommunications scams code.

Proposed definition of a scam under the Framework:

A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information¹³ or a financial benefit by deceptive means.

The proposed definition intends to strike a balance between certainty for regulated businesses and ensure enough flexibility to capture new and emerging categories of scams over time. The definition is

¹³ ‘Personal information’ is defined under the *Privacy Act 1988*. It is relevant to a definition of scams as some scams do not create immediate financial harms. For instance, phishing scams that compromise a person’s personal and financial information can later lead to identity theft, or re-victimisation by other scammers.

intended to cover the types of scams identified by the ACCC under its *Targeting Scams* report, including, but not limited to, common scam types such as investment scams, romance scams, phishing scams, employment scams, and remote access scams.¹⁴

Scams are related to, but distinguished from, other types of fraud. The proposed definition is not intended to capture unauthorised fraud, such as cybercrimes that may use hacking, data breaches, and identity theft, that do not involve the deception of a consumer into ‘authorising’ the fraud.

The definition is also not intended to include consumer disputes about misleading and deceptive practices relating to the sale of goods and services, other than where a seller profile or website is not legitimate.

Definition of a Digital Communications Platform

It is intended that the Framework would apply to digital communications platforms.

Online scam content can take many forms across a range of services, including, but not limited to, messaging and comments between users; advertisements and third-party links; endorsements for scam products or services across a range of media; and emails. For the purposes of the Framework, ‘digital communications platforms’ covers all digital platforms that provide communications or media-type services that can be exploited to share this material, including:

- *content aggregation services* – online services whose primary function is to collate and present content to end-users from a range of online sources
- *connective media services* – online services whose primary function is to enable interaction between two or more end-users
- *media sharing services* – online services whose primary function is to provide audio, audio-visual or moving visual content, including advertising content, to end-users.

These services are used by scammers as a primary origin and contact method of investment scams, which resulted in \$377 million in losses in 2022. Additionally, despite being reported as a contact method in 6 per cent of consumer reports to the ACCC, \$80 million in losses to scams were attributed to social media alone, higher than all other contact methods excluding phone calls.¹⁵

This definition is not intended to cover digital currency exchanges (cryptocurrency), and transaction-based digital platforms like online marketplaces. The Framework could be expanded to cover these and other types of digital platforms in the future.

Definition of a Bank

It is intended that the Framework would apply to a body corporate that is an Authorised Deposit-Taking Institution (ADI) under section 9 of the *Banking Act 1959*. Adopting this definition would mean that the scope of the Framework would extend to small and large banks, building societies, credit unions, and restricted ADIs.¹⁶

¹⁴ ACCC (2023), [Targeting scams: report of the ACCC on scams activity](#), ACCC, accessed 2 November 2023.

¹⁵ ACCC (2023), [Targeting scams: report of the ACCC on scams activity](#), ACCC, accessed 2 November 2023.

¹⁶ The regulatory obligations for PPFs are subject to ongoing consultation as part of the payments reforms. See [Licensing of payment service providers – payment functions](#).

Definition of a Telecommunications Provider

For the purposes of the Framework, telecommunications providers are defined as Carriers and Carriage Service Providers as per the *Telecommunications Act 1997* (Telecommunications Act).

Questions on definitions:

8. Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any unintended consequences of this approach that the Government should consider?
9. Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?
10. Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?
11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?
12. Will the proposed definitions for designated sectors result in any unintended consequences for businesses that could not, or should not, be required to meet the obligations set out within the Framework and sector-specific codes?
13. Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?
14. What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?

Principles-based obligations

It is intended that the CCA would set out clear and enforceable principles-based obligations. These obligations would require all businesses subject to the Framework to take a consistently proactive approach to combatting scams, irrespective of the sector in which they operate. The principles-based obligations would be flexible enough to account for the differing nature and sizes of regulated businesses. This would allow businesses to adjust their anti-scam efforts to the conditions of their sector, service offering or business model, and any changes in scam activity on their services.

Proposed ecosystem-wide obligations in the CCA

Prevention

- A business must develop, maintain, and implement an anti-scam strategy that sets out the business' approach to scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem.
- A business must take all reasonable steps to prevent misuse of its services by scammers, so that an undue burden is not placed on consumers or other market participants to prevent scams.
- A business must implement anti-scam systems that are responsive to new products, services, designs, technologies, and delivery channels.
- A business must provide their consumers or users with information about how to identify and minimise the risk of being scammed.
- A business must train staff to identify and respond to scams.

Detection and disruption

- A business must seek to detect, block and prevent scams from initiating contact with consumers.
- A business must seek to verify and trace scams where scam intelligence has been received.
- A business must act in a timely manner on scam intelligence received through information sharing, consumer reports, complaints and other means.
- Where a business receives intelligence that a consumer is or may be a target of a scam, the business must take steps to disclose this to the consumer in a timely manner to minimise the risk of consumer harm or loss.
- A business must provide their consumers or users with tools to verify information in real time.

Response (obligations with respect to consumers)

- Where a consumer has identified they have been affected by a scam, businesses must take all reasonable steps to prevent further loss to the consumer and treat consumers fairly and consistently.
- A business must have user-friendly, effective, efficient, transparent, and accessible options for consumers or users to report a scam, including people not directly targeted by a scam.
- A business must have user-friendly, effective, transparent, and accessible complaints handling processes for consumers or users to make a complaint about how a scam report was handled or in relation to a business's response to scam activity (including steps taken to prevent, detect, disrupt and respond to scam activity).
- Where a consumer escalates concerns with a business, they should be dealt with fairly and promptly, and consumers should be given access to information about dispute resolution options where applicable.

Reporting (obligations to regulators and other businesses)

- A business must take reasonable steps to notify other businesses, the NASC and relevant regulators promptly of intelligence about suspected or identified organised large-scale scam activity as well as rapidly emerging or cross-sectoral scam activity.
- A business must share data and information on the incidence of scams, and action taken in response, with designated industry bodies, law enforcement and regulators, and the NASC.
- A business must keep records of incidences of scams, and the action taken in response.

- A business must respond to an information request from the ACCC within the timeframe specified.

Questions on overarching principles-based obligations:

15. Are there additional overarching obligations the Government should consider for the Framework?
16. Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?
17. Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?
18. Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?
19. What changes could businesses be expected to make to meet these obligations, and what would be the estimated regulatory cost associated with these changes?

Anti-scam strategy

Businesses regulated under the proposed Framework would be required to develop, maintain, and implement an anti-scam strategy. The strategy would need to set out the business' approach to scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem. It is proposed that anti-scams strategies have a high-level of sign-off within the business, such as the board or similar level of governance. It is expected that this will ensure a high-level of priority and oversight within the regulated business. Businesses would be required to regularly review the effectiveness of the strategy against the risk assessment, as well as monitor and report on ongoing compliance. This should include regular reporting to senior levels of the business to ensure that the strategy is effective and being adhered to.

Publication of the anti-scam strategy would not be required. Businesses would be open to determine the level of detail on their anti-scam strategy that could be made available to the public, such as on the business's website. This would ensure that businesses are not required to disclose operational or technical detail that may be sensitive or useful to scammers. However, publication of anti-scam measures would help build industry and consumer confidence and demonstrate to the public that business practices are compliant with the Framework.

A business' anti-scam strategy would be subject to review by the ACCC. Under the Framework, the ACCC could play a role in working with businesses on their anti-scam strategies to ensure they are fit-for-purpose and consistent with similar businesses in their sector.

Questions on anti-scams strategy obligation:

20. What additional resources would be required for establishing and maintaining an anti-scam strategy?
21. Are there any other processes or reporting requirements the Government should consider?
22. Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?
23. How often should businesses be required to review their anti-scam strategies and should this be legislated?
24. Are there any reasons why the anti-scams strategy should not be signed off by the highest level of governance within a business? If not, what level would be appropriate?
25. What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?

Information sharing and reporting requirements

Current information sharing arrangements

Existing voluntary information sharing arrangements between businesses are often ad hoc and do not extend between all sectors in the scams ecosystem.

Businesses and consumers are encouraged to report scams on the Scamwatch website, managed by the NASC, to assist with coordinated information-sharing and action to combat scams. Information in the reports is used by the NASC to monitor scam trends and act where appropriate, including educating the public on new or emerging scams. The information is shared as needed with businesses, including from the telecommunications, digital communication platforms and banking sector, other government organisations and law enforcement, to prevent and disrupt scams.

The NASC is also building its data-sharing capability to enhance scams information sharing across the ecosystem. This will result in improved quality, timeliness and coverage over the next three years. This includes a technology build which will enable the NASC to:

- receive a report of a scam from any institution (private or Government) and centralise this intelligence
- distribute data to those who need it most – such as banks to freeze an account, telcos to block a call, and digital communication platforms to take down scam content or an account
- analyse and act on the trends sourced from this data to disrupt scams and educate Australians.

The NASC also shares information with the Australian Financial Crimes Exchange (AFCX). The AFCX is an independent, not-for-profit entity formed to assist businesses to coordinate intelligence and data-sharing activities to address financial crime and cybercrime. The NASC is working with the AFCX and other key businesses in the scams ecosystem to better coordinate the sharing scam information and intelligence.

Banks who are members of the AFCX can upload information and data on fraud to the AFCX exchange. They can also access a secure information sharing web portal co-ordinate actions to identify, analyse, prevent and action financial crime, scams and online fraud. In 2021, the AFCX entered a memorandum of understanding with the ACMA to exchange information, including data on cases and numbers associated with SMS fraud.

Under their industry code, telecommunications providers are required to share information on scam calls and SMS with other telecommunications providers and the ACMA. The ACMA also provides de-identified consumer complaint data to telecommunications provider to assist their identification and disruption of scams.

Information sharing under the Framework

Businesses regulated under the Framework would be required to share and act on information, to ensure that all businesses within the scams ecosystem have quality information to enable them to detect and prevent scams.

Businesses would be required to notify other businesses, where practicable, and the NASC, promptly of intelligence about suspected or identified organised large-scale scam activity (due to size or frequency), as well as rapidly emerging or cross-sectoral scam activity where there is a significant risk for consumers. This information would assist the NASC in monitoring scam trends, disrupting scams - including through its cross-sector 'fusion cells' - and informing rapid deployment of consumer

awareness campaigns. The information would also assist other businesses in the ecosystem, including their scam detection and response tools.

Given the potentially large volume of scams reports and incidences collected by each regulated business, there is unlikely to be a net benefit of sharing every individual scam instance across the ecosystem. However, under the Framework, the NASC or other relevant regulators would be able to request that data on individual scam instances or reports, and actions taken in response, be shared.

A business would also be required to take reasonable steps to act on scam intelligence shared with it by another business, industry bodies, law enforcement and regulators, including the NASC. This would include acting on intelligence to stop a current scam, prevent further scams from the same source occurring, or to otherwise address the consequences of a scam. Reasonable steps might include to promptly remove scam content or an identified scam account from a service, warning consumers or users that have also interacted with an identified scam or scammer and providing them with information or advice on actions to take if they have also been affected by a scam, or blocking an identified scam user from signing up to the service, to prevent further scams from occurring.

Questions on information sharing requirements:

26. What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?
27. What safeguards and/or limitations (regulatory, technical, logistical or administrative) should the Government consider regarding the sharing of information between businesses, the NASC or sector-specific regulators?
28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?
29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

Consumer reports, complaints handling and dispute resolution

The Framework would require regulated businesses to strengthen protections against scams through receiving consumer scam reports, complaints handling, and internal and external dispute resolution.

A business would be required to have a reporting mechanism in place for users to report scams, including in cases where they have identified but not been affected by a scam. This will allow users to notify the business of scam activity for investigation.

A business would also be required to have in place an Internal Dispute Resolution (IDR) process capable of addressing concerns or complaints by consumers or users in relation to a business's response to a specific report of a scam or scam activity in their services more generally. Where matters cannot be resolved through a business's IDR process, a consumer or user of that business would be able to access an External Dispute Resolution (EDR) process to resolve the complaint. This is intended to ensure that when a business has not met its obligations under the Framework, either the business or an EDR process can consider whether the consumer should be compensated for any losses they have incurred to a scammer.

Industry-specific IDR and EDR arrangements are currently in place for financial firms (including banks) and for telecommunications providers. There are no existing industry-specific IDR and EDR arrangements for digital communications platforms – IDR is managed separately by individual businesses, and EDR is currently handled through state and territory fair trading bodies and the courts, or through regulators and Ombuds schemes in some instances.

Under the Framework, there would be clear redress pathways for consumers. This would include consideration of leveraging existing IDR requirements and EDR schemes (such as the Australian

Financial Complaints Authority for banks and the Telecommunications Industry Ombudsman for telecommunications providers). IDR and EDR requirements for digital communications platforms in relation to scams will be informed by further work arising from the Government's Response to the ACCC's September 2022 DPSI interim report. This report recommended that the Government introduce mandatory IDR standards and ensure that users of digital platforms have access to an ombudsman scheme.

It is important that IDR and EDR operates coherently across the system, particularly for cases where businesses in multiple sectors have not met their obligations under the Framework, so that consumers are not referred back and forth between businesses and different EDR schemes.

Existing EDR bodies - Scope of action and limitations including redress options available to consumers

Australian Financial Complaints Authority (AFCA) – Banks

- Firms that provide financial and credit services to consumers must be members of AFCA and fund the body.
- AFCA handles complaints in accordance with its Rules (which forms part of a binding contract between AFCA, the member firm and the complainant). This includes complaints arising from a breach of legal requirements, the Privacy Act or Consumer Data Framework, that cannot be resolved through IDR.
- AFCA can also consider breaches of industry and voluntary codes, such as the ePayments Code that deals with mistaken and unauthorised payments (but which does not cover the vast majority of scam payments where the consumer has 'authorised' the payment).
- AFCA can determine that compensation be paid by financial firms to consumers for any direct loss or damage caused by a firm's breach of obligation owed to the consumer when providing a financial or credit product or service. This excludes an award for punitive or exemplary damages.
- AFCA can help with claims for direct financial loss – currently up to a \$542,500 cap per claim¹⁷ and also award compensation for non-financial loss (subject to monetary caps), for example if there is an unusual degree or extent of physical inconvenience, time taken to resolve the situation or interference with the complainant's expectation of enjoyment or peace of mind.
- AFCA can help with other non-monetary orders and remedies such as: releasing consumers from a contract, varying the terms of a contract etc.
- AFCA can consider what is fair in all the circumstances, including the conduct of the financial firm in processing the scam transaction. It cannot consider the scammers actions or the actions of other businesses (e.g. the receiving bank, telecommunications providers, platforms) that may play a role in the scam occurring.

Telecommunications Industry Ombudsman (TIO) – Telecommunications providers

- Telecommunications service providers are required to be members, to comply with and fund the dispute resolution scheme operated by the TIO.
- The TIO can help a consumer or small business with a complaint about service providers' compliance with current obligations included in legislation or industry codes registered with the ACMA, or industry

¹⁷ These limits are adjusted every three years and communicated by AFCA to stakeholders when they change.

standards made by the ACMA e.g. connection delays beyond the expected timeframes, network faults, breaches of privacy, etc.

- The TIO can use means such as referral, conciliation, investigation and determination to resolve a complaint.
- The TIO has MOUs with ACMA and ACCC to support telecommunications provider compliance with their scheme and facilitate information sharing about systemic issues and complaint trends.
- The TIO helps with consumer or business compensation for financial costs that are binding to telecommunications providers for amounts up to \$100,000 and up to \$1500 for non-financial losses.
- The TIO does not deal with complaints about fraudsters or scammers and their behaviour.

Questions on consumer reports, complaints handling and dispute resolution:

30. What are the limitations or gaps that need to be considered in leveraging existing IDR requirements and EDR schemes for the purposes of this Framework?
31. If the remit for existing EDR schemes is expanded for complaints in relation to this Framework:
 - a) what criteria should be considered in relation to apportioning responsibility across businesses in different sectors?
 - b) how should the different EDR schemes operate to ensure consumers are not referred back and forth?
 - c) what impacts would this have on your business or sector?
32. Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? Should these be equal across all sectors and how should they be set?
33. Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?

Sector-specific codes and standards

In addition to the principles-based obligations in primary law (discussed earlier in the paper), the Framework would also include mandatory sector-specific codes and standards, setting out further obligations tailored to each sector. Sector-specific codes and standards would initially apply to the banking, telecommunications and digital communications platforms sectors, with scope to expand to other designated sectors and/or subsectors in future. The Framework would leverage the existing arrangements for telecommunications providers and ensure consistency of obligations across all targeted sectors. The examples of obligations included in this paper are presented with the intention to gather preliminary feedback from industry on the obligations that could form part of the sector-specific codes. Further detail will be worked through via ongoing engagement and consultation with industry to finalise obligations.

Telecommunications Providers

The proposed Framework would acknowledge the existing powers under the Telecommunications Act, for the ACMA to establish codes and standards for telecommunications providers with regard to scams. Under these existing arrangements, telecommunications providers are subject to the *Reducing Scam Calls and Scam SMSs* industry code, which is an industry-developed code, registered with and

enforced by the ACMA, and other instruments requiring use of multi-factor ID to protect telecommunications services from scams.

To remain consistent with the overarching scams obligations, the telecommunications industry body, Communications Alliance, would be asked to review this code in 2024 and consider what changes are required to improve the operation of the Code and ensure consistency with the Framework. If changes are required, Communications Alliance would need to update the code and the ACMA would consider it for re-registration. The ACMA can also use its powers, if required, to make industry standards or service provider determinations to meet Government and community expectations.

Examples of current obligations in the Reducing Scam Calls and Scam Short Messages (SMs) code

Prevention and detection

- Make available on their website up-to-date guidance materials on the type of scams calls and SMs that consumer may be exposed to, information about how to block suspicious calls or SMs and what to do if they receive these including how to report to Scamwatch.
- Originating telecommunications providers must verify a call /SMs originator has the right to use a number or alphanumeric Sender ID, to prevent unauthorised spoofing.
- Must monitor their network for scam calls/SMs based on characteristics identified in the code and have systems in place to trace the origin of suspected scams calls/SMs.

Disruption and response

- Investigate and take action to stop unauthorised spoofing once it has identified an issue.
- Share information with other providers and ACMA once a material case has been identified as soon as practicable.
- Where a scam call or SMs is confirmed, block the phone number/alphanumeric sender ID or message header as soon as practicable.

Reporting


- Providers must report to ACMA by 20 business days after the end of the calendar quarter, on the number of scam calls and SMs blocked.

Banking

The banking sector code would outline specific obligations for banks (ADIs as defined above), tailored to their role in the scams ecosystem.

The Government, through the Department of Treasury, would develop the banking sector code, drawing on the technical expertise of regulators and industry to ensure that obligations are fit-for-purpose and able to be implemented by different types and sizes of businesses in the sector, as well as have a meaningful impact on reducing scam activity across the sector. The Government would establish powers in relevant legislation, such as ASIC's administered legislation, for ASIC to enforce the banking sector code.

The box below sets out potential obligations that could form part of the banking sector code to prevent, detect, disrupt, and respond to scams. The obligations under this code are intended to address scams as defined earlier in this paper and do not seek to address unauthorised transactions.



Obligations in relation to unauthorised transactions will be considered as part of the future review of the ePayments Code.¹⁸

The obligations would apply consistently across businesses in the sector, while providing sufficient flexibility for businesses to determine how best to meet the intent of the obligations considering business size, risk profile, and complexity.

The proposed obligations set out below may interact with or be similar to requirements banks must comply with under other regulatory regimes and frameworks, such as the AML/CTF regime. Stakeholder feedback is welcomed on the extent to which banks are already meeting these proposed obligations in response to existing regulatory requirements, and the effectiveness or gaps in existing requirements in addressing scams and reducing scam activity.

¹⁸ [A Strategic Plan for...~https://treasury.gov.au/publication/p2023-404960](https://treasury.gov.au/publication/p2023-404960)

Possible bank-specific obligations

Prevention

- A bank must implement processes to enable confirmation of the identity of a payee to reduce payments to scam accounts.
- A bank must implement processes to verify a transaction is legitimate where a consumer undertakes activity that is identified as having a higher risk than their normal activity and is or is likely to be a scam.
 - A bank must have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts). Additional steps must be taken if the consumer is identified as having a higher propensity to be affected by a scam.
- A bank must implement and have in place processes and methods to detect higher risk transactions and take appropriate action to warn the consumer, block or suspend the transaction, or as well as take other measures to reduce scam activity and limit exit channels for the proceeds of scams, including blocking or disabling the scammer account (if in the same bank) or working with the recipient bank to do so.

Detection and disruption

- A bank must have in place methods or processes to identify and share information with other banks that an account or transaction is likely to be or is a scam.
- A bank must have in place processes to act quickly on information that identifies an account or transaction is likely to be or is a scam, including blocking or disabling the scammer account or the transaction (if in the same bank) or working with the recipient bank to do so.

Response (obligations to consumers)

- A bank must have user-friendly and accessible methods for consumers to immediately take action where they suspect their accounts are compromised or they have been scammed (e.g. an in-app 'freeze switch').
- A bank must assist a consumer to trace and recover transferred funds to the extent that funds are recoverable, including a receiving bank to revert a transfer within 24 hours of receiving a recall request from a sending bank.
- A business must respond to an information request from ASIC within the timeframe specified.

Digital Communications Platforms

The digital communications platforms code would outline specific obligations for digital communications platforms (as defined above), tailored to their role in the scams ecosystem.

To be consistent with the Government's election commitment, the primary law, and obligations on other sectors, it is intended that obligations on digital communications platforms would be mandatory. To achieve this, the Government would establish powers in the relevant legislation, such as ACMA's administered legislation (e.g. *Broadcasting Services Act 1992* (BSA) or *Telecommunications Act*), for the ACMA to establish and enforce codes and standards for digital communications platforms regarding scams. The Minister for Communications would then direct the ACMA to develop a new industry standard applying to digital communications platforms, consistent with the obligations under the CCA.

The ACMA would consult with industry to ensure that obligations are fit-for-purpose and able to be implemented by different types and sizes of businesses in the sector, as well as have a meaningful impact on reducing scam activity across the sector.

An alternative pathway to the ACMA developing obligations would be to allow the digital communications platforms industry to develop a code itself, to be registered and enforced by the ACMA to provide mandatory obligations, if the Government considers the industry code to be consistent with obligations across other regulated sectors.

Regardless of the pathway, any resulting mandatory obligations would need to meet the same criteria - be effective in reducing scam activity while applying the minimum necessary regulatory burden across the sector.

The box below sets out potential obligations that could form part of the digital communications platforms code to prevent, detect, disrupt, and respond to scams. The obligations would apply consistently across businesses in the sector, while providing sufficient flexibility for businesses to determine how best to meet the intent of the obligations, considering business size, risk profile, and complexity.

Possible digital communications platform specific obligations

Prevention

- A provider of a digital communications platform must implement processes to authenticate and verify the identity and legitimacy of business users and advertisers, to prevent users from selling or advertising scam products and services on the platform.
- A provider of a digital communications platform must have in place processes and methods to detect higher risk interactions, and take appropriate action to warn the user, block or disrupt the interaction, or take other measures to reduce scam activity, content or profiles such as blocking or disabling accounts based on shared intelligence.
- A provider of a digital communications platform must have in place processes and methods to prevent user accounts from being hacked by scammers, and to restore user accounts to the correct users in a timely manner.

Detection and disruption

- A provider of a digital communications platform must have in place methods or processes to identify and share information with other digital communications platform providers and the NASC that an Australian user is likely to be or is a scammer.
- A provider of a digital communications platform must have in place processes to act quickly on information that identifies a user or interaction is likely to be or is a scam, including blocking or disabling the account being used by the scammer.

Response (obligations to consumers)

- A provider of a digital communications platform must ensure that its platform has user-friendly and accessible methods for consumers to take action where they suspect their accounts are compromised or they have been scammed.
- A business must respond to an information request from the ACMA within the timeframe specified.

Questions on sector-specific codes:

34. Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?
35. Are there additional obligations the Government should consider regarding the individual sector codes?
36. Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?
37. Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?
38. Are the proposed approaches to developing sector-specific codes appropriate, and are there other approaches that could be considered to meet the objectives of the Framework?
39. Should any of the proposed sector-specific obligations specify a timeframe for a business to take action, and if so, what timeframe would be appropriate?
40. What changes could businesses be expected to make to meet the sector-specific code obligations, and what would be the estimated cost associated with these changes?
41. What are the relative costs and benefits of other available options, pathways or mechanisms, such as co-regulation, to set out additional mandatory sector-specific obligations?
42. Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?

Approach to oversight, enforcement and non-compliance

The Framework would have a multi-regulator oversight and enforcement model. This approach recognises the existing roles, responsibilities, expertise, and links regulators have across different parts of industry in combatting scams.

The Government proposes that under this model:

- The **ACCC** would be responsible for monitoring compliance and enforcing the principles-based obligations and other requirements set out in the CCA overarching regime. The ACCC, as the regulator responsible for enforcing Australia's consumer protection laws, is the most appropriate regulator for the overarching Framework. The ACCC would have a strong role in monitoring and taking enforcement action for systemic, significant or cross-sectoral breaches of the CCA. The ACCC would also issue guidance to industry on best practices to comply with the Framework.
- **ASIC** would be responsible for monitoring compliance and enforcing the bank-specific code. ASIC has an existing relationship with the banking sector through its regulatory functions and has already undertaken work looking at the responses of major banks in detecting, preventing and responding to scams. This approach would expand ASIC's existing powers and leverage ASIC's role in monitoring compliance with other codes, including the ePayments Code. ASIC's costs to administer any additional functions under the Framework may be recoverable through its Industry Funding Model and levies charged to industry .
- The **ACMA** would be responsible for enforcing the digital communications platforms and telecommunications sector codes. ACMA engages with the digital platform industry and deals with lateral issues that would support its duties with regards to online scams, such as broadcaster advertising regulations and telecommunications scams. This approach would align regulation of digital communications platforms with other media and communications industries, such as telecommunications providers which are already being regulated by the ACMA. The ACMA's costs to administer any additional functions under the Framework may be recoverable through its Industry Funding Model and levies charged to industry.

The Government also wishes to leverage the sector-specific regulators' enduring relationships with each sector and established technological and digital capabilities, as this will lead to better results at the sector level.

The Government recognises the need for a consistent and whole-of-ecosystem approach to enforcement. Memoranda of Understanding (MOUs) would set responsibilities between regulators to manage and coordinate enforcement and compliance actions. There would be a strong expectation that regulators would work closely together to consistently administer and enforce the Framework. Regulators responsible for enforcing future codes or standards will be determined by Government on a case-by-case basis.

Penalties for non-compliance

Where a regulated business fails to comply with their obligations under the Framework, in addition to redress options through applicable IDR and EDR such as compensation for scam losses, penalties for non-compliance would also apply.

The CCA provides penalties for non-compliance for 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.

Similarly, additional penalties for breaches of sector-specific obligations would be set under the sector-specific enabling legislation. Consideration will be given to whether there should be consistency between penalties for breaches of sector-specific obligations and penalties for non-compliance with the principles-based obligations in the CCA, as well as consistency of penalties across sectors. Currently, the enforcement regime for codes under the Telecommunications Act is different to that under the BSA, and the ASIC-administered legislation. During legislative design, Government and regulators will work through the necessary arrangements to avoid two regulators taking simultaneous action against a breach under the Framework.

Questions on approach to oversight, enforcement and non-compliance:

43. How would multi-regulator oversight impact different industries within the scams ecosystem? Are there any risks or additional costs for businesses associated with having multi-regulator oversight for enforcing the Framework?
44. Are there other factors the Government should consider to ensure a consistent enforcement approach?
45. Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?

Appendix A – List of stakeholder questions

Stakeholders are invited to consider the Framework set out in this paper and examples of potential obligations that are designed to meet the Framework’s objectives.

The proposed Framework and potential obligations outlined in this paper have not received Government approval and are not yet law. This paper is merely a guide as to how potential obligations might operate.

A list of consolidated questions is set out below. In providing feedback on examples, stakeholders should consider how proposals would meet objectives of the Framework, alongside the cost to businesses and regulatory burden of obligations, as well as any implementation challenges.

Questions on the proposed Framework

1. Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?
2. Is the structure of the Framework workable – can it be implemented in an efficient manner? Are there other options for how a Framework could be structured that would provide a more efficient outcome?
3. Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?
4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?
5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?
6. What future sectors should be designated and brought under the Framework?
7. What impacts should the Government consider in deciding a final structure of the Framework?

Questions on definitions

8. Is maintaining alignment between the definition of ‘scam’ and ‘fraud’ appropriate, and are there any unintended consequences of this approach that the Government should consider?
9. Does a ‘dishonest invitation, request, notification, or offer’ appropriately cover the types of conduct that scammers engage in?
10. Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?
11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?
12. Will the proposed definitions for designated sectors result in any unintended consequences for businesses that could not, or should not, be required to meet the obligations set out within the Framework and sector-specific codes?

13. Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?
14. What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?

Questions on overarching principles-based obligations

15. Are there additional overarching obligations the Government should consider for the Framework?
16. Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?
17. Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?
18. Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?
19. What changes could businesses be expected to make to meet these obligations, and what would be the estimated regulatory cost associated with these changes?

Questions on anti-scams strategy obligation

20. What additional resources would be required for establishing and maintaining an anti-scam strategy?
21. Are there any other processes or reporting requirements the Government should consider?
22. Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?
23. How often should businesses be required to review their anti-scam strategies and should this be legislated?
24. Are there any reasons why the anti-scams strategy should not be signed off by the highest level of governance within a business? If not, what level would be appropriate?
25. What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?

Questions on information sharing requirements

26. What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?
27. What safeguards and/or limitations (regulatory, technical, logistical or administrative) should the Government consider regarding the sharing of information between businesses, the NASC or sector-specific regulators?
28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?
29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

Questions on consumer reports, complaints handling and dispute resolution


30. What are the limitations or gaps that need to be considered in leveraging existing IDR requirements and EDR schemes for the purposes of this Framework?
31. If the remit for existing EDR schemes is expanded for complaints in relation to this Framework:
 - a. what criteria should be considered in relation to apportioning responsibility across businesses in different sectors?
 - b. how should the different EDR schemes operate to ensure consumers are not referred back and forth?
 - c. what impacts would this have on your business or sector?
32. Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? Should these be equal across all sectors and how should they be set?
33. Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?

Questions on sector-specific codes

34. Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?
35. Are there additional obligations the Government should consider regarding the individual sector codes?
36. Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?
37. Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?
38. Are the proposed approaches to developing sector-specific codes appropriate, and are there other approaches that could be considered to meet the objectives of the Framework?
39. Should any of the proposed sector-specific obligations specify a timeframe for a business to take action, and if so, what timeframe would be appropriate?
40. What changes could businesses be expected to make to meet the sector-specific code obligations, and what would be the estimated cost associated with these changes?
41. What are the relative costs and benefits of other available options, pathways or mechanisms, such as co-regulation, to set out additional mandatory sector-specific obligations?
42. Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?

Questions on approach to oversight, enforcement and non-compliance

43. How would multi-regulator oversight impact different industries within the scams ecosystem? Are there any risks or additional costs for businesses associated with having multi-regulator oversight for enforcing the Framework?

- 
44. Are there other factors the Government should consider to ensure a consistent enforcement approach?
 45. Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?

Attachment A – International developments

This attachment includes some examples of the most recent international developments regarding policies to combat scams.

Singapore

In October 2023, the Monetary Authority of Singapore (MAS) released a consultation paper¹⁹ setting out a proposed 'Shared Responsibility Framework' for addressing scam losses across the financial and telecommunications sector.

This consultation builds on a range of existing measures that the Singaporean Government, banks, and other ecosystem players have progressively implemented to tackle scams. These were intended to immediately strengthen controls, while longer-term preventative measures were evaluated.

The Shared Responsibility Framework aims to strengthen direct accountability of financial institutions (both banks and relevant payment service providers) and telecommunications sectors to consumers in relation to preventing, detecting and responding to scams. The Framework is designed to cover phishing scams with a digital nexus, where a consumer is deceived into clicking on a phishing link and entering their credentials on a fake digital platform, thereby unknowingly revealing these credentials to the scammer.

The box below includes Anti-scam measures introduced as part of the Framework for telecommunications and banking sectors.

Telecommunications:


- Connect only to authorised aggregators to deliver SMS sender IDs to ensure messages originate from bona fide senders.
- Block SMS sender IDs that are not from authorised aggregators.
- Implement an anti-scam filter for all SMS that pass through the operator's network to block SMS with known phishing links.

Banking:

- Impose a 12-hour cooling off period upon activation of a digital security token during which 'high-risk' activities cannot be performed.
- Provide notification alert(s) on a real-time basis for the activation of a digital security token and conduct of high-risk activities.
- Provide outgoing transaction notification alerts on a real-time basis.
- Provide a 24/7 reporting channel and kill-switch to enable consumers to report and block unauthorised access to their accounts.

A failure to meet these obligations under the Framework would be the starting point for determining the party to be held responsible for losses. This is intended to incentivise financial institutions and telecommunications organisations to strictly uphold their obligations.

¹⁹ Monetary Authority of Singapore (MAS) (25 October 2023) [Consultation Paper on Proposed Shared Responsibility Framework](#) accessed 9 November 2023.



Assessment of liability involves a 'waterfall' approach, which assesses the bank as the first line of responsibility as the custodian of consumer monies. If the responsible financial institution has breached any of its duties under the framework it is expected to fully compensate the consumer for the loss. If it is found to have met its obligations, telecommunications organisations will be assessed to ensure they have upheld their obligations and will be required to compensate the consumer for their loss if they have breached requirements. If both the responsible financial institution and telecommunications organisation are found to have upheld their obligations, the consumer will bear the loss and may seek recourse via dispute resolution bodies. The responsible bank and telecommunications organisation will be responsible for conducting the investigation in the first instance.

The consultation on Singapore's proposed 'Shared Responsibility Framework' is due to conclude at the end of 2023.

United Kingdom

The United Kingdom (UK) has a charter in place for both the telecommunications and retail banking sectors. These charters both set out voluntary commitments undertaken by the sectors to combat fraud. Signatories to the telecommunications charter have agreed to a nine-point action plan which sets out commitments including:


- identify and implement techniques to block scam calls and share data on the source of these calls across the sector
- identify and implement techniques to block 'smishing' texts (text messages that deceive the recipient into sharing personal or financial information, clicking on malicious links, or downloading harmful software)
- work with banks to strengthen authentication checks at the point a device contract is applied for and at the point a customer requests to move their number to a new provider.

Through the retail banking charter, signatories have agreed to a seven-point action plan, including:

- consistent data collection sets on fraud reporting to produce sector-wide analysis of the nature of fraud in the sector
- working with the ecosystem to explore opportunities to enhance fraud protection, identify vulnerabilities and repatriate stolen funds to those affected by a scam
- developing a strategy to respond to and reduce practices of money mule activity with the Government and law enforcement.

In July 2023, the UK Security Minister convened a meeting of the Joint Fraud Taskforce to discuss the development of an online fraud charter with the tech sector to respond to the growing volume of fraud originating on social media platforms. The charter will ensure that tech firms take action to block scams, make it easier to report frauds and ensure that fraudulent content is removed swiftly.²⁰ The Charter will enhance and complement obligations imposed on providers of certain regulated internet services, including user-to-user and search services, in relation to fraudulent advertising through the Online Safety Act enacted on 26 October 2023.

²⁰ <https://www.gov.uk/government/news/government-and-industry-meet-to-progress-the-fight-against-fraud>.



In May 2022, the UK Treasury announced the intention to allow the UK Payments System Regulator (PSR) to require reimbursement for authorised push payment scams. This follows four years of voluntary reimbursement by 10 UK banks under the Contingent Reimbursement Code and requires both the sending and receiving bank to each reimburse 50 per cent of the total loss to the consumer.

The PSR is expected to publish information on the claims excess, maximum level of reimbursement, and guidance on customer standards of caution (gross negligence) later this year. The mandatory reimbursement requirement will come into effect in 2024.²¹

²¹ UK Payment System Regulator (PSR) (28 June 2023), [Confirmation of mandatory reimbursement for APP fraud](#), accessed 12 November 2023.