



s 22



Scams

- Treasury is meeting regularly with COBA representatives on scams, s 22 


s 22



- Treasury has indicated it will undertake further consultation with COBA and other banking sector representatives in the coming weeks.

s 22



Meeting with Anna Bligh

Tuesday, 8 August 2023, 2:45pm

Treasury attendees: Brenton Philp

Market Conduct and Digital Division

Scams

- Treasury is meeting regularly with ABA representatives on scams, which the ABA has identified as a top priority.

s 22

s 22



Scams

s 22



- The Government has also committed to introduce tough, new mandatory codes for banks, digital platforms and telecommunications providers to combat scams.
- The Assistant Treasurer's preferred model involves a hybrid approach of:
 - high-level, principles-based obligations in primary legislation under the *Competition and Consumer Act*, including requirements for businesses to develop a strategy outlining how they will identify, disrupt and respond to scams, and

- sector-specific codes, to provide tailored obligations for sectors, taking into account the size and complexity of regulated businesses.
- Treasury is undertaking targeted consultation with agencies, regulators, and industry bodies to seek views on the proposed approach, including the scope and content of possible obligations.
 - Market Conduct and Digital Division is meeting with NAB representatives on s 22 [REDACTED], and is also meeting with the ABA and key member banks on s 22 [REDACTED].

Scams

Key point/s

- Treasury has commenced targeted stakeholder consultation on the Government's election commitment to introduce new industry codes for banks, telcos and digital platforms on scams.
 - We are meeting with the ABA and member representatives after the ABA Council meeting.

s 22

Item overview

- The Assistant Treasurer's preferred model for industry codes on scams is a hybrid of primary legislation (containing principles-based obligations) and sector-specific codes (that would apply more tailored obligations).
- Treasury is undertaking targeted consultation with other agencies, regulators, and industry bodies to seek views on the preferred model, including the scope and content of possible obligations.
 - We are meeting with the ABA and member representatives on the afternoon of s 22 to seek their views on the preferred model, s 22

s 22

Treasury views and sensitivities

- Industry codes will ensure a whole-of-ecosystem approach to scams, setting clear responsibilities and lifting the bar for businesses to prevent, detect and respond to scams.
 - The banks support this approach, as they want to ensure the digital platforms and telcos have similarly tough obligations to address scams.

s 22

- Market Conduct and Digital Division will work with the Assistant Treasurer’s Office to organise a workshop between the Minister and the banks s 22

Treasury SES contact

David Pearl, Assistant Secretary, Market Conduct and Digital Division

Meeting Brief

MB22-000371

FOR INFORMATION - Minister Jones meeting s 22

- ANZ - Wednesday, 31 August 2022

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

CC: Treasurer – The Hon Jim Chalmers MP

PURPOSE OF MEETING

- Meet and greet with ANZ representatives, and an opportunity to discuss and seek views on:
 - the Government’s commitment to combat scams and online fraud;

s 22

KEY MESSAGES

- The Government has committed to introducing a range of measures to combat **scams** and online fraud, including establishing a new national anti-scam centre and developing new obligations for banks to clearly define responsibilities for protecting consumers and businesses.


s 22

s 22



BACKGROUND

Scams

- Treasury has been engaging with the ABA on the Government's election commitment on addressing scams. s 22
- 

s 22



- The Government acknowledges that a whole of government approach will be most effective to combat scams and is committed to developing measures across a broad range of sectors.

s 22



Noted



Meeting Brief
MB22-000389

FOR INFORMATION - Minister Jones meeting with NAB Group, s 22
[Redacted]

Thursday 1 September 2022

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP
CC: Treasurer – The Hon Jim Chalmers MP

PURPOSE OF MEETING

- Meet and greet with National Australia Bank (NAB) representatives, and an opportunity to discuss and seek views on:
 - the Government’s commitment to combat scams and online fraud;

s 22
[Redacted]

KEY MESSAGES

- The Government has committed to introducing a range of measures to combat **scams** and online fraud, including establishing a new national anti-scam centre and developing new obligations for banks to clearly define responsibilities for protecting consumers and businesses.


s 22
[Redacted]

s 22



BACKGROUND

Scams

- Treasury has been engaging with the ABA on the Government's election commitment on addressing scams. s 22
- 

s 22



s 22

- The Government acknowledges that a whole of government approach will be most effective to combat scams and is committed to developing measures across a broad range of sectors.

s 22

Meeting Brief

MB22-000493

FOR INFORMATION - Minister Jones Scams Roundtable with representatives from the four major banks, Australian Financial Crimes Exchange (AFCX) and the Australian Banking Association (ABA) on Thursday 3 November 2022

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

PURPOSE OF MEETING

- You are meeting with representatives from the four major banks, AFCX and the ABA on Thursday, 3 November 2022 at 11am.
- This roundtable ^{s 22} [REDACTED] has been organised to discuss options for the banking sector to strengthen measures to address scam activity.
- A draft agenda is at [Attachment A](#) and an attendee list is at [Attachment B](#).

KEY MESSAGES

- The Government has committed to a new long-term, coordinated, whole-of-government approach to reduce scam losses for Australians.
 - A key element of this approach is to bring together resources from the private sector, Commonwealth, states and territories to enable better collaboration, information sharing and coordinated disruption of scams.
- This meeting is an opportunity to reaffirm the Government's anti-scams agenda as a high priority.

Opportunities for discussion

s 22





Introduction of new scam codes

- Banks have asked for you to share insights into how the Government will deliver on its election commitment to introduce tough new industry codes for banks to clearly define responsibilities for protecting consumers and businesses.



Ministerial Brief

MB23-000186

FOR INFORMATION – Scams – Options for Industry Codes

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

CC: Treasurer – The Hon Jim Chalmers MP

KEY POINTS

- You requested, through your office, an initial high-level briefing on scam code options.
- Strong industry codes, placing obligations on industries at the frontline of the scams threat, will help to eliminate loopholes for scammers to exploit.
- The Government has committed to ‘strengthening industry codes for banks, telecommunications providers, social media providers and Government agencies to clearly define responsibilities for protecting consumers and businesses online’.
 - This recognises the central role of the private sector in preventing and disrupting scams at their source.
 - Stakeholders have expressed support for a ‘whole-of-ecosystem’ approach to scams, which Treasury also supports. This will help ensure coherence between obligations placed on the digital platforms, telecommunications providers and banks.

s 34(3)

- Any proposals for new industry codes should seek to:
 - clarify obligations on businesses across the scam ecosystem, including scam prevention, detection and response, noting that obligations may differ depending on where in the scam ecosystem a business sits
 - assign responsibility for anti-scam measures among businesses based on those best able (or at least cost) to address scams and where incentives best align
 - ensure that obligations are graduated, based on the level of risk and business size (for example, obligations on banks could be graduated by size, and obligations for digital platforms could focus on the major platforms)

- ensure more consistent protection for consumers, including minimum expectations and potentially ‘safe harbours’ if businesses meet these expectations.
- Obligations in industry codes should act as a floor rather than a ceiling, so businesses are not prevented from competing with each other on their anti-scam practices.
- Further information on current anti-scam activities across the scam ecosystem is at [Additional Information](#).

s 22



Table: Possible code options to be canvassed in the consultation paper

	Option 1 (Single Code)	Option 2 (Hybrid Code)	Option 3 (Sector-Specific Codes)
--	------------------------	------------------------	----------------------------------

s 22



<p>Obligations</p>	<p>Establishes general obligations that apply to a wide range of businesses, covering scam prevention, detection and response.</p> <p>For example, each business must establish a clear, publicly-available policy on its approach to supporting scam victims, must collect reports of scams from its customers, and report to the National Anti-Scam Centre (NASC) using the form specified by NASC.</p>	<p>Establishes high-level, risk-based principles that apply economy-wide, covering scam prevention detection and response.</p> <p>For example, high-level duties to:</p> <ul style="list-style-type: none"> • protect consumers from scams • maintain an anti-scam program which sets out an approach to scam prevention, detection and response based on its assessment of the risk faced by the relevant business (similar to the Anti-Money Laundering and Counter-Terrorism Financing requirements). <p>More detailed obligations for specific sectors could be included in sub-codes. For example, an obligation on banks to make reasonable attempts to recover scammed funds.</p>	<p>Each sector-specific code would set out detailed obligations relevant to the sector it regulates.</p> <p>For example:</p> <ul style="list-style-type: none"> • banks to make reasonable attempts to recover scammed funds • digital platform providers to take down scam advertisements and verify advertisers are legitimate businesses.
---------------------------	---	--	--

<p>Benefits</p>	<ul style="list-style-type: none"> • Sets clear and consistent expectations for all sectors. 	<ul style="list-style-type: none"> • Allows the setting of high-level expectations initially but also an incremental approach, as sub-codes could be introduced over time. This would allow initial focus on sectors for which compliance is a priority, such as digital platforms. 	<ul style="list-style-type: none"> • Provides flexibility to ensure regulatory arrangements are best suited to each sector. • Allows for an incremental approach, as new sector-specific codes could be introduced over time. For example, the Government may wish to wait to introduce a code for the banking sector
------------------------	---	--	---

	Option 1 (Single Code)	Option 2 (Hybrid Code)	Option 3 (Sector-Specific Codes)
			pending outcomes from the Australian Banking Association's (ABA's) anticipated industry standard on scams (ABA Industry Standard).
Challenges	<ul style="list-style-type: none">• May not adapt well to the unique context of each sector.• May be perceived to duplicate or conflict with the proposed ABA Industry Standard to commence in early 2024.	<ul style="list-style-type: none">• Sub-codes may lead to inconsistent expectations across sectors.• Complexities with defining specific sectors for sub-codes.• Potential for legislative complexities, particularly with different regulatory agencies responsible for enforcement.	<ul style="list-style-type: none">• Harder to achieve a coherent 'whole-of-ecosystem' response to scams.• Complexities with defining specific sectors, particularly digital platforms, and where businesses operate across several sectors, for example by providing a digital platform and payments system.

Clearance Officer
s 22
Director, Scams Taskforce
Competition and Consumer Branch
Market Conduct Division
11 May 2023

Contact Officer
s 22
Director, Scams Taskforce
s 22

CONSULTATION

Financial System Division; Law Division; Labour Market, Environment, Industry and Infrastructure Division

ATTACHMENTS

A: Additional Information

ATTACHMENT A – ADDITIONAL INFORMATION

s 22



Banks

- The recent ASIC report ‘Scam prevention, detection and response by the four major banks’ (April 2023) found the overall approach to scams strategy and governance of Australia’s four major banks was variable and less mature than expected. While some banks are taking proactive steps to address scams (such as partnering with telecommunications providers) these efforts are voluntary and irregular.

s 22



Ministerial Brief

MB23-000319

FOR INFORMATION - Briefing Request - UK Scams Model

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

CC: Treasurer – The Hon Jim Chalmers MP

Mandated reimbursement

- The UK Payments Systems Regulator (PSR) is responsible for current and planned measures in the payments system to protect and reimburse consumers exposed to APP fraud.
- In May 2019, the PSR introduced the Contingent Reimbursement Model Code, a voluntary standard committing signatories to implement procedures to detect, prevent and respond to APP fraud and provide reimbursement to victims. The Code is signed by 10 firms representing 21 UK banks, including the UK 'Big Four' banks.
 - Reimbursement applies where a customer has been the victim of an APP fraud. Claims must be assessed by the firm as no-fault, excluding circumstances such as where customers ignore warnings or fail to take appropriate action.
 - Oversight of the Code is administered by the industry-led Lending Standards Board (LSB), with dispute resolution over decisions made under the Code administered by the Government's Financial Ombudsman Service.
 - A review of the Code by the LSB in 2021 found that take up of the Code was slower than expected, and expressed concerns about inconsistencies and delays in how firms applied the Code to their customers.
- In June 2023, the PSR published a plan to implement a mandatory reimbursement model for APP fraud in 2024. Under this model, eligible claims must be reimbursed by payment operators, with costs evenly split between sending and receiving firms.
 - Reimbursement will be subject to several limits yet to be confirmed. Payment system operators will be able to impose limits to claims, a claim excess, maximum levels of reimbursement, and a thirteen-month time limit on claims. Assessment and dispute resolution will also be the responsibility of operators.

- The PSR plans to engage an independent payment system operator, Pay.UK, to implement the reimbursement system and enforce compliance under its real-time Faster Payment system.
- The Bill to enable the new reimbursement arrangements, the Financial Services and Markets Bill, passed the UK Parliament in June 2023. The PSR will undertake further consultation on draft legal instruments in late 2023, with the new arrangements expected to commence in 2024.
- The mandatory reimbursement model has been endorsed by consumer groups such as the Consumer Action Law Centre.
- If asked about the UK approach, draft talking points are at [Attachment A](#).

Clearance Officer

s 22

Director, Scams Taskforce
Competition and Consumer Branch
Market Conduct and Digital Division
30 June 2023

Contact Officer

s 22

Policy Analyst
s 22

CONSULTATION

Financial System Division

ATTACHMENTS

A. Draft Talking Points

Draft Talking Points

- The Government has committed to introducing tough new industry codes for banks, telcos and digital platforms, outlining their responsibilities in responding to scams.
- We want to raise the bar and set clear obligations on businesses to protect their consumers from scams.
- As part of this work, we are looking closely at overseas regulatory approaches, including in the United Kingdom.
- We intend to consult on these issues in the coming months.

Meeting Brief

MB23-000423

FOR INFORMATION - Minister Jones meeting with NAB and Microsoft on Scams – 13 September 2023

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP
CC:

PURPOSE OF MEETING

- You are meeting with ^{s 22} [REDACTED] of the National Australia Bank, and ^{s 22} [REDACTED], on 13 September 2023.

s 22

[REDACTED]

KEY MESSAGES

Industry codes

- The Government has committed to introduce tough, new mandatory codes for banks, digital platforms and telecommunications providers to combat scams.
 - This will ensure a whole-of-ecosystem approach to scams, setting clear responsibilities and lifting the bar for businesses to prevent, detect and respond to scams.
- The proposed model involves a hybrid approach of:
 - high-level, principles-based obligations in primary legislation under the *Competition and Consumer Act*, including requirements for businesses to develop a strategy outlining how they will identify, disrupt and respond to scams, and
 - sector-specific codes, to provide tailored obligations for sectors, taking into account the size and complexity of regulated businesses.
- Obligations would be enforced through a multi-regulator approach, with relevant industry regulators enforcing each sector-specific code.

- Treasury is currently undertaking targeted consultation with agencies, regulators, and industry bodies.
 - Treasury is meeting with NAB on s 22 [REDACTED], and the ABA and key member banks on s 22 [REDACTED] (timing TBC), to seek views on the proposed approach, including the scope and content of possible obligations under the codes.
- Once the proposed framework is settled within Government, Treasury expects to consult further with industry participants later in 2023, s 22 [REDACTED]

s 22



Clearance Officer

s 22

Director, Scams Taskforce
Market Conduct and Digital Division
6 September 2023

Contact Officer

s 22

Policy Officer
Ph: s 22

s 22



Meeting Brief

MB23-000425

FOR INFORMATION - Treasurer meeting with Australian Banking Association on Wednesday 13 September 23

TO: Treasurer - The Hon Jim Chalmers MP

PURPOSE OF MEETING

- You are meeting with Ms Anna Bligh, Chief Executive Officer (CEO) of the Australian Banking Association (ABA), along with the following representatives of the ABA and regional Australian banks:

- s 22 Bendigo and Adelaide Bank

- s 22 AMP Bank

- s 22 Bank of Queensland

- s 22 MyState Limited

- s 22 CEO, Suncorp

- Attendees may wish to discuss s 22
scams s 22 .

s 22



Industry codes on scams

- Industry codes will ensure a whole-of-ecosystem approach to scams, setting clear responsibilities and lifting the bar for businesses to prevent, detect and respond to scams.
- The proposed model involves a hybrid approach of:
 - high-level, principles-based obligations in primary legislation under the *Competition and Consumer Act*, including requirements for businesses to develop a strategy outlining how they will identify, disrupt and respond to scams, and
 - sector-specific codes, to provide tailored obligations for sectors, taking into account the size and complexity of regulated businesses.
- Treasury is undertaking targeted consultation with agencies, regulators, and industry bodies to seek views on the proposed approach, including the scope and content of possible obligations.
 - Treasury is meeting with the ABA on s 22, to seek views on the proposed approach, including the scope and content of possible obligations under the codes.
- Once the proposed scams code framework is settled within Government, Treasury expects to consult further with industry later in 2023, s 22

s 22



Clearance Officer
s 22
Director A/g
Financial System Division
8 September 2023

Contact Officer
s 22
Analyst
Ph: s 22

s 22



Meeting Brief

MB23-000583

FOR INFORMATION – Minister Jones meeting with Australian Banking Association (ABA) on Wednesday 29 November 2023

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP
CC:

PURPOSE OF MEETING

- You are meeting with Anna Bligh, CEO of the Australian Banking Association (ABA).
- Possible topics include scams, s 22

KEY MESSAGES

- Treasury has undertaken targeted stakeholder consultation on the Government's election commitment to introduce new industry codes for banks, telecommunications companies and digital platforms on scams. Wider public consultation will be announced shortly.
- The Government welcomes the launch of the ABA Scam Safe Accord, which will complement and help inform the Government's work on industry codes.

s 22

BACKGROUND

Scams

- Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and Arts (DITRDCA) are planning to launch a public consultation process (consultation paper and survey) on mandatory industry codes on scams. We have provided you with the submission **MS23-002386** to seek agreement to launch this process.
 - The objective of the consultation paper and survey is to seek feedback on the key features of the scope of the Scams Code Framework, proposed industry obligations, and the regulatory impact and compliance costs for businesses.

s 22



- Treasury has met regularly with the ABA and member banks to align Government and industry efforts on the above work.
 - On 1 November, you held a ‘hot house’ workshop with the banking sector in which ABA and member banks outlined the Accord, and discussed possible banking sector obligations under the Scams Code Framework.

s 22



Clearance Officer

s 22

Director

Scams Taskforce

Market Conduct and Digital Division

27 November 2023

Contact Officer

s 22

Policy Analyst

Ph: s 22

s 22

ATTACHMENTS

A: s 22

B: ABA Scam Safe Accord

ATTACHMENT B: ABA SCAM-SAFE ACCORD

The Accord applies to all members of the Australian Banking Association and the Customer Owned Banking Association, and includes banks, mutual banks, credit unions and building societies.

Disrupt
<p>Banks will deliver an industry-wide confirmation of payee solution to customers All banks will roll out this name checking technology so customers know who they are dealing with, mitigating the possibility of people being manipulated into paying a scammer when the name does not match. design of the new system will start straight away and it will be built and rolled out over 2024 and 2025.</p>
<p>Banks will take action to prevent misuse of bank accounts via identity fraud All banks will adopt further technology and controls to help prevent identity fraud, including major banks using at least one biometric check for new individual customers opening accounts online by the end of 2024. these checks will be either detectable to a person’s behaviour or involve a check of a customer’s face or fingerprint, enabling banks to use these characteristics to verify their customer’s identity.</p>
<p>Banks will introduce warnings and payment delays to protect customers If a customer is transferring money to someone they haven’t paid before or raising payment limits, they can expect more questions, warnings and delays from their bank to protect them from falling victim for a scam. It will act as a mitigant when scammers put customers under pressure to act quickly to transfer funds. banks will work to introduce enhanced warnings and delays by the end of 2024.</p>
Detect
<p>Banks will invest in a major expansion of intelligence sharing across the sector All ABA and COBA members will join the Australian Financial Crimes Exchange (AFCX) to be ready to use their scams intel to fight scams from mid-2024, and the Fraud Reporting Exchange over 2024-25 to help customers recover money faster. this means scams intelligence can be shared at speed between banks, helping banks prevent more scams and recover funds for customers faster.</p>
Respond
<p>Banks will limit payments to high-risk channels to protect customers Banks will make these risk-based decisions when they identify high risk getaway vehicles being used by scammers to move money out of Australia. expect more banks to start limiting payments to high-risk channels such as some crypto currency platforms to protect customers from possible theft. once stolen funds are in a getaway vehicle to a high risk crypto currency platform it is virtually impossible to recover them.</p>
<p>Banks will implement an Anti-Scams Strategy All banks will implement an anti-scams strategy to enhance oversight of the bank’s scams detection and response.</p>

Meeting Brief

MB23-000595

FOR INFORMATION – Urgent - Treasurer meeting with Australian Banking Association on Wednesday 29 November 2023

TO: Treasurer - The Hon Jim Chalmers MP

PURPOSE OF MEETING

- On Wednesday, 29 November, you are meeting with Anna Bligh, CEO of the Australian Banking Association (ABA), s 22 .

s 22



Scams

- Treasury has undertaken targeted stakeholder consultation on the Government’s election commitment to introduce new industry codes for banks, telecommunications companies and digital communication platforms on scams. Public consultation will be announced shortly.
- The Government welcomes the launch of the ABA Scam Safe Accord and supports the agreed banking sector initiatives, which will complement the Government’s work on industry codes.

s 22



Clearance Officer
s 22
Director
Financial System Division
27 November 2023

Contact Officer
s 22
Assistant Director
Ph: s 22

s 22



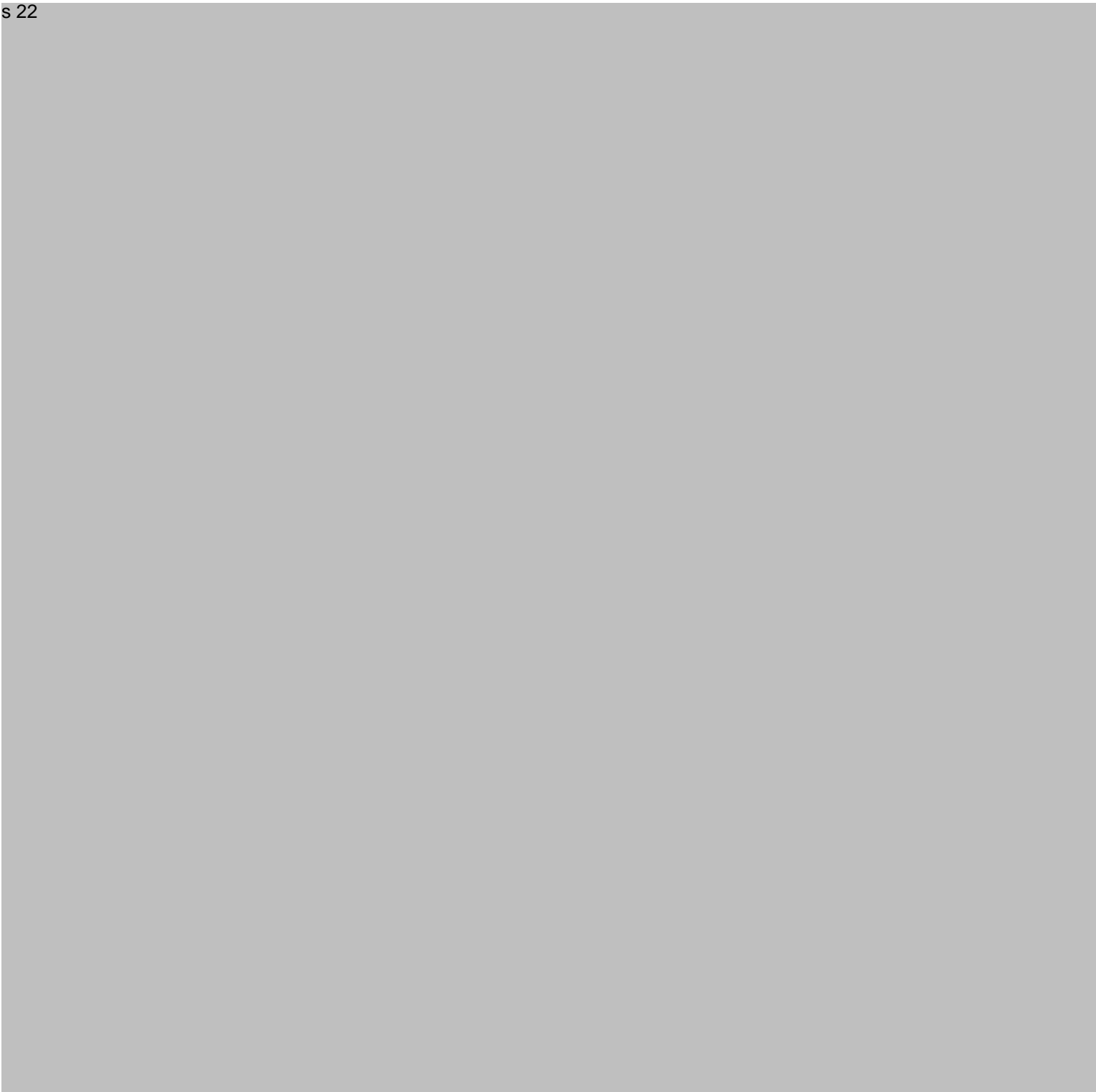
ATTACHMENTS

A: Additional information
s 22



ATTACHMENT A: ADDITIONAL INFORMATION

s 22



Scams

- Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and Arts (DITRDCA) are planning to launch a public consultation process (consultation paper and survey) on mandatory industry codes on scams.

s 22

- The objective of the consultation paper and survey is to seek feedback on the key features of the scope of the Scams Code Framework, proposed industry obligations, and the regulatory impact and compliance costs for businesses.
- You may wish to raise that the Assistant Treasurer and Minister Rowland expect to announce the consultation in coming days or week, and that Treasury will engage the ABA during the consultation process.

s 22

- On 1 November, the Assistant Treasurer held a ‘hot house’ workshop with the banking sector in which ABA and member banks outlined the Accord, and discussed possible banking sector obligations under the Scams Code Framework.

s 22

Meeting Brief
MB23-000608

FOR INFORMATION - Treasurer and Assistant Treasurer meeting with NAB on Tuesday 5 December 23

TO: Treasurer - The Hon Jim Chalmers MP, Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

PURPOSE OF MEETING

- s 22 [Redacted]
- He is seeking your views about the priorities he is considering, including:
 - scams and fraud

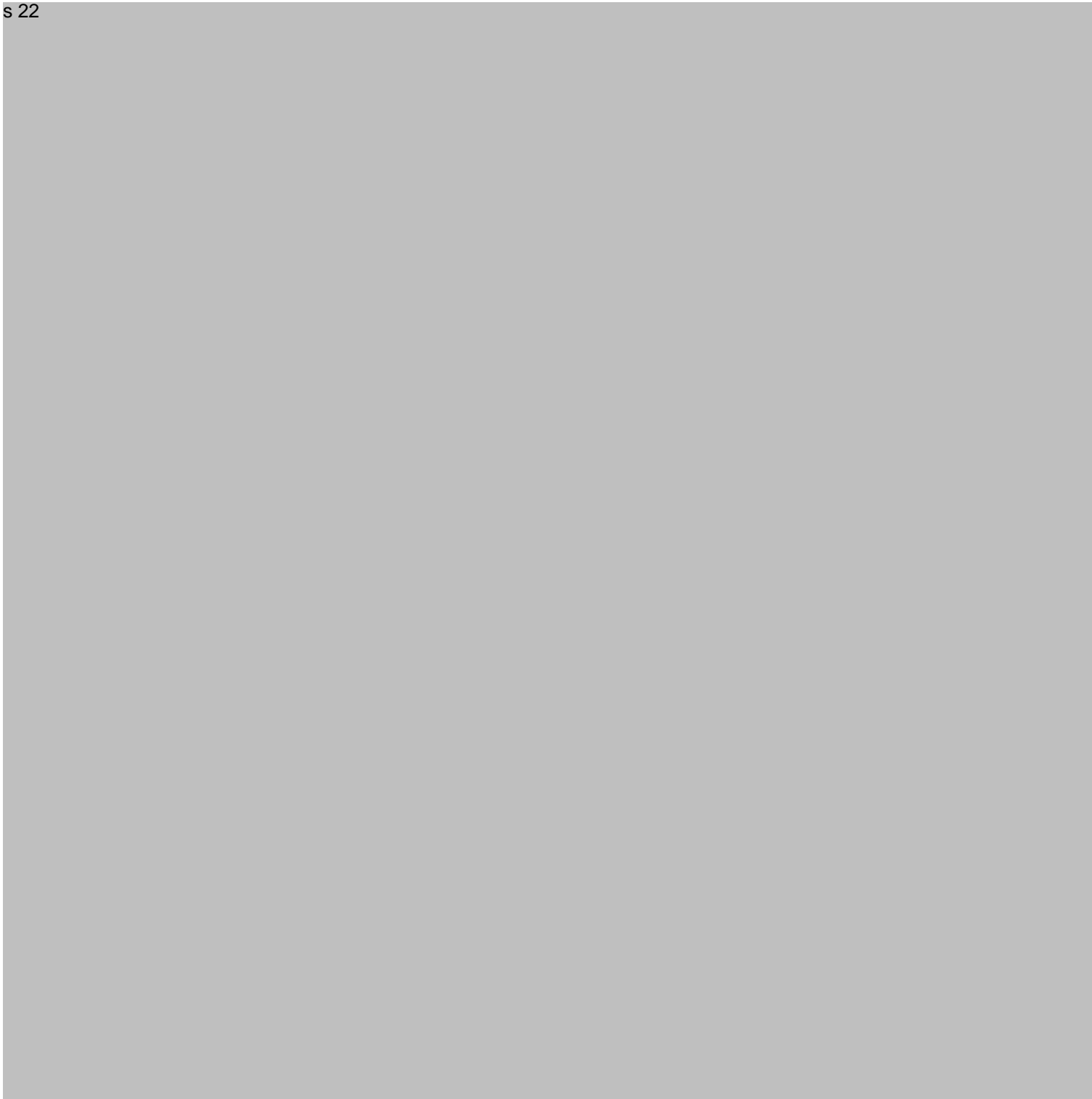
s 22 [Redacted]

KEY MESSAGES

Scams and Fraud

- Addressing scams and fraud is a priority for Government, with Treasury and the Department of Infrastructure, Transport, Regional Development and Communications (DITRDCA) currently undertaking public stakeholder consultation on the election commitment to introduce new industry codes for banks, telecommunications companies and digital platforms on scams.
- The Government welcomes the launch of the ABA Scam Safe Accord, which will complement and help inform the Government’s work on industry codes.

s 22 [Redacted]



BACKGROUND

Scams

- On 30 November 2023, the Assistant Treasurer announced a public consultation process (consultation paper and survey) on mandatory industry codes on scams co-led by Treasury and DITRDCA (submission [MS23-002386](#) refers).

- The objective of the consultation paper and survey is to seek feedback on the key features of the scope of the Scams Code Framework, proposed industry obligations, and the regulatory impact and compliance costs for businesses.

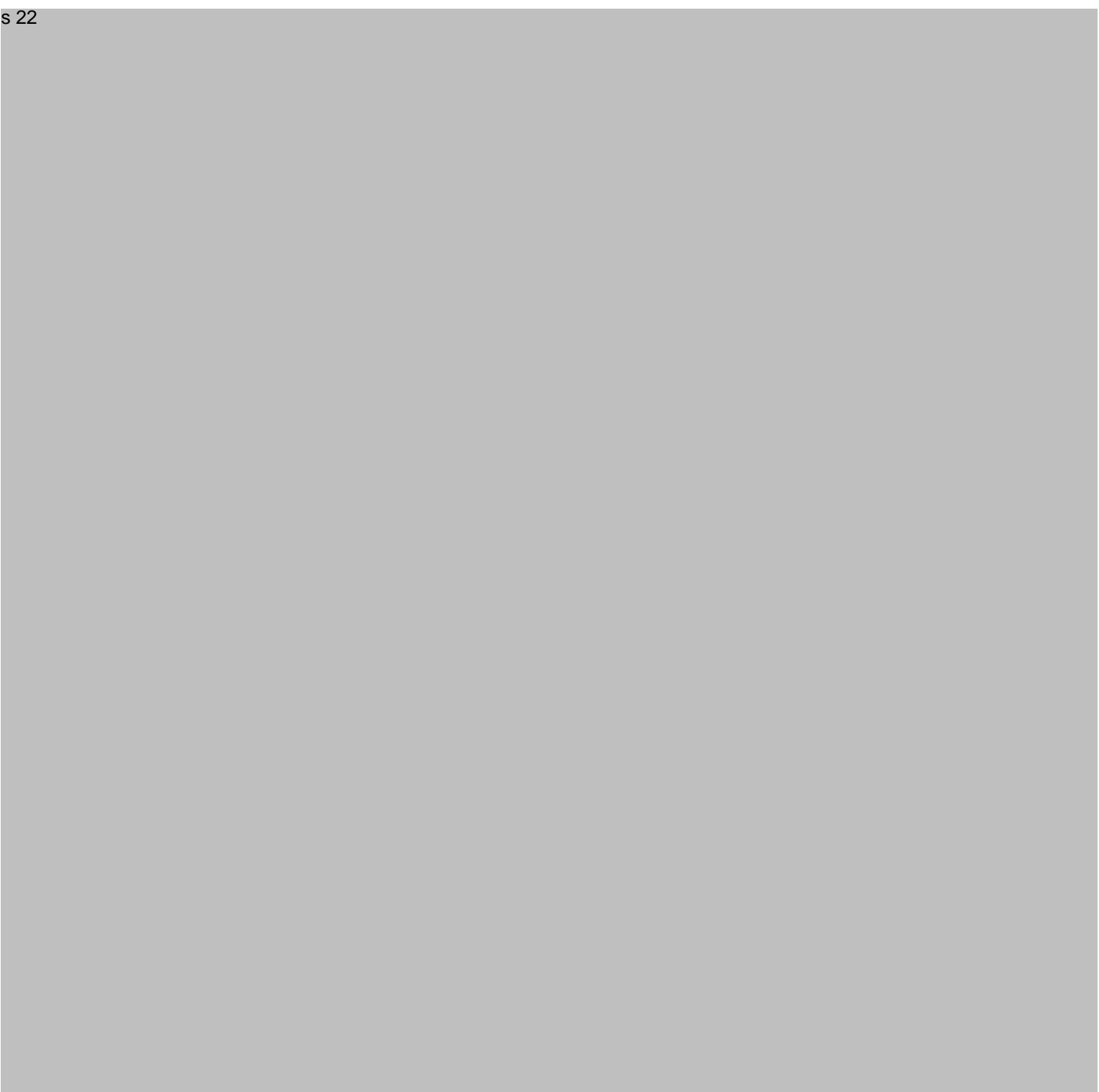
s 22



- Treasury has met regularly with the ABA and member banks to align Government and industry efforts on the above work.
 - On 1 November, the Assistant Treasurer held a ‘hot house’ workshop with the banking sector in which ABA and member banks, including NAB, outlined the Accord, and discussed possible banking sector obligations under the Scams Code Framework.

s 22





Clearance Officer
s 22
Director
Financial System Division
4 December 2023

Contact Officer
s 22
Analyst, Banking Unit
Ph: s 22

s 22



OFFICIAL

s 22

- We are now focused on delivering a framework that introduces tough, new mandatory codes on the private sector to prevent, detect and disrupt scams on their services. We are focussed on introducing obligations for banks, telecommunication providers and digital platforms in the first instance, which are the key sectors on which scams occur.

s 22

3. Where would we like to be in two years' time?

- In the Australian context, our key focus is on ensuring there is an overarching framework that sets clear roles and responsibilities of the Government, regulators, law enforcement and the private sector to take a coordinated approach in combatting scams.

2. How can we use legislation, for instance on the reimbursement or regulating industry to incentivise counter-fraud action?

- In the Australian context, we are focussing on legislative and regulatory levers we can use to incentivise action from industry. Every business in the scams ecosystem has a role to play in combatting scams.
- While we have seen some proactive and innovative voluntary industry initiatives to protect Australian consumers from scams, these efforts can be irregular and inconsistently applied across industry.
- The Australian Government is taking the next step in its commitment to fight scammers and publicly consulted on a proposed Scams Code Framework that would introduce mandatory industry codes for the private sector to address scams on their services.
- The proposed Framework will set clear roles and responsibilities across the scams ecosystem, with an initial focus on banks, telecommunications providers and digital platforms, to make Australia an even harder target for scammers.
- The proposed Framework would introduce minimum, consistent obligations for all regulated businesses to prevent, detect, disrupt, and respond to scams. This will be complemented with sector-specific obligations that are tailored to the role of each sector.
- Regulated businesses would be expected to have robust measures in place to address the risk of scams on their services. Strong regulator action and penalties would apply if businesses fail to comply with their obligations.
- Government, regulators, and industry have a mutual interest in making sure scams are identified and stopped before they can harm Australian consumers and businesses.

3. What is the one thing that would have the biggest impact in reducing fraud?

- Industry needs to step up to the plate and hold each other to account. They have the evidence base on the scale of fraud; and they can take action to remove scammers' access to the tools they use to cause harm.
- Industry needs to take a more increase their effort to identify and remove scam materials and scam attempts.

Australian Government action on scams

s 22

- The Government is also committed to introducing new, mandatory industry codes to outline the responsibilities of the private sector in relation to scam activity. These codes will place robust obligations on key sectors to protect consumers from scams.

Consultation – Scams Code Framework

- On 30 November 2023, Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) consulted on the design of a model to deliver on the Government’s commitment to mandatory industry codes for scams.
 - Treasury also released a survey seeking information about public experience with scams and views on potential improvements to address scams.
 - Consultation closed on 29 January 2024. The Government is considering the outcomes of consultation and the survey results and will provide an update in due course.
- The consultation proposal included a Scams Code Framework (Framework), which would establish a whole-of-ecosystem response to scams.
 - The proposed design of the Framework would leverage existing initiatives and systems to combat scams, while being flexible and responsive to the evolving scams threat.
 - The Framework would also address the current absence of a regulatory regime outlining and clarifying the roles and responsibilities of Government, regulators and the private sector to respond to scams and support victims.
- The proposed Framework is characterised by:
 - overarching legislation in the *Competition and Consumer Act 2010* setting out mandatory, principles-based obligations for businesses in regulated sectors to address scams perpetrated through their services

OFFICIAL

- industry codes, setting out tailored obligations for key sectors to deter, detect, disrupt and respond to scams.
- The Government’s initial focus would be on bringing banks, telecommunications providers and digital communications platforms into the Framework. These sectors are most commonly targeted by scammers.

s 22

Q&A

Scams Code Framework

1. When was consultation conducted and what sectors did you engage with?

- Treasury and DITRDCA consulted on the Framework from 30 November 2023 to 29 January 2024.
- Roundtables and bilateral meetings were held with the banking and financial services, digital platforms and telecommunications sectors, consumer and other advocacy organisations, external dispute resolution bodies and regulators.

s 22

2. What sectors would be subject to an industry code?

- Initial sectors covered by the Framework would be those most targeted by scammers: banks, telecommunications providers and digital communications platforms.

s 22

3. What are stakeholder and regulator views on the Framework?

- There was broad support on the overall objective and principles of the Framework, however differing views on its features.

4. When will Government introduce the Framework and when will industry be required to adhere to the new obligations?

- Government is considering the outcomes from Treasury and DITRDCA’s consultation and will provide an update in due course.

s 22

6. Why do we need new regulation?

- Currently, there is no overarching regulatory framework which outlines and clarifies the roles and responsibilities of the private sector for deterring, detecting, disrupting and responding to scams and supporting victims.
- Consumers have experienced inconsistent responses to scams, both across and within sectors. For example, a consumer may have very different exposure to, and experience of, scams depending on their bank, digital platform and telecommunications provider.
- All Australians would benefit from industry codes that help standardise consumer protections.

8. Will the Framework require banks or other sectors to compensate scam victims?

- The Government is considering the stakeholder feedback it received on complaints handling and dispute resolution mechanisms under the proposed Framework.
- It is important that any complaints handling, and dispute resolution processes operate coherently across the scams system.
- This may require regulated businesses to strengthen protections against scams through processes for receiving consumer scam reports, complaints handling, and internal and external dispute resolution.
- The Government is considering whether regulated businesses should be required to provide redress to consumers where they have not met their obligations under the Framework.

Anti-scam strategy

11. What is the proposed anti-scam strategy requirement?

- An anti-scam strategy would set out a business' approach to scam prevention, detection, disruption and response based on its assessment of its risk in the scams ecosystem.

Meeting Brief

MB24-000057

FOR INFORMATION - Minister Jones meeting with Consumer Action Law Centre on Wednesday 07 February 2024

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

s 22



KEY MESSAGES

s 22



- The Scams Code Framework ('Framework') proposed in the Government's recent consultation would establish obligations for businesses in line with the Government's view that industry should be held to a high bar to protect consumers against scams.
- The Government thanks CALC and other consumer groups for their submission to the consultation and their detailed feedback on how the consumer journey for scam victims could be improved.

s 22



s 22



Clearance Officer
s 22
Director
Scams Taskforce
6 February 2024

Contact Officer
s 22
Policy Analyst
Ph: s 22

s 22



Meeting Brief

MB24-000263

FOR INFORMATION - Assistant Treasurer meeting with CHOICE CEO Ashley de Silva on 6 June 2024

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

s 22



Scams

s 22



- The aim of the Government’s scams framework is to incentivise businesses to develop strong scam protections leading to reduced consumer harms due to scams. The new

Framework will include clear pathways for redress for consumers including in some cases, reimbursement for scam losses.

s 22



s 22



Clearance Officer

s 22

Director

Competition and Consumer Branch

31/05/24

Contact Officer

s 22

Analyst

s 22

s 22



ATTACHMENT D: SCAMS, s 22

This attachment covers CHOICE advocacy and Government policy on the following topics:

1. Scams

s 22

1. Scams

s 22

Background

The 2024-25 Budget provided funding for the development, introduction, and enforcement of mandatory industry codes, and for a public awareness campaign. This builds on the 2023-24 Budget's measures to address scams harms, which included the establishment of the National Anti-Scam Centre.

The Scams Code Framework and industry codes will start with banks, telcos, social media, digital messaging and search advertising services, and will require these groups to have measures in place to prevent, detect, disrupt, respond to and report scams.

Consultation for the proposed Framework closed in January 2024 and draft legislation is currently being prepared.

Talking points / next steps

s 22

The Framework's robust obligations will increase

s 22

s 22

The aim of the Government's scams framework is to incentivise businesses to develop strong scam protections leading to reduced consumer harms due to scams. The new Framework will include clear pathways for redress for consumers including in some cases, reimbursement for scam losses.

protections for consumers and improve the experiences of victims. There will be tough penalties for non-compliance.

Where a business does not meet its obligations, internal and external dispute resolution mechanisms will ensure consumers have access to appropriate redress.

s 22

s 22

Meeting Brief

MB24-000263

FOR INFORMATION - Treasurer meeting with CHOICE CEO - 5 June 2024

TO: Treasurer - The Hon Jim Chalmers MP

CC: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP;
Assistant Minister for Competition, Charities and Treasury, Assistant Minister for Employment -
The Hon Dr Andrew Leigh MP

s 22



- The aim of the Government’s scams framework is to incentivise businesses to develop strong scam protections leading to reduced consumer harms due to scams. The new Framework will include clear pathways for redress for consumers including in some cases, reimbursement for scam losses.

s 22



Clearance Officer

s 22

Director

Competition and Consumer Branch

29/05/2024

Contact Officer

s 22 sch

Analyst

s 22

s 22



s 22



C.1.	Background brief on scams in Australia
------	--

s 22



s 22



Assistant Treasurer (14:45 – 15:00)

s 22

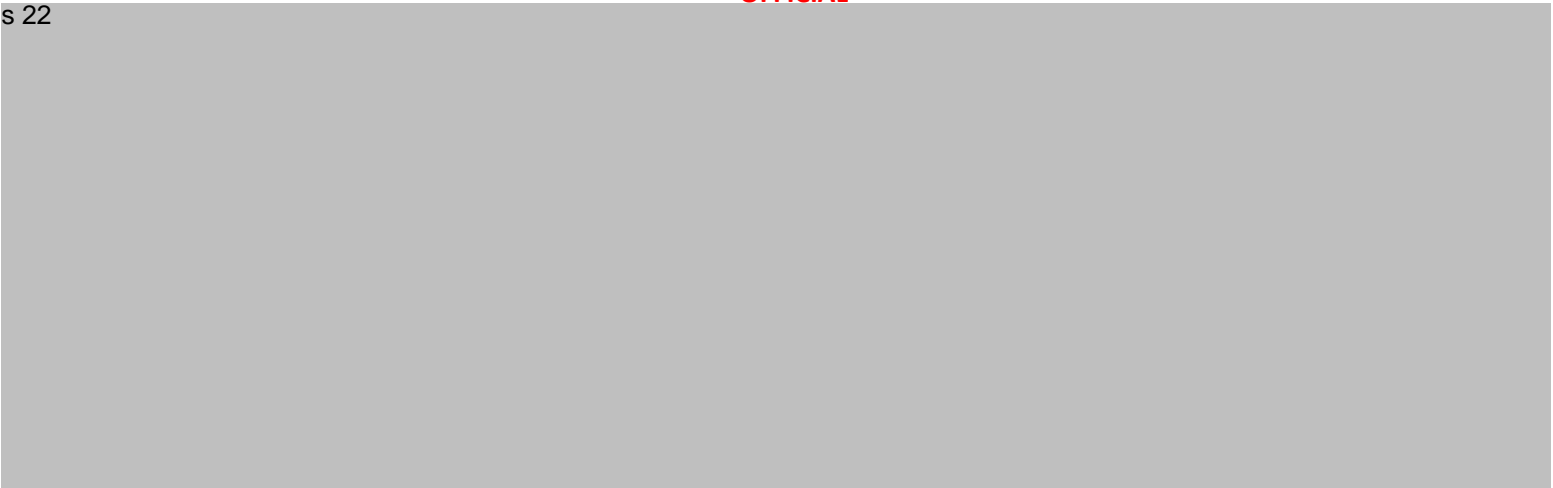


- The agenda is a multi-agency, whole-of-economy strategy to harden Government and industry action and properly respond to the recent rise in scams.
 - Many businesses and industry sectors in the ecosystem are taking voluntary action to improve their approach, such as the banking sector Scam-Safe Accord.
 - Piecemeal action is not sufficient. Mandatory measures are needed to ensure businesses or sectors that are not responding to the scam threat to protect their consumers are held accountable.
- To realise ambition, the Government is pursuing several initiatives including:
 - Establishing a mandatory industry Scams Code Framework to outline the responsibilities of banks, telecommunication companies and digital platforms.

s 22



s 22



- The Scams Code Framework, to be established in legislation this year, will introduce obligations in key sectors such as banks, telecommunications providers and digital platforms providing social media, private messaging, and search advertising

s 22



s 22

Scams

s 22

- The 2024-25 Budget includes additional measures to further strengthen protections and awareness to help reduce the incidence and harm of scams targeting Australians. It includes \$67.5 million in funding to:
 - legislate a Scams Code Framework and introduce and enforce mandatory industry codes under the Framework, which will set out obligations for regulated businesses to address scams on their services or platforms

s 22

Scams Code Framework

- The Government is progressing its commitment to establish new a mandatory industry codes framework (the Framework) for key industry sectors in the ecosystem to address scams.
- Initial designated sectors, will require banks, telecommunication providers and digital platform service providers to adhere to the Framework. s 22
- The Framework will establish principles-based obligations for entities to prevent, detect, disrupt and respond to scams, and principles relating to governance and reporting. The obligations will be complemented with sector-specific obligations in mandatory codes, which will be consistent with one or more principles in the Framework.

s 22

- The Framework will include strong penalties and enforcement tools to ensure compliance. External dispute resolution will be available to consumers from the commencement of the Framework under existing dispute resolution schemes to ensure access to appropriate redress for consumers affected by scams. Regulated entities would be required to reimburse consumers where they have breached the obligations under the Framework.

Scam-Safe Accord

- In November 2023, Australian banks agreed to a voluntary industry Scam-Safe Accord, led by the Australian Banking Association and Consumer-Owned Banking Association, committing members to implement measures that disrupt, detect and respond to scams:

Disrupt	<ul style="list-style-type: none"> - Industry-wide confirmation of payee solution to be designed immediately and built and rolled out over 2024-25. - Actions to prevent misuse of accounts via identity fraud including the use of at least one biometric check for new individual customers opening accounts by the end of 2024.
----------------	--

	<ul style="list-style-type: none">- New warnings and payment delays to protect customers for transfers to new payees or raising payment limits by the end of 2024.
Detect	<ul style="list-style-type: none">- Expanding intelligence sharing across the sector with all members joining the Australian Financial Crimes Exchange by mid-2024 and Fraud Reporting exchange by 2024-25 to recover money faster.
Respond	<ul style="list-style-type: none">- Limit payments to high-risk channels to protect customers, including risk-based decision-making such as limiting payments to high-risk channels such as cryptocurrency platforms to protect customers.- Implement an Anti-Scams Strategy in every bank to enhance oversight of the bank's scams detection and response.

Ministerial Submission
MS23-001808

FOR ACTION – Scams Code Framework: progress and update on key design features

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP
CC: Treasurer - The Hon Jim Chalmers MP

TIMING

By 18 September 2023, to settle the key features and outstanding design questions on the Scams Code Framework (the Framework) and enable you and the Minister for Communications to bring forward a Cabinet Submission seeking approval of the Framework in the 2023-24 MYEFO context.


Recommendation

- That you **note** the update and timing of the work to develop the Scams Code Framework.

Noted / Please discuss

- That you **agree** to the key features of the proposed Scams Code Framework at Attachment A, or indicate if you would like to discuss further, including any alternative approaches.

Agreed / Please discuss as indicated

Signature 	Date: 2 / 10 / 2023
---	---------------------

KEY POINTS

s 22

- As you are aware, since then Treasury has been working with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) to develop a Scams Code Framework (the Framework) in accordance with your preferred (hybrid primary law and sector codes) option, that would:
 - implement the Government’s commitment for mandatory industry codes
 - have a whole-of-ecosystem approach to scams
 - lift the bar for businesses across the scams ecosystem to prevent, detect, disrupt and respond to scams, and
 - clarify and set clear roles and responsibilities for the private sector, Government agencies and regulators to educate and protect consumers from scams.
- This brief provides an update on the progress made with DITRDCA and the agreed features of the Framework, outstanding design questions, and next steps and indicative timing.

Agreed features of the Framework

- As you are aware, Treasury and DITRDCA have reached agreement on the following key features for the Framework:
 - an overarching framework set out in the *Competition and Consumer Act 2010* (CCA) that would include principles-based obligations and other requirements that businesses must comply with to combat scams
 - the Australian Competition and Consumer Commission (ACCC) to have oversight of the overarching framework and would be responsible for monitoring and enforcing systemic issues and breaches
 - the CCA to establish the power to develop sector-specific codes that would apply tailored obligations on businesses, based on the level of risk and business size
 - a multi-regulator approach for enforcement of the sector-specific codes
 - obligations in the primary law and sector-specific codes to apply to the banking sector, digital platforms and telecommunication providers (telcos) in the first instance
 - strong penalties for breaches of the obligations in the primary law and the sector-specific codes, and

- an external dispute resolution (EDR) mechanism (such as through the Australian Financial Complaints Authority) to determine redress and reimbursement of funds to a consumer where a bank has breached its obligations under the sector-specific code.

s 22





Next steps



- Treasury is undertaking targeted consultation over the coming weeks with regulators (ACCC, ASIC), s 22 [redacted] and key stakeholders in industry (banks, s 22 [redacted] industry associations) on the key features of the Framework.



Treasury has already started meeting with key stakeholders (such as the Australian Banking Association) to discuss the following:

- : what the principles-based obligations could include
- : specific obligations for banks
- : what banks can do now and opportunities to fast track anti-scam initiatives

~~PROTECTED CABINET~~

Ministerial Submission

MS23-001808

ATTACHMENT A – KEY FEATURES AND OUTSTANDING DESIGN QUESTIONS ON THE FRAMEWORK

- Table 1 sets out the key features and outstanding design questions on the Framework. Please indicate the features you agree with or wish to discuss further, including any alternative approaches.
- Please note that these features are subject to further legislative design and advice.

Table 1: Key features and outstanding design questions on the Framework

Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
<i>Framework and obligations in the primary law</i>			
Principles-based obligations that would apply to businesses across the scams ecosystem, irrespective of the type or size of the business	<ul style="list-style-type: none">• High-level obligations that would set out requirements for businesses in respect of prevention, detection, disruption and response to scams.• The principles-based obligations would give flexibility for businesses to adjust their anti-scam efforts to the particular conditions of their sector, service offering or business model.• This could include principles such as requiring businesses to take robust steps to prevent the misuse of services, platforms or marketplaces by scammers and imposing a positive obligation to respond to reports by customers or the community of a scam involving the business.		Agreed / To discuss

Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
	<ul style="list-style-type: none">• The principles would also include obligations for businesses to have in place anti-scam measures for vulnerable cohorts and internal dispute resolution processes and procedures.• Industry stakeholders have raised concerns with Treasury that there are limitations in the system that prevent businesses from implementing certain anti-scam measures and sharing scam intelligence – for example, privacy laws and tipping off provisions. Treasury will work with relevant agencies and industry stakeholders to reduce impediments to businesses implementing anti-scam measures, where practicable and appropriate.		
Entities to develop and maintain an anti-scam strategy that is commensurate to the nature of scam risks and the size and complexity of the business in the scams ecosystem	<ul style="list-style-type: none">• This would be a separate requirement where a business must demonstrate how they will meet the principles-based obligations.• The strategy would need to set out the business’s approach to scam prevention, detection and response based on its assessment of its risk in the scams ecosystem.• The strategy must have approval and oversight by the business's board and senior management, or executive equivalent, and it would be required to monitor and review the strategy to assess its effectiveness and compliance against the Framework.• The ACCC would work with businesses to ensure strategies are fit-for-purpose, with businesses to incorporate feedback or guidance issued by the ACCC.		Agreed / To discuss
Businesses would be subject to information sharing and reporting requirements	<ul style="list-style-type: none">• Businesses would be required to share information and data with the National Anti-Scam Centre and relevant regulators. This could include information about the number of scam-related complaints that have been raised with the business and the outcomes of those complaints and internal dispute resolution.• Businesses may also be required to share information and data with other businesses to help prevent scams. Treasury will work with the Attorney-		Agreed / To discuss

Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
	General's Department and industry to explore opportunities for information sharing that balances privacy considerations, leverages existing systems (such as the Australian Financial Crimes Exchange) and does not duplicate existing reporting requirements.		
s 22			
The overarching scams code framework to be set in the <i>Competition and Consumer Act 2010</i> (CCA)	<ul style="list-style-type: none">• The Framework would likely be set out in a new part in the CCA.• The ACCC would be responsible for monitoring and enforcing the overarching framework including significant and systemic issues/breaches, working with businesses on their anti-scam strategies and working with the other regulators to monitor and evaluate the impact of the Framework on the scams ecosystem.		Agreed / To discuss

Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
	<ul style="list-style-type: none">The ACCC would be the whole-of-scams-ecosystem regulator and would leverage its experience in dealing with scams and other forms of consumer harm across multiple sectors.		
<i>Sector-specific codes</i>			
The scope of the sector-specific codes would apply to banks, digital platforms and telecommunication providers	<ul style="list-style-type: none">Consistent with the Government’s commitment, sector-specific codes would be developed for the banking sector, digital platforms and telcos. Subject to legislative resourcing and prioritisation considerations, this could occur alongside development and introduction of the primary legislation.Future reform could look at bringing in other types of businesses and sectors, such as smaller banks and platforms, non-bank lenders, cryptocurrency exchanges, payment system participants or the superannuation sector.		Agreed / To discuss
The sector-specific codes would have obligations tailored to entities based on their role in the scams ecosystem	<ul style="list-style-type: none">The sector-specific codes would have more detailed obligations for businesses, including obligations tailored to their specific role in the scams ecosystem.Obligations in the sector-specific code would be graduated based on the level of risk and business size. Applying consistent (but not scalable) obligations across all businesses, risks watering down the obligations to the lowest common denominator.See <u>Table 2</u> for examples of sector-specific codes for each sector.		Agreed / To discuss
Government develops the sector-specific codes	<ul style="list-style-type: none">Policy agencies would draft the sector-specific codes and draw on the technical expertise of regulators and industry.Treasury would be responsible for developing the sector-specific codes for banks, and would develop the sector-specific codes for digital platforms in consultation with DITRDCA. DITRDCA would be responsible for drafting the sector-specific codes for telcos.This would lift the bar for businesses and would be perceived as the tougher approach to combatting scams.		Agreed / To discuss

Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
	<ul style="list-style-type: none">You would be responsible for approving the sector-specific codes for banks, and co-approving the sector-specific codes for digital platforms with the Minister for Communications. The Minister for Communications would approve the sector-specific code for telcos.		

s 22



<i>Multi-regulator model for enforcement</i>			
ASIC would enforce the sector-specific code for banks	<ul style="list-style-type: none">ASIC would enforce the sector-specific code for banks and other sectors in the financial system that are designated in future tranches, for example, cryptocurrency exchanges, payment system participants, superannuation entities.There would be a clear demarcation between the 'scams banking code' (which would cover authorised payments) and the current ePayments Code (which covers mistaken and unauthorised payments) to ensure there is no overlap in remit and obligations.		Agreed / To discuss

s 22



Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
s 22			
<i>Penalties and redress</i>			
Strong penalties for breaches of the CCA	<ul style="list-style-type: none">• Civil penalties for non-compliance in the overarching legislation would be set at the same level for other breaches of the CCA, namely the greater of:<ul style="list-style-type: none">- \$50 million- three times the value of the benefit obtained, or- 30 per cent of the corporations adjusted turnover during the breach.• Other remedies (such as non-party redress, mandatory injunctions etc.) and powers, including information gathering and investigative powers, would also be available to the ACCC to ensure compliance.		Agreed / To discuss
Consistent penalties for breaches of the sector-specific codes	<ul style="list-style-type: none">• Penalties for breaches of the sector-specific codes would be consistent across regulators.• This would ensure that all businesses in the scams ecosystem would face the same maximum penalties for non-compliance. Different penalty regimes or instances where penalties are weaker than others may create gaps in enforcement which scammers could target.		Agreed / To discuss

Key feature (Treasury preferred)	How it would operate	s 22	Agreed / To discuss
	<ul style="list-style-type: none">• Treasury will test this approach with stakeholders during consultation or whether to introduce sector-specific penalties that is tailored to the nature of harm.• Regulators would not be expected to respond to or undertake enforcement action on each individual complaint or breach of the code. As per usual enforcement processes, it would be up to the regulator if and when they take enforcement action, however, they would be expected to take action for significant breaches and systemic issues.		
A mechanism to determine redress and reimbursement of funds for breaches by a bank	<ul style="list-style-type: none">• An external dispute resolution (EDR) mechanism (such as through AFCA) to determine redress and reimbursement of funds to a consumer where a bank has breached its obligations under the sector-specific code.• Developing and implementing a multi-sector EDR scheme would be complex and time consuming, and would be a future consideration.• Clear obligations on businesses and strong penalties in the Framework will provide incentives for businesses to reduce scam losses, and the need for a multi-sector EDR scheme would be considered at a later stage.		Agreed / To discuss

Table 2: Examples of obligations in a sector-specific code (to be informed through stakeholder consultation)

Sector	Key vulnerabilities in the sector	Examples of specific obligations
Banking	<ul style="list-style-type: none">• Bank transfer remains the most reported payment method for scams with 13,098 reports totalling \$210.4 million in 2022.• Frictionless and instant payments has made it harder for consumers to identify a scam and recover funds where they are a victim of a scam.• Payments in Australia only match BSB and account numbers. This facilitates scam payments where the account name provided by the scammer differs from the real account name, and occurs in email compromise scams and some investment scams.	<ul style="list-style-type: none">• A bank must include warnings to customers when they are making a bank transfer sufficiently different from their normal activity.<ul style="list-style-type: none">- A phone call by the bank is more likely to be required when increasing daily transfer limits immediately precedes a transaction.- Additional steps must be taken if the customer is identified as having a higher propensity to be a victim of a scam.• A bank must act on information it receives that identifies an account is likely to be or is a scam account. This could include closing the account or locking the account until it is verified by the bank as being legitimate.• A bank must implement processes to improve the checking of the account name (payee), BSB and account number when a customer transfers funds.<ul style="list-style-type: none">- In addition to this, sending banks must check recipient accounts against known or suspected scam accounts within AFCX data, and not send money if that is the case.• A bank must take reasonable steps to reduce the level of ‘money mule’ activity by taking additional steps to authenticate the identity of an applicant or customer that opens an account.

s 22

SCAMS CODE FRAMEWORK – FLOWCHART OF KEY FEATURES (TREASURY-PREFERRED OPTION)

OVERARCHING FRAMEWORK

Examples of principles-based obligations

Prevention

- Entities must take robust steps to prevent misuse of services, platforms, or marketplaces by scammers.
- Entities should provide consumers with information about how to identify and avoid scams.

Detection and disruption

- Entities must seek to verify, trace and block scams from initiating contact with consumers.

Response (obligations to consumers)

- Entities must have effective, efficient, and accessible complaints handling and redress processes.

Competition and Consumer Act 2010 – ACCC to regulate and enforce

- s 22
- Principles-based obligations, including anti-scam measures for vulnerable cohorts and processes for internal dispute resolution
- s 22
- Power for sector-specific codes to be developed in legislative instruments
- Anti-scam strategy to be developed by entities
- Information sharing and reporting obligations for entities
- Information sharing arrangements for regulators
- Penalties for breaches of principles-based obligations and other requirements

s 22

SECTOR-SPECIFIC

Legislative Instrument – Banks (Tsy portfolio Minister)

- Sector-specific codes for banks including consideration for vulnerable cohorts, such as:
 - Banks to introduce ‘friction’ in bank transfers, such as warnings for consumers when making unusual payments
 - Banks to verify payee information in addition to BSB and account numbers
- Treasury to develop

Australian Securities and Investments Commission Act 2001 – ASIC to enforce sector-specific codes for banks

- Reporting obligations for banks
- Information sharing arrangements for regulators
- Penalties for breaches of sector-specific codes

Redress

- A mechanism (e.g. AFCA) to determine redress / reimbursement of funds to a consumer where a bank has breached its obligations under sector-specific codes

s 22

Scams Code Framework – Proposed obligations on regulated businesses

PRIMARY LEGISLATION (ECOSYSTEM-WIDE)

Competition and Consumer Act (CCA)

Prevention

- Take robust steps to prevent misuse of its services by scammers.
- Provide consumers with information about how to identify and avoid scams consistent with the messaging of the NASC.
- Implement anti-scam systems which are responsive to new products, services, designs, technologies, and delivery channels.
- Provide training to customer-facing staff on scam detection, response processes and customer support.

Detection and disruption

- Seek to verify, trace and block scams from initiating contact with consumers.
- Take reasonable steps to act on scam intelligence shared with it by another entity (such as the NASC).
- Provide consumers with tools to verify information in real time.
- Warn consumers that they may be the target of a scam (if intelligence reflects this).

Response (obligations to consumers)

- Provide reporting options for customers and users, including people not directly targeted by a scam to be able to report a scam.
- Have user-friendly, effective, efficient, and accessible complaints handling and redress processes.
- Respond to reports from customers or the community of a scam involving the entity or assuming the identity of the entity.
- In response to complaints and reports, provide clear information on action/s taken, the basis on which decisions were made, outcome/s and next steps, including dispute options.

Reporting (obligations to regulators, other businesses)

- Take reasonable steps to notify other entities and the National Anti-Scam Centre (NASC) promptly of intelligence about suspected or identified organised large-scale scam activity.
- Share data and information on the incidence of scams, and action taken in response, with industry bodies, law enforcement and regulators, including the National Anti-Scam Centre.
- Keep records of incidence of scams and action taken in response.
- Respond within 28 days to a report request from the ACCC.

Anti-scam strategy

- Each entity must have in place an anti-scam strategy that would set out and have further detail on:
 - the processes the entity will take on how it will comply with the sector-specific obligations, including a detection and disruption plan using intelligence sharing mechanisms
 - the governance and accountability mechanisms the entity will use to track progress and compliance
 - periodic reviews of the strategy
- Entities must provide their anti-scam strategy to the ACCC. The ACCC may provide further guidance on best practice to meet the sector-specific obligations and work with entities to ensure their anti-scam strategies are fit-for-purpose.

s 22

CCA REGULATIONS

Banks (Assistant Treasurer to approve)

- Take reasonable steps to authenticate and verify the identity of an applicant, customer or payee information, to reduce 'money mule' activity and payments to scam accounts.
- Take reasonable steps verify a transaction is legitimate where a customer undertakes activity sufficiently different from their normal activity.
- Have in place methods to detect high-risk transactions and take appropriate action to warn the customer, block or suspend the transaction, or other measures to reduce scam activity.
- Have user-friendly and accessible methods for customers to immediately take action where they suspect their accounts are compromised or they have been scammed (e.g. an in-app 'freeze switch').
- Assist with tracing and recovery of transferred money to the extent funds are recoverable.
- Act quickly on information that identifies an account or transaction is likely to be or is a scam.

s 22

Banks

TBC

NON-CCA STANDARDS

A14: Scams Code Framework

Market Conduct and Digital Division

Talking points on Proposal

- Option 1 will implement our election commitment to introduce tough new industry codes for scams.
- It will allow the Government to set principle-based obligations in 2024 for sectors that are part of the scams ecosystem, and more specific minimum standards for the most critical sectors: banking, telecommunications, and digital communications platforms.



**The Hon Stephen Jones MP
Assistant Treasurer and Minister for Financial Services**

**The Hon Michelle Rowland MP
Minister for Communications**

MEDIA RELEASE

Select date

Consultation on next steps for the Government's anti-scam agenda

Today the Albanese Government has commenced public consultation on our commitment to introduce new, mandatory industry codes for the private sector to combat scams.

The proposed Scams Code Framework is the next stage in the Government's ambitious agenda to tackle the scourge of scams, which cost Australians over \$3.1 billion last year.

Government, regulators, and industry have a mutual interest in making sure scams are identified and stopped before they can harm Australian consumers and businesses.

The proposed Framework would set clear roles and responsibilities across the scams ecosystem, with an initial focus on banks, telecommunication providers and digital communications platforms, to make Australia a harder target for scammers.

The proposed Framework would introduce minimum, consistent obligations for all regulated businesses to prevent, detect, disrupt, and respond to scams. This would be complemented with sector-specific obligations that are tailored to the role of each sector in the scams ecosystem.

Regulated businesses would be expected to have robust measures in place to address the risk of scams on their services. Strong penalties would apply if businesses fail to comply with their obligations.

The discussion paper released today seeks feedback on:

- the design, structure and scope of the proposed Framework
- proposed obligations for regulated businesses to prevent, detect, disrupt and respond to scams, including in the sector-specific codes
- requirements for regulated businesses to develop and maintain an anti-scam strategy
- improving reporting and information sharing arrangements
- establishing clear complaints handling and dispute resolution pathways for consumers
- the role of the regulators that will monitor and enforce the Framework.

The consultation paper can be found on the Treasury [website](#). Individuals interested in participating in the consultation, but who do not wish to make a formal submission, can complete a five-minute survey available [here](#).

Submissions to the consultation and the survey will close on **29 January 2024**.

Ends

The requirement for a media release should be agreed with the relevant Ministerial Office before drafting commences. Requests for media releases should be forwarded to Treasury's Media Unit who will liaise with the press office on your behalf. Where a media release is requested, the Media Unit will work with you to draft.

Policy areas are required to check facts and provide final approval of all media releases.

The Media Unit can be contacted via s 22 [REDACTED].



Scams – Mandatory Industry Codes

Consultation paper

November 2023

^ This is a basic consultation paper cover for general consultations or draft documents. For a cover with an image, **Insert>Cover Page** and select **Cover_with photo** from the drop down menu. This is a placeholder image only, contact the Creative Services Team (creativeservices@treasury.gov.au) to obtain a custom image for your consultation.

Notes to participants
[Enter advice to participants if appropriate, otherwise delete box.]

© 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 comments](#)..... 3
- [Proposed Scams Code Framework](#) 4
- [Introduction](#) 4
 - [Current approaches to addressing scams](#) 4
- [Objectives and key principles](#) 6
 - [Key guiding principles](#) 6
- [Key features of the proposed Scams Code Framework](#) 8
 - [Figure 1. Proposed Scams Code Framework](#)..... 8
 - [Definitions](#) 9
 - [Principles-based obligations](#) 11
 - [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-compliance](#)..... 22
 - [Penalties for non-compliance](#)..... 23
- [Appendix A – List of stakeholder questions](#) 24
- [Attachment B – International developments](#)..... 27

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 email to scampolicy@treasury.gov.au. For accessibility reasons, please submit responses via email 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**

Email	scampolicy@treasury.gov.au
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.

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
- provide clear pathways of support and complaints handling for those who have been affected by scams

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

- 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:

- the Government's response to the competition and consumer recommendations made by the ACCC in its September 2022 interim report of the DPSI
- 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.

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

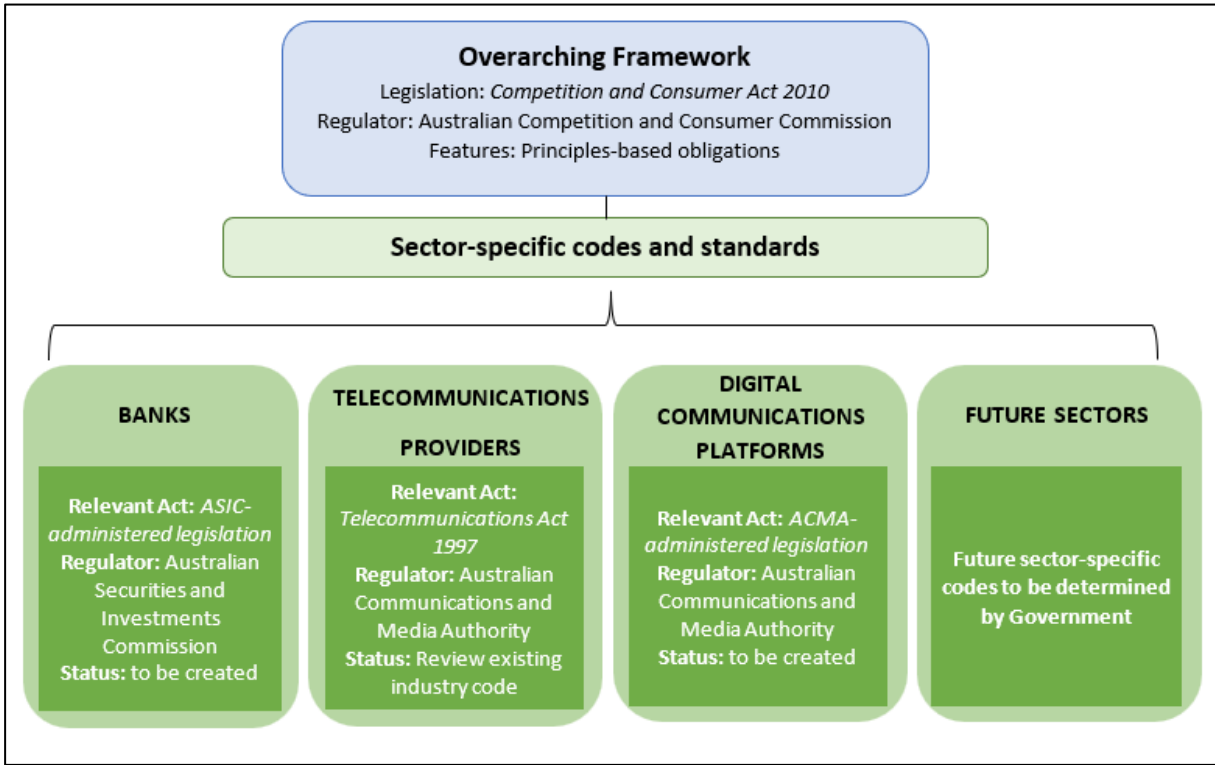
The implementation of the Framework is subject to future Government decisions, and legislative design and development. References to amending existing legal frameworks are demonstrative of policy intent only. The focus of this paper is to seek feedback on the proposed key features and obligations that 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 Scams Code 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 intended to cover the types of scams identified by the ACCC under its *Targeting Scams* report,

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.

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


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?

[licensing of payment service providers – payment functions.](#)

- 
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).
- In response to consumer scam reports and complaints, a business must provide clear information on action taken, the basis on which decisions were made, outcome and next steps, including escalation and dispute resolution options. Where a consumer escalates concerns with a business, they should be dealt with fairly and promptly.

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:

24. 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?

25. 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?

26. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?

27. 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.

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

- 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 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:

28. 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?
29. 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?
30. 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?
31. 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 SMS 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:

32. Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?
33. Are there additional obligations the Government should consider regarding the individual sector codes?
34. Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?
35. Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?
36. 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?
37. 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?
38. 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?
39. 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?
40. 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, penalties for non-compliance would 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:

41. 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?
42. Are there other factors the Government should consider to ensure a consistent enforcement approach?
43. 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 Scams Code 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 B – 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.²⁰The 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.

KEY POINTS

s 22



- Attachment B outlines, and seeks your agreement to, proposed design elements of the Framework, including:
 - principles-based obligations that focus on regulated businesses preventing, detecting, disrupting and responding to scams
 - sectors initially within scope of the Framework (banks, telecommunication providers, and social media and advertising technology (ad-tech) services)

s 22



- This streamlined Framework would:
 - implement the Government’s commitment for mandatory industry codes

s 22

- Some stakeholders may perceive the Government as walking back on previous support for mandated dispute resolution and consumer redress mechanisms, and may expect Government to commit to a timeframe for legislating a dispute resolution regime. This risk could be mitigated by including a principles-based obligation in the Framework for consumer reporting and internal complaints handling mechanisms.
- Similarly, the Framework would not introduce detailed obligations for other technical features canvassed during consultation, including compliance reporting, information sharing, and anti-scam strategies.
 - Stakeholder feedback highlighted the significant complexity and sensitivity of these features, and the different regulatory approaches required for the diverse sectors regulated under the Framework.
 - We propose to streamline these features into the Framework’s principles-based obligations, with more prescriptive requirements to be included in sector codes.

s 22



Clearance Officer
Tony McDonald
Assistant Secretary
Market Conduct and Digital Division
16 February 2024

Contact Officer
s 22
Director
s 22



ATTACHMENTS



B: Stakeholder feedback on consultation and proposed policy positions



Industry actions

- Respondents supported the need for greater industry accountability to address scams but were less supportive of business measures that raised consumer costs, frictions, or privacy risks.
- Respondents suggested ideas to improve access to reporting, improve account authentication and verification and information sharing, and sector-specific obligations, including for:
 - Banks to improve methods to create and verify new accounts, and improve processes to recall user funds, with mixed views on the appropriateness of payment friction.

s 22



8. Will the Framework require banks or other sectors to compensate scam victims?

- The Government is considering the stakeholder feedback it received on complaints handling and dispute resolution mechanisms under the proposed Framework.
- It is important that any complaints handling, and dispute resolution processes operate coherently across the scams system.
- This may require regulated businesses to strengthen protections against scams through processes for receiving consumer scam reports, complaints handling, and internal and external dispute resolution.
- The Government is considering whether regulated businesses should be required to provide redress to consumers where they have not met their obligations under the Framework.

s 22



Attachment C – Talking points

s 22



- Without Government action to lift industry standards across the scam ecosystem, there is likely to remain incremental and inconsistent action – or even continued resistance from some sectors to acknowledge the importance of their role in preventing scammers.

s 22



- The Scams Code Framework is the most significant element of the Package, and appropriate resourcing will ensure robust action by regulators to hold the private sector to account for the obligations that will be established to protect Australians.

s 22



- Access to redress is an important feature for consumer advocates. I do not consider that international approaches of ex-ante liability allocation create effective incentives across the whole scam ecosystem to align responsibility for protections and liability for losses.
 - The Framework includes an obligation that all regulated entities participate in a recognised external dispute scheme. I intend to have a workable interim solution, utilising existing schemes where possible in the first instance.



Australian Government
The Treasury



Ministerial Submission

MS24-000756

FOR ACTION - Scams Framework - Policy Update and Next Steps

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP

CC: Treasurer - The Hon Jim Chalmers MP

s 22



Recommendations

s 22



- That you **agree** the recommended approach for consumer redress, which involves the exposure draft legislation setting up the architecture for external dispute resolution (Attachment B).



Agreed / Not agreed

s 22



Signature

A handwritten signature in black ink, appearing to be 'Alfred', written in a cursive style.

Date: 9/5/2024

KEY POINTS

s 34(3)

Policy positions for the Framework

- Treasury recommends key policy positions outlined at Attachment A to establish the Framework,^{s 34(3)}
 - The principles-based approach for the design of obligations under the Framework will allow flexibility to accommodate differing activities that may be regulated under the Framework over time and allow regulation to respond to scam threats without requiring legislative amendments.
 - : Stakeholders may raise concerns regarding lack of detail in the legislation and uncertainty on how the principles apply to their business.

s 22

External dispute resolution

- Treasury has developed an approach for consumer redress, following your feedback on MS24-000215.
 - We recommend the primary legislation for the Framework establish the obligation for regulated businesses (including relevant digital platform service providers) to be a member of a prescribed external dispute resolution (EDR) scheme.
 - Sector-specific EDR schemes would be prescribed in the sector codes.

- For the initial sectors under the Framework, Treasury recommends using existing EDR schemes, meaning consumers would have access to EDR from the commencement of sector codes (subject to any transitional arrangements).

s 22



s 47C, s 47E(d)



s 22



Clearance Officer
Tony McDonald
Assistant Secretary
Market Conduct and Digital Division
3 May 2024

Contact Officers
s 22



s 22



ATTACHMENTS

A: Policy implementation

B: External dispute resolution

s 22

~~PROTECTED//CABINET~~

Attachment B – External Dispute Resolution

- Following feedback received from stakeholders in response to the consultation paper on the proposed Scams Code Framework and your feedback on MS24-000215, Treasury has developed the following approach to delivering EDR.

New EDR arrangements under the Framework

Legislation

- The primary legislation for the Framework to set up the architecture for EDR. This would involve requiring regulated businesses, including digital platform service providers (DPSPs) to be a member of a prescribed EDR scheme.

s 42

s 22

Sector codes

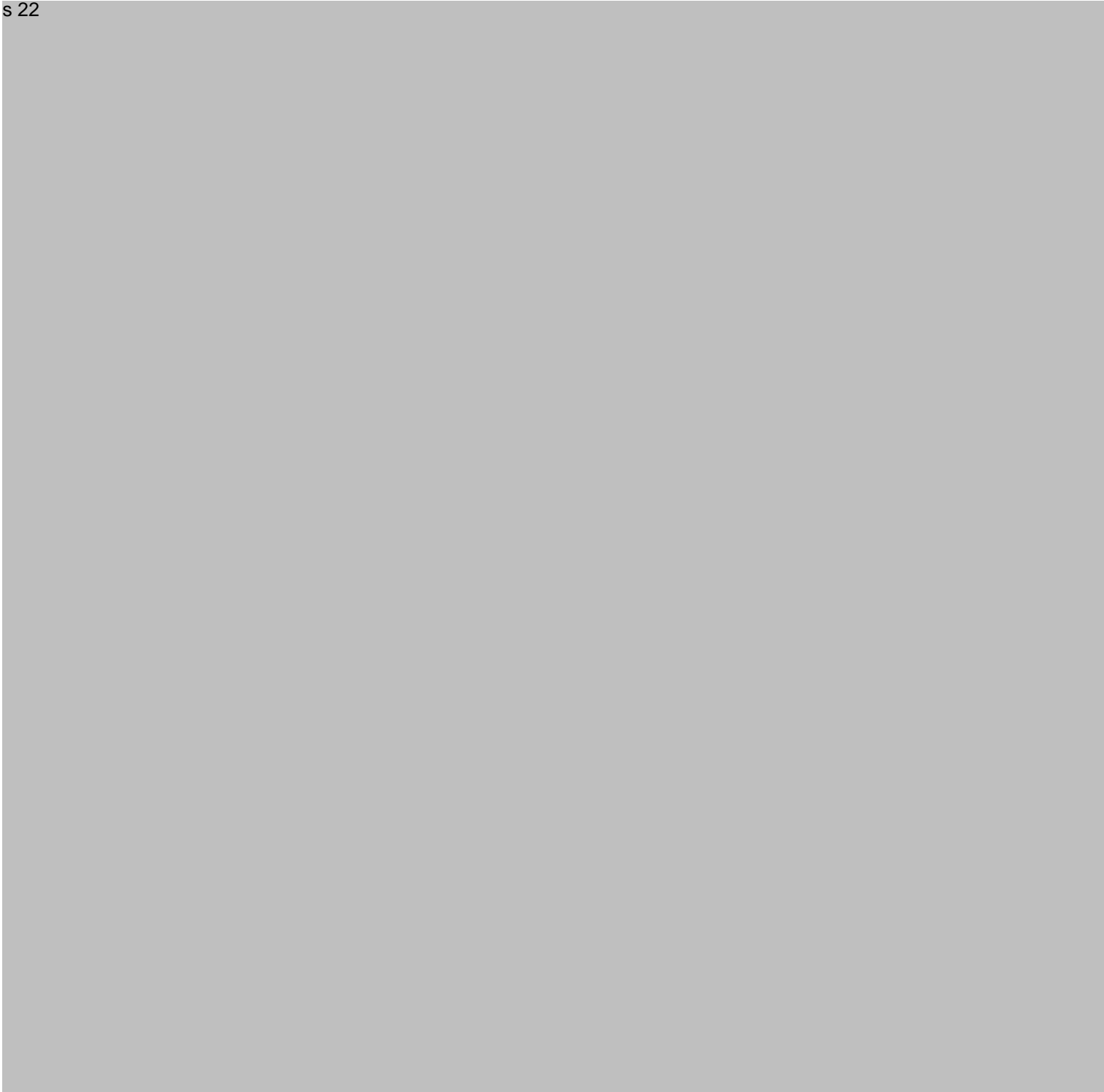
- Sector codes would, among other things, prescribe the specific EDR scheme that businesses are required to be a member of.

s 22



- To the extent banks and telecommunications providers are already subject to EDR requirements, consumers would still be able to access EDR prior to the commencement of the sector codes in relation to the requirements in the primary legislation.





- The Government has committed to introducing industry codes to make social media companies, banks and telecommunications providers responsible for reducing the prevalence of scams.
- Codes could help clarify accountabilities and promote consistent consumer protection across the scams landscape.



- On 20 April 2023, ASIC released *Report 761: Scam prevention, detection and response by the four major banks*, which found:
 - scams strategy and governance was variable across the banks, and overall less mature than expected

- the banks had inconsistent and narrow approaches to determining liability, with bank customers overwhelmingly the bearer of scam losses (96 per cent of total scam losses across the banks)
- banks' detection and stopping of scam payments had gaps and inconsistencies, with banks collectively detecting and stopping only about 13 per cent of scam payments
- banks' reimbursement and/or compensation to victims ranged from two to five per cent; at the three banks for which data was available, only around 11 per cent of scam loss cases were reimbursed or compensated
- steps taken by banks to help prevent customers fall victim to scams varied across banks (although there were examples of emerging good practice).

SCAMS

Headline Statement

- The Government is delivering its commitment to combat scams and online fraud, with an approach focused on strong public-private collaboration, and the development of a new Scams Code Framework.

Key Points

- The Government has committed to introduce new mandatory industry codes to outline the responsibilities of the private sector in relation to scams.
 - Treasury undertook public consultation on a draft Scams Code Framework, which would introduce new responsibilities for banks, telecommunications companies and digital communications platforms in relation to scams, from 30 November 2023 to 29 January 2024.
 - Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) are currently considering stakeholder submissions and survey responses.

s 22

Policy Commitments

Scams Code Framework

- On 30 November 2023, Treasury and DITRDCA released a public consultation paper and survey to seek feedback on a proposed model for a Scams Code Framework, with consultation closing on 29 January 2024.

Contact Officer:

Name: s 22
Division: Market Conduct and Digital Division
Telephone: s 22
Last updated: 25/01/2024 11:06:00 AM

- The Framework would set mandatory obligations for banks, telecommunications companies, and digital communications platforms to address scams delivered over their services.
- The proposed model would also require these businesses to develop a strategy to address scams in their business, and have measures in place to prevent, detect, disrupt and respond to scams.
- Where a regulated business does not meet its obligations under the Framework, clear dispute resolution pathways would ensure consumers have access to appropriate redress, such as compensation for scam losses. This would be complemented by regulator enforcement action and penalties for non-compliance.

Background

Scams Code Framework – targeted consultation

- Treasury and DITRDCA have met with a range of stakeholders as part of consultation on the Scams Code Framework, including through consultation roundtables and bilateral meetings. This has included meetings with the following sectors:
 - Banking sector: the Australian Banking Association (ABA) and the Customer Owned Banking Association (COBA) and their respective members

s 22

Scams-related work in the banking sector

- On 24 November 2023, the ABA and COBA launched the ‘Scam-Safe Accord’ as a sector-wide agreement for members to implement measures that disrupt, detect, and respond to scams over 2024 to 2025.
 - Treasury is considering this and other industry developments as part of its work on the Scams Code Framework.

s 22