Australian Government
The Treasury

Impact Analysis
Scams Prevention Framework

October 2024

treasury.gov.au

Manager
Media 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

Executive summary

Scams are a growing issue in Australia inflicting significant harms on Australians. There are a range of impacts of scams including harms to consumers, reputational damage for businesses, withdrawals from the digital economy and undermining public trust.

Current industry initiatives lack a coordinated cross-sector approach to protect Australians from scams. Without government action, industries providing services that are vectors of scam activity are unlikely to be sufficiently incentivised and coordinated to respond to the rising cost of harms from scams.

The core objectives of the government's policy response would be to both reduce scam harms and align the benefits and costs of scam prevention. These objectives are supported by secondary goals to uplift industry actions to prevent, detect, disrupt, and report scam activity and to better support Australians who experience a scam.

Treasury has considered two options:

- Option 1: Maintain the status quo.
- Option 2: Establish the Scams Prevention Framework (SPF), implementing the Government's election commitment to introduce a mandatory framework for industry codes on scams initially applying to banks, telecommunications providers and certain digital platforms.

Option 2 would involve regulatory costs for banks, telecommunications, and certain digital platforms to uplift their anti-scam activities, information sharing and dispute resolution capabilities. Option 2 has been assessed as likely to involve a net benefit through reducing scam exposure, losses and redress. The SPF would improve the regulatory framework for industry scam prevention activities, improve sharing of actionable scam information across the economy and improve dispute resolution systems and outcomes for scam victims.

Treasury undertook public consultation on policy options from November 2023 to January 2024. Targeted consultation with industry continued in mid-2024 and draft legislation underwent public consultation from September to October 2024. Consultation has informed the design of the SPF under option 2 as well as the level of regulatory burden it would involve.

Option 2 is the preferred option to implement the government's objectives to both provide benefits in reducing scam harms and improve the alignment of the costs and benefits of scam prevention activity. Implementing the SPF is preferable to the status quo, under which there would not be an overarching framework to enable uplift in industry's scam prevention activities.

The SPF would be implemented through legislating a framework for industry codes, designating relevant services of banking, telecommunications and certain digital platforms, and developing sector codes to prescribe further specific obligations.

Upon implementation the SPF would be evaluated by the government through several measures using data from government and industry sources. These include consumer and industry reports about scams, agency monitors of consumer victimisation and evaluation of industry compliance with mandatory obligations.

Background

Scams are a significant source of financial crime that inflict unacceptably high harm to Australian consumers and industry. Scams target a wide range of people by exploiting the social and technological vulnerabilities in the way Australians interact and do business online. Scams are often linked to other crimes, including identity theft and cybercrime.

Scams are attempts, directly or indirectly, to deceive a consumer into obtaining financial benefits or personal information. The scope of 'scam' activity is not currently defined in legislation. Most scams aim to induce an individual to act to initiate payments to the scammer or disclose account or security credentials. Scams can be carried out through a wide range of communication channels, including phone, text message, social media, and email.

In response to the rising impact of scams, the Government made an election commitment to introduce tough, new mandatory industry codes for banks, telecommunication providers and social media companies to combat scams. Policy options considered in this Impact Analysis (IA) would build on $58 million in funding to launch the National Anti-Scam Centre (NASC) on 1 July 2023.[1] The NASC co-ordinates efforts to prevent scams by improving intelligence sharing across Government and the private sector, raising public awareness about scams and making it easier for consumers to report scams to a single agency. These efforts have contributed to a 13 per cent annual decrease in scam losses in 2023, the first downward trend since combined reporting on scam losses began in 2015.

At the 2024-25 Budget, a draft version of this IA was provided to inform a Budget decision on developing mandatory industry codes for regulated businesses to address scams on their platforms and services. Subsequently, a full IA was developed alongside finalisation of policy, informed by public consultation on the draft legislation in September 2024, to support the Government's final policy decision in October 2024.

1 Budget 2023-2024, *Budget Paper No. 2 – Budget Measures*, page 211.

1. Policy problem

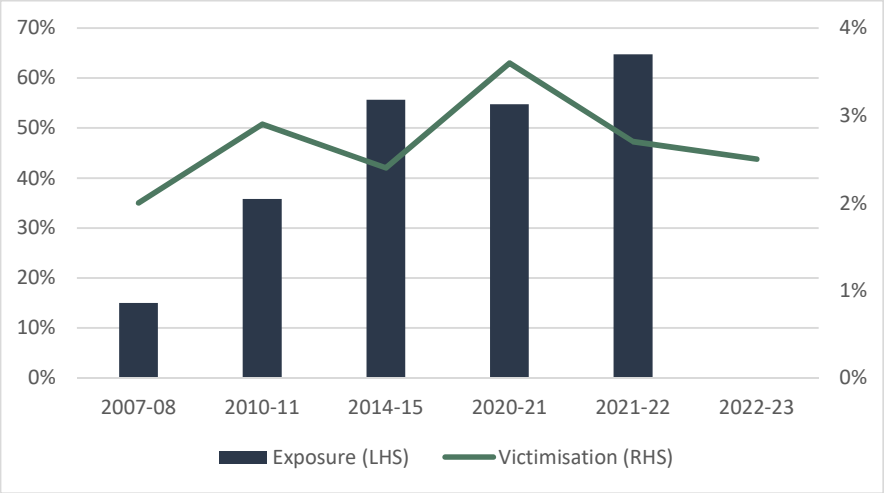
1.1 Scams are a significant issue of growing concern

1.1.1 The recent growth in scam activity

The impact of scams on Australians has risen sharply and has accelerated since 2020. High-value losses, driven by the growth in investment scams, have led to billions being stolen from Australians, peaking at $3.1 billion in 2022.[2] Most, if not all Australians, have been targeted by a scam attempt.

The Australian Bureau of Statistics (ABS) has periodically surveyed Australians in the Personal Fraud report (see Chart 1) to estimate the annual incidence of scam exposure and victimisation.[3] ABS figures estimate that 2.5 per cent of Australians (514,300) were victimised by a scam in 2022-23, only slightly higher than the rate of 2.0 per cent in 2007-08. Scam exposure rates have risen from 15 per cent in 2007-08 to 65 per cent of the population in 2021-22.[4] Australian Institute of Criminology (AIC) surveys that found 13.6 per cent of those surveyed were scammed in their lifetime, and 3.6 per cent were scammed in the year 2023.[5]

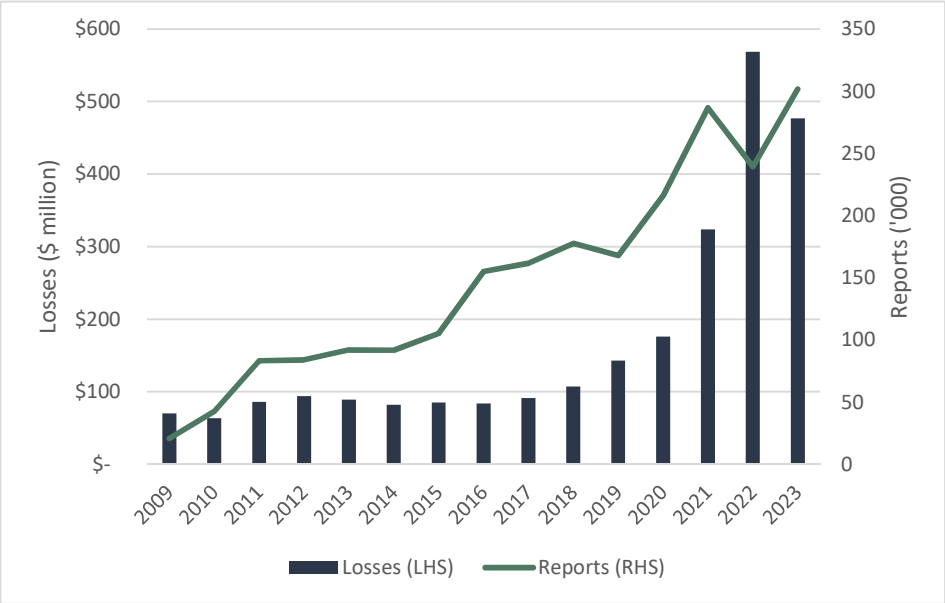
Chart 1 - Exposure to scams[6]



The increasing prevalence in scams is also shown in the rapid rise of reports through reporting portals including Scamwatch. Scamwatch reports provide details on a scam from individuals who have encountered or been affected by a scam, allowing the Australian Competition and Consumer Commission (ACCC) and the NASC to co-ordinate responses. Although reporting of scams to Scamwatch has steadily risen over time, annual losses abruptly increased from 2020 (see Chart 2). Australians have reported over 164,000 scams totalling $160 million losses in the year to September 2024.[7]

2 ACCC, *Targeting Scams* 2022
3 Data attempts to measure the impact of scam attempts through exposure and victimisation rates. Exposure to scams includes all incidences where a scammer uses a contact method to target a consumer, regardless of its impact on them. Victimisation rates only capture experiences of scams where the victim has been defrauded and experienced a loss.
4 ABS, *Personal Fraud, 2022-23*, 20 March 2024. A person was considered to have been exposed to a scam if they had received an unsolicited invitation, request, notification or offer, and read, viewed, or listened to the material.
5 AIC, *Cybercrime in Australia 2023*, 27 June 2023 p. 30-32
6 ABS, *Personal Fraud, 2022-23*, 20 March 2024
7 ACCC, Scamwatch online data dashboard

Chart 2 - Consumer reports to Scamwatch[8]



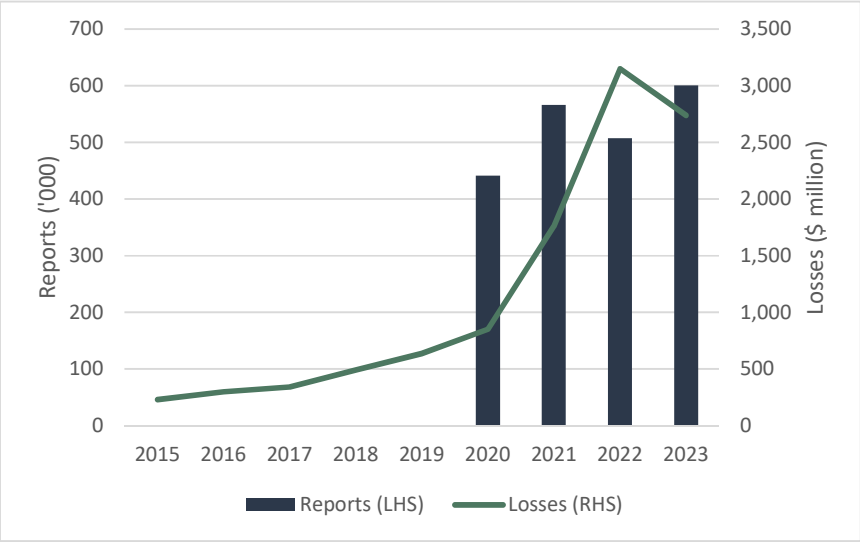
In 2023, business made 4,933 scam reports to Scamwatch, an increase of 27.9 per cent from 2022.[9] Scams on businesses resulting in the most losses involved false billing and investments. Of the $29.5 million in reported scam losses for businesses $17.3 million were reported by small and micro businesses.

In recent years, the information sharing infrastructure of the ACCC has been enhanced to enable reporting on 'combined' figures from consumers and industry. This includes data sourced from Scamwatch, ReportCyber, the Australian Financial Crimes Exchange (AFCX), IDCARE, and the Australian Securities and Investments Commission (ASIC).

Combined data shows a consistent trend with Scamwatch reports, depicting a rapid rise in losses from 2020 as shown in Chart 3. Annual reported losses to scams made by Australians increased from $634 million in 2019 to $1.8 billion in 2021, and further increased to a peak of $3.1 billion in 2022.[10] In 2023, reported scam losses declined for the first time since 2016 to $2.7 billion. Although, expanding combined reporting infrastructure could be impacting the growth in figures.

8 ACCC, Scamwatch online data dashboard
9 Ibid.
10 ACCC, *Targeting Scams*, 2023

Chart 3 - Combined industry and consumer reports[11]



In 2023, Australians made over 601,000 reports about scams to combined data sources, including 302,000 reports to Scamwatch. In the 29,000 reports to Scamwatch involving losses to a scam, the average loss was $16,000 and the median was $500.[12] The largest reported losses and the driver of growth in scams are largely from investment scams, which form around half or $1.3 billion in combined losses. Individuals often lose their entire savings or have their accounts drained from investment schemes. The median loss is much lower than the average as many of the more reported scam types, including phishing or buying and selling scams, are lower, one-time fraudulent payments.

1.1.2 Scams inflict a broad range of harms

While not quantifiable, ongoing trends of elevated losses to scams arising from insufficient consumer protections and inconsistency in industry approaches can cause broader societal costs.[13] Beyond the financial losses, scams can have a devastating impact on victims' lives, causing significant psychological, emotional and social distress to the individual and their families. The prevalence of scam activity also reduces confidence in digital commerce, communication and government authorities. A selection of these and broader costs are outlined in Table 1.

Table 1 – Broader impacts inflicted by scams

Personal	• The increased need for diligence and caution by consumers imposes costs for individuals, including through the time to assess or verify legitimacy of sources. These self-imposed costs by consumers add to frictions industry puts in place to prevent scam activities. Heightened diligence and caution could also drive withdrawals of participation in the wider digital economy. • The prominence and frequency of exposure to scams attempts on communications platforms such as social media, chat services and telecommunications inflict nuisance costs on individuals. These exposures to scams result in wasted time and effort by individuals. • Australians invest in personal administrative or external security measures to help them avoid falling victim to a scam. This may include the time and cost

11 ACCC, Targeting Scams, 2015 to 2023 reports. Combined figures for the number of consumer reports are not comparable prior to 2020 due to changes in data sources and methodology.
12 ACCC, Targeting Scams report 2023.
13 International Public Sector Fraud Forum, *Guide to Understanding the Total Impact of Fraud,* 2023.

	involved in considering changing service providers, establishing alternate contact details, or changing how they manage their banking to minimise the potential for scam activity. • Losses from scams inflict emotional, and psychological impacts upon victims, potentially creating long-term burden and costs. Financial losses to scams reduce the financial independence and wellbeing of victims. • Those affected by a scam may face the resulting additional time, cost and psychological burden associated with seeking support to recover. This arises from a lack of clarity on responsibility for industry to respond to reports of scams and provide support to victims.
Business	• Scams can create financial and reputational risks for businesses. Businesses that provide services which are vectors of scam activity may choose to invest in systems or processes to minimise the exposure of their brand or may otherwise need to devote additional resources to rebuild public trust. • Businesses which are vectors of scam activity or that are impersonated by scammers may suffer loss of revenue as consumers disregard legitimate dealings or look to minimise risk by avoiding interacting with them.
Broader economic	• Managing scam-related risks requires industry to absorb greater costs, staffing and resources into detecting, investigating and responding to scams, affecting competitiveness. Some of these costs may be passed onto consumers through higher prices. Activities to reduce the harm of scams impose inefficiencies for economic activity. • The frequency of scam activity can change consumer behaviour or create inefficiencies in digital transactions. • If costs of managing scams are inequitably distributed across the scams ecosystem, it may result in inefficient allocation of capital or labour across the economy and detract from productivity outcomes. • The erosion of trust in digital interactions damages the reputation and economic standing of impersonated businesses or government agencies, potentially unwinding efficiency of digital interactions and if not addressed may lead to withdrawal from digital technology by parts of Australian society.
Security	• Scams often intersect with other fraud and cybercrime offences, including data breaches and identity theft. The increased proliferation of scams affects the privacy and information security of businesses and their consumers.
Social	• The behaviour of scammers acts to undermine public trust in the brands and services which are being impersonated or co-opted by the scam, causing inefficiency and reducing confidence in online commerce and digital communication. • Scams may lead to risk aversion or undermine trust and confidence in essential functions of the economy, including the reliability of communications and transactions and the capacity of industry and government to protect consumers.
Government	• Government revenue collection and expenditure required to deliver programs may be impacted due to distrust of government communication channels and institutions.

- The erosion of trust damages the reputation of impersonated businesses and government agencies which, if not addressed, may lead to withdrawal of digital technology from government administration.

Inaction to combat scams will see these problems increase over time, with consequential increases in the cost and time required to rectify them in the future.

1.2 Drivers of scams

Australia, as with many other countries, is experiencing spikes in losses. A list of several underlying factors as to why this has occurred is outlined in Table 2. This section examines some of these factors in detail below.

Table 2 – Drivers of recent growth in scam losses

Drivers of recent scam losses	
Cybersecurity threats	As more data is collected about consumers, high-profile data breaches and cyber threats have compromised consumer security and personal details that can be used by malicious actors to target scam victims and carry out scams.
Increased digitalisation of the economy	The pandemic created abrupt shifts across the economy towards remote work and communication, leading to increased uses of digital services in ways that were unfamiliar or at a far higher rate than before. The efficiency gains and speed of transactions, from communication to payments channels, have enabled significant acceleration of interactions between parties.
Use of crypto and digital assets	The emergence and increasing uptake of unregulated digital assets such as cryptocurrencies, unfamiliar to many consumers and of increasing interest to others, has been exploited by scammers as an exit channel to direct funds out of the control of the victim.[14]
New technologies	Scammers have become increasingly sophisticated in their efforts due to the take up of newer technologies at their disposal, such as chat bots and artificial intelligence, that allow them to impersonate legitimate entities with far greater accuracy and deploy communications to a wide audience.[15]
Economic pressures	Economic pressures during and after the pandemic have led to greater financial pressure on consumers, increasing the panic of responses to scam demands for unpaid fees or the allure of profiting from scam investments.

1.2.1 Growth of low-cost frequent consumer contact

Low barriers to entry and costs to initiate digital communication and commerce (including via online and social media) allow scammers to initiate direct consumer contact at high frequency. The high volume and prevalence of unsolicited offers or communication from scammers works on the basis that

14 ACCC, *Targeting Scams 2021*, p. 1, 27, 69
15 ACCC, *Targeting Scams 2022*, p. 14

a proportion of those targeted will pursue the illegitimate offer. Scam tactics can be seen as lucrative activity for criminals as they succeed due to these high volumes of communications creating many opportunities propagating illegitimate offers.

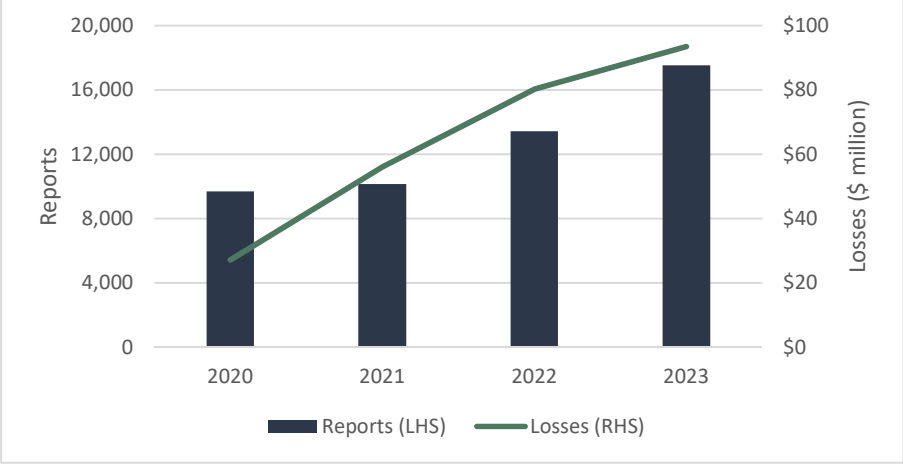
Growing use of digital communication and media channels by industry and governments have generally not been supported by robust and readily available means for the public to validate the identity and legitimacy of the source, or to authenticate commerce offers. Requirements for customer identity validation, such as those which exist in the financial sector, are not universal in all sectors. Consumers also lack easy methods to verify whether communications are from a legitimate business or a scammer.

The 2023 Scamwatch consumer reporting data[16] provides information on the major channels used by scammers including:

- contact methods most commonly reported were text message (36 per cent), email and phone.
- contact methods most frequently associated with financial losses were phone (24 per cent), social networking and online forums and email.
- phishing scams were the most common scam approach, representing 36 per cent of all reports. Despite the inconvenience of their prevalence, only 2 per cent of phishing reports were associated with a financial loss.
- investment scams, while only 3 per cent of all reports, were associated with $292 million or 61 per cent of all reported losses. Additionally, investment scams were associated with a high average loss of $81,300.

Digital platform service providers are a rapidly expanding conduit for scammers to target consumers. In particular, social media is over-represented as a source of losses to scams, accounting for 6 per cent of reported contact methods in 2023, but is the second most common source of scam losses. Chart 4 illustrates the consistent rise in consumer reports on social media scams to Scamwatch, leading to $93.5 million in losses reported in 2023.

Chart 4 – Social media and online forum scams reported to Scamwatch[17]



1.2.2 Awareness and response lags evolution in scam tactics

It can be very hard to spot a scam. Scammers are sophisticated and may interact with a target over multiple communication platforms to build a false connection. Scammers rapidly adapt their approach

16 ACCC, Scamwatch online data dashboard
17 ACCC, Scamwatch online data dashboard

to take advantage of modern technology, products, services, and major events to convince everyday Australians that a scam is a legitimate offer.

Scammers also take advantage of the immediacy of online transactions by using urgency and psychological pressure to motivate targets to act without further consideration or investigation. Scammers' demands for real-time financial transfers or the use of difficult to trace forms of payment (such as gift cards and crypto assets) reduce the opportunity for those targeted to stop payments or seek recovery of financial losses.

Consumers play an important role in detecting and preventing scams, but can also be affected in ways that diminish their ability to disclose, report and seek help when they have been scammed. Shame and social stigma associated with falling victim to a scam is a disincentive for reporting and can prevent discussion of experiences to help consumers understand that anyone can get scammed. Although communication and education activities are important prevention activities, these alone are not likely to be impactful as scammers continue to change strategies and adapt to new technologies and trends.

1.3 Industry responses to scams activity

1.3.1 Lack of clear responsibility and accountability for mitigating scam harms

A successful scam will often involve illegitimate activity across multiple sectors to engage the consumers. The sectors scammers most used as a conduit for consumer harm are banks, telecommunications providers and digital platform service providers. For example, a scam may be initiated via a fraudulent advert on a social media platform, which leads to engagement via phone before payment being made by the victim via a bank transfer.

Businesses and industry associations in these sectors have recognised the growing prevalence of scams and have independently begun to take steps to mitigate the impact and harm scams have on Australians. However, businesses that are co-opted by scammers currently have differing approaches in how they respond to reports of potential scam material. In some cases, businesses are perceived to prioritise direct commercial or economic outcomes for their business over investigating the potential harm, disruption, victimisation, and financial losses to their consumers. Poor or sluggish responses to potential scam reports perpetuates the exposure and likelihood of success of a scam.

A successful scam often involves illegitimate activity across multiple sectors in the scams ecosystem, leading to an array of challenges for consumers, industry and government such as:

- which sector the consumer contacts to report the scam and seek support or redress,
- how to share relevant information between industry, law enforcement agencies and regulators to investigate scam reports and improve disruption of scams by sharing intelligence of evolving scam patterns,
- how to determine the specific actions or failures by sectors in the scams ecosystem which contributed to the compromise of consumer protection,
- what regulatory avenues can be used to pursue illegitimate scam activity, and
- how to determine the appropriate and proportional accountability and responsibility for failures in consumer protections, and related liability for losses and appropriate penalties.

The involvement of many sectors means there are inconsistent views across the scam ecosystem regarding the responsibility and accountability of each sector to mitigate harms and to provide support or pathways for redress to consumers. Sectors, which are by their nature at differing points in consumers experience of a scam, face differing reputational detriment and incentives to disrupt scam activity or to help consumers to verify the legitimacy and identity of digital commerce and communication.

The regulatory landscape needs to evolve to better protect consumers from scams in an environment where multiple sectors play a role. Consumers can experience frustration in seeking action, investigation, or support from entities at different stages of the scam life cycle. These issues are compounding as scams increase in complexity and sophistication over time. Clear and effective regulation is needed to balance the competing interests of establishing co-ordinated responses and consumer protections for scams while not limiting industry competition or innovation.

1.3.2 Inconsistent dispute resolution processes for scams

Dispute resolution arrangements vary in the banking, telecommunications, and digital platforms sectors, resulting in inconsistent outcomes for scam victims seeking redress. Industry-specific internal dispute resolution (IDR) and external dispute resolution (EDR) arrangements are currently required to be in place for banks and telecommunications providers. The Australian Financial Complaints Authority (AFCA) is the EDR body for complaints against banks and the Telecommunications Industry Ombudsman (TIO) for telecommunications-related complaints. There are no existing industry-specific IDR or EDR arrangements operating for digital platforms. As a result of these varying arrangements across the ecosystem, there is often confusion for consumers in how to report scams, or seek support and redress. Industry-specific EDR arrangements mean scam victims may find themselves lodging complaints with multiple EDR schemes and be bounced between different EDR schemes This results in additional time and psychological burden when dealing with the financial and emotional harm of scams.

Further, industry specific EDR arrangements mean there is no holistic consideration of the role multiple entities in different sectors play in a scam complaint. The realisation by a consumer they have been scammed often occurs after payment has been made, meaning payment providers such as banks are frequently the point of the ecosystem where consumers report a scam and seek assistance to recover the financial loss. Where there is a dispute between a bank and a consumer, and a satisfactory outcome could not be reached through IDR, the consumer may escalate a complaint to AFCA. However, AFCA is only able consider the conduct of the bank involved, and not other industry sectors which may have been involved in the scam chain (e.g. digital platforms) and could have acted to prevent the financial loss or scam.

1.3.4 Piecemeal and slow industry action

Industry self-regulation is occurring in some sectors, but not at the pace consistent with growth in scam activity.

Some individual businesses or areas of industry sectors have made efforts to address scams, such as the introduction of the Reducing Scam Calls and Scam Short Messages (SMs) industry code for telecommunications providers, the Australian Banking Association (ABA) and Customer Owned Banking Association's (COBA) Scam-Safe Accord, and the Digital Industry Group Inc. (DIGI) Australian Online Scams Code (AOSC). Of these only the Reducing Scam Calls and Scam SMs industry code is compulsory with enforcement by ACMA.[18]

Several banks, telecommunications and digital platforms providers, participate in the AFCX (an industry-led information sharing and reporting regime) where members can use an online platform to identify and analyse suspicious transactions and alert other members.[19] In 2023, the AFCX expanded the platform to build a Fraud Reporting Exchange that enables members to send and receive near real-time reports to co-ordinate and halt multiple transactions in the chain of a single scam. However,

18 ACMA carries enforcement powers to issue warnings and directions to participating entities to comply with relevant industry codes, and can issue infringement notices and penalties if these are not met. See Part 6 of the *Telecommunications Act 1997*.
19 Full membership of the AFCX is not publicly disclosed, however participants include the four founding major banks, Macquarie and Bendigo Bank, and COBA.

as these information sharing arrangements are not supported by legislative provisions, participants face legislative constraints in sharing information which may contain personal identifiers between member organisations. The scope of the Fraud Reporting Exchange is also limited to organisations which voluntarily participate and invest in information sharing.

The current voluntary approach to addressing and introducing anti-scam measures by industry has been inconsistent and slow relative to the sharp rise in scam activity. Industries across the scam ecosystem have taken a piecemeal approach to addressing the scams threat, with the result that efforts have been misaligned and haphazard.

See Appendix 1 for further detail on industry actions to date.

2. Need for Government action

2.1 Need for government action

Government action is required to ensure effective coordination, and a whole-of-ecosystem response to reduce financial losses from scams and restore trust in digital commerce and communication. Without government action, it is unlikely the cost of harms will be adequately considered by industries which are vectors of scam activity. As a result, there will not be consistent and effective anti-scam protection measures implemented by industry across the entire scam ecosystem and the costs will fall inequitably across society.

2.1.1 Economy-wide coordination of anti-scam activity

Clear and consistent standards for preventative action across all high priority sectors in the scam ecosystem are needed to ensure gaps in consumer protections are minimised. Effectively achieving this outcome will depend on action by those who have the best opportunity and most appropriate resources to address scams. Voluntary action by industry has not proven sufficient to date.

Effective and coordinated action across the economy is limited by the absence of an overarching regulatory framework that sets clear roles and responsibilities for government, regulators, consumers and the private sector. The current piecemeal and fragmented voluntary approach has made it easier for scammers to exploit regulatory gaps across the ecosystem. It has also made it difficult for consumers and victims of scams to understand the role and responsibility of a business in combatting scams and providing clear responses to scam reports.

Prevention actions must be taken across all sectors in the ecosystem that are high-risk for scam activity. In the absence of action across the ecosystem, scammers will shift their activity to the sectors which have weaker practices relating to scam protections. This would leave Australians exposed to sophisticated scam activity.

2.1.2 Improving alignment of costs and benefits of action

Reliance on voluntary market action is unlikely to be effective as losses and detrimental reputational impacts are inequitably distributed across the scam ecosystem between government, industry and consumers. Incentives for comprehensive voluntary action are lacking for key sectors as the business and reputational cost of scam activity are misaligned with the relative roles sectors' play as vectors of scam activity. For example, although digital platforms encounter reputational risks and potential loss of users from the presence of scams hosted on their platforms, this content persists on many platforms. Scams reported to Scamwatch originating on social media led to the largest growth in losses from 2022 to 2023 (16.5 per cent from $80.2 million to $93.5 million), while losses have been decreasing for scams perpetrated using most other contact methods (e.g. 17.7 per cent decrease in losses from scam phone calls).[20]

Government action is required to create consistent incentives and obligations for action to minimise harm from scams across the scam ecosystem. Government action is needed to ensure that the treatment of consumers who report scams or seek redress is not determined predominately by the service providers through which the scam occurred.

20 ACCC, *Targeting Scams 2023*. p. 14

2.1.3 Providing a consistent message

There are currently many competing voices in the scam disruption space, with various perspectives creating confusion and inconsistent messaging for Australians. The Government can provide a consistent voice of authority that Australians could rely on to improve consumer protections. Government can establish expectations for how businesses respond to scams, support victims and establish pathways for equitable redress where a business has failed to meet these expectations.

Government action to set expectations across the entire ecosystem would reduce confusion and inconstant messages, allowing consumers to:

- feel more confident engaging with the digital economy without being overly exposed to scams;
- increase trust in communications from government and industry and feel better protected from scams;
- be less disrupted by scam activity, and the time required to assess or verify the validity of digital communication or commerce; and consequentially result in fewer reports of scams;
- increase confidence that industry and government will respond to scam reports; and
- incur less financial, psychological, emotional and social distress from scam activity.

2.1.4 Co-ordination with international anti-scam initiatives

Government action is needed to ensure scam prevention activities are co-ordinated economy-wide, in alignment with international activities and commitments. Internationally, government-initiated actions are being taken to establish pathways for consumers to report scams, and for policies to tackle scams economy-wide which inform the policy approaches in Australia. In the United Kingdom there are voluntary sector charters for fraud between the government and industry sectors to address scams.[21] In Singapore, proposals have been put for adoption of a Shared Responsibility Framework to allocate liability for scams across sectors. [22]

In March 2024, the Government participated in multilateral dialogue at the inaugural Global Fraud Summit hosted by the United Kingdom Government. The outcomes of the Summit included a communique establishing an agreed global framework for addressing fraud, including commitments to co-ordinate and strengthen international government and industry collaboration on scam prevention. These commitments have been supported by bilateral dialogue with countries, including Singapore, the United Kingdom and New Zealand.

2.2 Successful government action

2.2.1 Improvements have been associated with Government action

The work by Government to date has had an impact on reducing scam activity and losses. For example, ASIC's takedown capability removes or limits access to fraudulent and malicious websites on the internet to disrupt scam activity, which has led to takedowns of more than 7,300 investment scam and phishing websites between July 2023 and August 2024.[23] The takedown service has mostly targeted fake investment platforms appearing to offer high-risk products like foreign currency derivatives and crypto assets. ASIC is also targeting impersonation scams where legitimate businesses are cloned to trick consumers, and fake celebrity endorsements used to fraudulently promote

21 United Kingdom Finance, *2023 Half-Year Fraud Update;* United Kingdom Home Department, *Online Fraud Charter 2023.*
22 Monetary Authority of Singapore, *Consultation Paper on Proposed Shared Responsibility Framework,* 20 December 2023.
23 ASIC, *Online investment trading scams top ASIC's website takedown action ,* 19 August 2024.

financial products.[24] These actions have helped drive investment scam losses down by around 60 per cent in the second quarter of 2024 compared to the same quarter in 2022.[25]

Following the introduction in July 2022 of the Reducing Scam Calls and Scam SMs industry code, telecommunications providers have blocked 1.5 billion scam calls and 668 million scam SMS.[26] Between April and June 2024, telecommunications providers reported blocking over 156 million scam calls and over 134 million scam SMS.[27]

Government provided $10.9 million over four years to launch[28] a SMS Sender ID Register to combat scammers impersonating key industry or government brand names in text message headers. The voluntary pilot, commenced by the Australian Communications Media Authority (ACMA) in December 2023[29], consolidates existing provider-level initiatives to protect participating alphanumeric sender IDs from impersonation by scammers. Following an extension of the pilot,[30] and a consultation on the design of a mandatory Register,[31] the legislation amending the *Telecommunications Act* to establish the SMS ID Register received royal assent on 22 August 2024.[32]

While Australian Government initiatives to combat scams are showing initial signs of reducing the acceleration of scam losses and exposure, scam harms remain unacceptably high. Despite positive signs, consistent and integrated economy-wide action is hindered by the lack of incentives some sectors have for robust voluntary action.

2.2.2 Objectives for scam prevention policy

Further government action is needed to make Australian consumers and small businesses harder targets for scammers. Australia needs the ecosystem targeted by scammers to be as robust as possible to prevent, detect, report, disrupt and respond to scam activity, and provide flexibility to adjust as scammers adapt to responses by authorities and exploit gaps in protections.

The government has two core objectives to address the rising impact of scams on the economy:

1) **Reduce scam harms**: Reduction of the rates of reported exposure and victimisation of consumers from scam activity occurring in sectors which are key vectors targeted by scammers. Success can be measured by a sustained reduction in the number and size of reported scam losses by consumers.
2) **Align benefits and costs of scam prevention**: Alignment of industry responses as appropriate to the presence of scam activity on platforms and services across the ecosystem. Greater symmetry and co-ordination of anti-scam responses will contribute to reducing the exposure of business activities open to exploitation by scammers. Success can be measured by reductions in scams taking place across services as opposed to an aggregate reduction in one area of the economy.

The government aims to facilitate improved outcomes against these core objectives through:

- Improvements to the consistency, quality, and timeliness of industry responses to scam activity. Uplift in scam prevention action across the ecosystem is required to minimise gaps in the responses and protections provided by businesses, with the weakest links in the ecosystem

24 The Hon Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, *Thousands of scam investment websites removed in takedown blitz,* 2 November 2023.
25 ACCC Scamwatch, *Scam Statistics* data dashboard
26 Calculated from ACMA's "Action on telco consumer protection" quarterly reports from the July to September 2022 to April to June 2024.
27 ACMA, *Action on telco consumer protections:* April to June 2024, 12 August 2024.
28 The Hon Michelle Rowland MP, Minister for Communications, *Albanese Government acts to disrupt illegal text message scams,* 23 April 2023.
29 ACMA, *The SMS Sender ID Registry*
30 ACMA, *Action on Scams, Spam and Telemarketing: January to March 2024*, 31 May 2024.
31 DITRDCA, *SMS Sender ID Registry: Fighting SMS Impersonation Scams*, 18 February 2024.
32 *Telecommunications Amendment (SMS Sender ID Register) Bill 2024*

often exploited by scammers. The impact of actions would be measured through analysis of business practices and the quality of anti-scam policies, procedures, and resourcing.

- Greater levels of industry collaboration, reporting and information sharing between businesses and to regulators about scam activity. Information sharing improves the capability of parties in the scams ecosystem to quickly detect and disrupt scam activity as it arises or prevent similar activity by the same perpetrator. Collaboration would be measured through volume, quality, and use of reporting data.
- Increased accessibility and transparency of pathways for consumers to report and seek support when experiencing a scam. The impact of scams on consumers can be mitigated when they are able to quickly report scam activity and receive support through dispute resolution and redress arrangements. Improvements to consumer experience would be measured by factors, including timeframes, consumer satisfaction, and the outcomes of reporting and dispute resolution.

Government commitments have not set a timeframe for achievement of these objectives. However, the Government aims to reduce the impact of scams as a priority due to the unacceptably high losses experienced to scams in Australia. These objectives are in line with the aim of the NASC to make Australia the world's hardest target for scammers by improving co-operation between government, industry and law enforcement to prevent scams and empower Australians to avoid scams.[33]

For more information about the objectives and evaluation of outcomes, see Appendix 3.

33 NASC, *Quarterly Update, January to March 2024,* 21 May 2024

3. Policy options considered

Consistent with guidance from the Office of Impact Analysis (OIA) on election commitments, Treasury has considered two policy options. The options considered are:

- Option 1: Maintain the status quo.
- Option 2: Implement the Government's election commitment to introduce economy-wide, mandatory scams codes by establishing the Scams Prevention Framework (SPF).

Further industry-led initiatives have not been considered in this IA. While beneficial, existing industry-led actions are not capable of delivering consistent and co-ordinated ecosystem wide preventions for scam activity. Current voluntary codes do not deliver comprehensive coverage of the vectors of scam harms, and have limited ability to hold signatories to account creating gaps which can be exploited by scammers.

Mandatory and pre-determined bank liability is not considered in this IA because it is inconsistent with the policy problem of determining an appropriate sharing of responsibilities and incentivising a system-wide improvement in scam prevention. Compensation mechanisms that cover multiple sectors, not just banking, are considered in Option 2.

Additionally, a non-regulatory option has not been considered in this IA, as the government is separately implementing non-regulatory responses to the policy problem, including through the implementation of the NASC and a public awareness campaign.

3.1 Option 1 – Status quo

Without further government action, Australians will continue to rely predominately on voluntary responses by industry to combat scams. Those efforts would be complemented by existing Government initiatives introduced to address scams and the current regulatory oversight and enforcement powers of regulators relating to more general consumer or financial protections.

Protections in Australia for consumers and businesses would comprise of the following initiatives with limited reach to address and manage scam threats:

- the NASC in receiving scam intelligence and convening Fusion Cells to target solutions to emerging threats;
- ACCC/NASC and ASIC engaging with takedown providers to identify and taken down investment scams and phishing websites;
- the voluntary approaches of industry sectors, including the ABA/COBA Scam-Safe Accord and the DIGI Australian Online Scams Code;
- the SMS Sender ID Registry protecting participating sender IDs from impersonation;
- ACMA enforcing the *Reducing Scam Calls and Scam SMs* industry code; and
- existing non-targeted consumer protection regulatory and enforcement powers to respond where those laws have been breached.
- existing consumer dispute and ombudsman schemes for complaints in the telecommunications and banking industries.

There would be no change to the fragmented response to voluntary anti-scam activity, where the protections and outcomes for victims could differ greatly depending on the sectors involved in their specific scam experience and processes of their service providers. Industry would be engaged further by government where they offer to take voluntary actions to contribute to national anti-scam measures, such as expanded information sharing with the NASC.

3.2 Option 2 – Scams Prevention Framework

Under Option 2, the government would introduce new mandatory industry codes to outline the responsibilities of the private sector in relation to scam activity under an overarching SPF. If the entities in these industries fail to comply with their obligations, they may be subject to penalties or be liable to compensate consumers for losses experienced due to these failures.

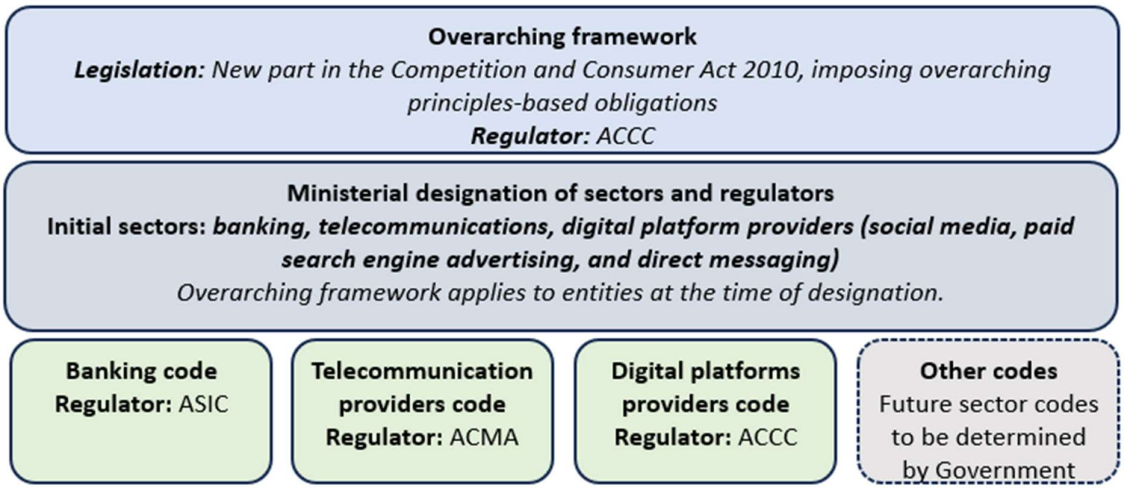
A new framework that creates mandatory obligations for sectors targeted by scammers would provide appropriate guardrails to reduce the scam threat activity across key sectors and make Australia a less attractive target for scammers.

The introduction of an overarching regulatory framework, supported by sector-specific mandatory codes, will deliver the Government's 2022 election commitment of introducing tough, new mandatory industry codes for banks, telecommunication providers and social media companies to combat scams.[34]

This option would have a two-tiered regulatory design that enables an overarching legislation of the SPF in the *Competition and Consumer Act 2010* and subordinate legislation to introduce sector-specific obligations (Figure 1). This option would promote a whole-of-ecosystem approach to scams by directly legislating minimum standards that are enforceable in the designated sectors where scammers are prevalent.

The SPF design will enable flexibility to designate additional sectors as future challenges arise. This approach will fulfil the Government's election commitment as it would enable the development and enforcement of sector specific codes on banks, telecommunication providers, and digital platform service providers, which at the outset, would cover social media, direct messaging and paid search advertising services.

Figure 1 – The Scams Prevention Framework



Overarching framework

The SPF establishes an overarching framework to set principles-based obligations that would be adaptable to the various operating models of regulated businesses. The SPF would enable an increase in baseline requirements commensurate with the size and risk profile of the entity targeted by scams

[34] The Hon Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, *Fighting back against scammer scrouge – Government announces new anti-scams centre,* 15 May 2023

and allow for consideration of future sectors to be designated by government. The SPF would drive consistency in expectations and responses across sectors.

Under the SPF there would be 6 types of obligations for regulated entities:

- Prevent: Implementation of responsive anti-scam processes, procedures and/or systems, and make information available to consumers in relation to the steps they can take to minimise the risk of scams.
- Detect: Taking proactive steps to detect scam activity on its platform and/or service, and act in a timely manner on scam intelligence received to prevent further loss to impacted consumers.
- Disrupt: Taking proactive and timely steps to disrupt scam activity identified on its platform and/or service and share relevant scam intelligence with impacted consumers in a timely manner.
- Respond: Having an accessible mechanism for consumers to report a scam, an IDR mechanism for a consumer to make a complaint, and membership of the prescribed EDR scheme for their sector.
- Report: Sharing scam intelligence with a government regulator in real-time and responding to information requests from regulators within a specified timeframe. Government regulators would also be expected to share scam intelligence with other entities, government agencies and people who may be able to respond to the scam activity.
- Governance: Documentation of policies and procedures for managing the risk of scams on their platform and/or service and regularly review their effectiveness against established performance metrics and targets.

IDR and EDR requirements would apply consistently across all designated entities. Where a consumer has experienced loss due to a scam, they would first approach a relevant regulated entity for redress through the entity's IDR mechanism. If a consumer complaint is not resolved or if the consumer is not satisfied with the outcome at the IDR stage, they will have an option to escalate their complaint to EDR. All entities that provide a service that is regulated by the SPF would be required to become a member of an authorised EDR scheme. An EDR mechanism would provide pathways for redress (including compensation) where regulated entities have not met their SPF obligations. AFCA would become the single EDR body for the three sectors initially designated under the SPF. Consumers would be able to raise scam complaints related to banks, telecommunication providers and certain digital platforms, ensuring a holistic 'no wrong door' approach to seek redress.

The SPF would also establish a network for reporting intelligence to protect against scams. By requiring entities which detect scam activities to share information with a government regulator, and establishing systems for such intelligence to be shared with relevant entities across the scam ecosystem; anti-scam activities can be coordinated across multiple entities, industry sectors and potentially with international partners.

Certain requirements around scam disruption and response action will be framed as principles-based obligations, leaving open the potential for more prescriptive details in sector-specific codes.

The SPF would introduce a responsive and adaptable framework that allows the Government, industry and regulators to respond to changes in scam activity in the economy, by allowing for additional sectors or services of the economy to be regulated, and for sector-specific codes to be made and enforced for that sector.

Mandatory sector-specific codes

In addition to the principles-based obligations, the SPF would introduce mandatory sector-specific codes, setting out more specific obligations for each sector.

Sector-specific codes would ensure measures are appropriate for each industry, as well as providing flexibility for obligations to be developed in further detail as scams evolve. This design is intended to enable rapid response to evolving scam patterns, without requiring changes to the primary law.

Sector-specific codes may incorporate prescriptive expectations on businesses to:

- Document policies and procedures setting out their approach to managing scam-related risks in their business;
- Comply with certain obligations related to IDR and EDR, including timeframes for response to consumer complaints at the IDR level, and cooperating and providing reasonable assistance to the prescribed EDR scheme; and
- Act on scam intelligence, supported by guidance on the actions expected of businesses.

The mandatory sector-specific codes will initially apply to sectors designated to be covered under the SPF (banks, telecommunication providers and digital platform service providers). Consideration of designating additional sectors and introducing sector-specific codes would be available under the proposed SPF model where there is a constitutional basis to do so.

4. Net benefit of each option

The net benefit of each option is assessed through analysis of expected:

- 4.1 Regulatory costs Regulatory costs incurred by:
  - Banks
  - Telecommunication providers
  - Digital platforms
  - Consumers
- Government costs
- Benefits of:
  - Reducing exposure to scams
  - Reducing scam losses
  - Improving redress for victims of scam losses

The 4.4 of options 2 has been assessed using a break-even analysis. This method is chosen as the benefits of each policy option are highly uncertain and not fully unquantifiable.

The following evaluation establishes the threshold break-even level of reduction in scam losses required to achieve a net benefit, considering the expected costs of each option. Although there are other monetary and non-monetary benefits from reducing scam harms (see section 1.1.2 Scams inflict a broad range of harms), the dollar amount of losses to scams is a clear measure of the level of benefit related to each option.

The likely effectiveness of each option reducing scam losses to outweigh its overall costs is assessed to establish which option would achieve the greatest net benefit. Expected change in the volume of amounts reimbursed to scam victims from relevant entities has not been considered as the primary objective of anti-scam actions and are not considered as benefits or costs of each option. The dollar amounts paid as reimbursements are equally a benefit to victims and a cost to regulated entities.[35]

As quantification of the benefits of anti-scam activities is not possible a cost-benefit analysis is not appropriate in this case. As policy options 2 would be an innovative approach to strengthening protections from scam activity, there is a lack of evidence on the level to which these approaches would be effective.

The broad reach of benefits, including non-monetary impacts in areas like consumer confidence or businesses' reputational damage, also means it is not possible to make a quantitative assessment of all benefits. Benefits would apply to a diverse group of Australian society, including individual consumers, sectors in the scams ecosystem and legitimate businesses at risk of impersonation. These broader benefits would be result from improvements in the 3 types of benefit assessed.

Details of the assumptions used in calculations of regulatory costs are included in **Appendix 2 – Regulatory cost calculations**.

35 These payments represent a transfer of monies between entities and consumers rather than a benefit to society overall.

4.1 Regulatory costs

4.1.1 Banks

Option 1 – Status quo

Under the status quo, banks would maintain current commitments to address scams on their services, including implementation of the Scam-Safe Accord.

Banks currently dedicate significant resourcing to fraud prevention and account verification activities. In recent years, individual banks have introduced measures in response to the rising impact of scams, including new measures to detect scams, verify accounts, and share and receive intelligence. An overview of current sector uplift across various banking sector initiatives is provided below at Table 3.

Most domestic banks are members of industry associations ABA and COBA, who have co-ordinated sector-wide commitments under the Scam-Safe Accord to commit members to anti-scam measures. The Scam-Safe Accord includes a confirmation of payee system with an industry-estimated cost to the sector of $100 million.[36] More information on the Scam-Safe Accord and relevant commitments for banking sector members is at **Appendix 1**.

Table 3 – Banking sector initiatives

Activities	Examples of sector initiatives
Detection measures	Some banks have announced the use of new technologies, including artificial intelligence, to detect suspicious and unusual behaviour on its platforms and use analytics to predict the risk level of potential scam activity, including a *Scam Scoring* model announced by ANZ in April 2024.
Payee verification	Some banks have announced additional checks and warnings for payments, including account name matching measures including CommBank *NameCheck* and Westpac *Verify* initiatives in March 2023.
High-risk transaction controls	Banks have announced a series of new holds, declines and limits on high-risk transactions, including changes for payments to high-risk cryptocurrency exchanges announced by all major banks over 2023-24.
Caller identification and verification	Some banks have announced in-app communications and partnered with telecommunications providers to verify bank calls, including CommBank *CallerCheck* in February 2023 *and Westpac Safecall* in July 2024.

Under status quo arrangements, industry voluntary information sharing arrangements will continue to develop, with all Scam-Safe Accord signatories committing to join the AFCX. In May 2023, the ABA reported that 14 of its 20 members were, or were in the process of, entering membership with the Fraud Reporting Exchange of the AFCX. Under the Scam-Safe Accord, participating banks committed to join the AFCX by mid-2024 and its Fraud Reporting Exchange over 2024-25.

Banks play a pivotal role in economy-wide information sharing arrangements and have developed more standardised sets of data and processes compared to other sectors. However, banks have less visibility of intelligence relating to contact or communication methods for scams beyond self-reported information from consumers, which is highly useful for early identification.

Under the status quo, banks would be subject to existing requirements to have appropriate IDR mechanisms in place and be a member of AFCA. Both of these obligations are set out in section 912A of the *Corporations Act 2001*. However, certain branches of foreign-owned authorised deposit-taking

[36] Australian Banking Association, *Banks unite to declare war on scammers*, 24 November 2023.

institutions (ADIs) that generally service wholesale clients and ADIs that provides services to industry (e.g. the Australian Settlements Ltd) do not hold an AFCA membership.

Being a member of AFCA includes paying AFCA's annual membership fee (~$389 for FY 2024-25), complaint handling fees and an annual proportionate user charge that is calculated based on prior year's AFCA dispute handling data. AFCA does not charge for the first five complaints against a member in a financial year. After that, the complaint handling fees vary on a case-by-case basis, depending on the stage the complaint is closed. Under status quo, AFCA would maintain its current jurisdiction as the EDR scheme for financial sector firms, including in relation to complaints involving scams.

Option 2 – Scams Prevention Framework

The impact of the SPF on the banking sector would result in a consistent standard of measures to prevent, detect, report, disrupt, and respond to scams additional to voluntary commitments or industry self-regulation. The uplift approach to the initial SPF would see the most changes in its capture of banks that do not participate in or meet current industry standards relating to scams as all businesses would be mandated to adopt new policies and procedures.

Under the SPF, the banking sector may be required to undertake additional activities to demonstrate compliance with its principles-based obligations, including the following:

- Prevention activities, including the design of appropriate banking in-app communications and warnings to consumers to reduce the risk that consumers will be exposed to a scam attempt.
- Detection activities, including information sharing and improving responsiveness to trace and action credible intelligence from consumer and industry reports of reasonably suspected scam activity.
- Disruption activities, including ensuring appropriate frictions are in place for transactions reasonably at risk of being a scam, which may include placing holds, delays and limits on accounts or transactions.

To document and review these activities, banks would also have overarching governance obligations to develop and implement governance policies, procedures, metrics and targets to combat scams. Whilst compliance costs for industry to perform governance obligations will vary based on the maturity of existing internal governance arrangements. Most banks have or have already voluntarily committed to implementing anti-scam activities under the Scam-Safe Accord, reducing the anticipated impacts.

Assuming existing strategies are in place, governance impacts additional to status quo governance activities may include capability and staffing to ensure the following functions can be performed:

- annual review of anti-scam policies and procedures by a senior officer within the entity,
- maintenance and record-keeping of documents relating to anti-scam policies and procedures,
- drafting and publication of information on how businesses are protecting consumers, as well as ensuring information is available to consumers on rights and available complaints avenues.

Information sharing requirements would create additional impacts relevant to new policies and procedures relating to escalating actionable scam intelligence. However, the costs of these arrangements are mitigated due to existing Accord banking sector commitments to join in the AFCX.

The extent to which banks would be required to incur additional costs is mitigated by the considerable extent of independent and self-regulated activity in the sector, and parallel regulatory obligations for similar harms, including those relating to money laundering offences covered under the *Anti-Money Laundering and Counter Terrorism Financing Act*.

The SPF will capture businesses in the banking sector by designating all ADIs overseen by the Australian Prudential Regulation Authority (APRA). As outlined in Table 4, this would capture some

businesses that are and are not a member of industry bodies and would potentially be subject to additional obligations. Depending on the size and complexity of these entities, regulatory capture may impose expectations for new activities and associated costs.

It is expected that the implementation of SPF obligations and associated costs will differ depending on the size and complexity of the entity. As of June 2024, APRA monitors 126 ADIs. Of the $1.469 trillion in deposits managed by these ADIs, 73 per cent are held by the major four banks.[37] The remainder of deposit-taking activity in Australia is managed by a range of smaller entities: including medium-sized banks, credit unions, building societies and neobanks, each with a variable customer base, resourcing and presence in the Australian financial system.

Table 4 – Potential regulated entities under the Banking Code[38]

Regulated sector	Potential known entities	Examples	Industry representation
Banks Defined as *authorised deposit-taking institutions*	**4** major banks	ANZ Banking Group, Commonwealth Bank of Australia	All **4** are members of ABA
	73 other domestic banks, credit unions, building societies and neobanks	Bendigo and Adelaide Bank, Newcastle Permanent Building Society	**64** are members of ABA or COBA
	7 Australian subsidiaries of foreign-owned banks	Bank of China (Australia), HSBC Bank Australia	**6** are members of ABA
	48 Australian branches of foreign-owned banks	Citibank, ING Bank	**2** are members or have subsidiaries that are members of ABA

The SPF would also impose obligations on regulated entities to have in place an accessible and transparent IDR mechanism for consumers to make complaints in relation to scams, and to be a member of a prescribed EDR scheme. AFCA would operate a single EDR scheme for scam complaints in relation to the three initial sectors subject to the Framework.

As indicated above, banks are already required to have appropriate IDR mechanisms in place, and most are a member of AFCA under section 912A of the *Corporations Act 2001*. The SPF requirement to be a member of AFCA would apply to all ADIs, including those that might not have existing membership with AFCA (such as branches of foreign-owned banks). This is because these entities could also be involved in a scam and their customers are not invulnerable to the threat of a scam. The number of scams complaints requiring EDR would be expected to increase initially because of improved complaints procedures and uplifted obligations resulting in greater benefit to consumers from taking complaints to AFCA. However, the number of complaints is likely to fall as the rate of scam victimisation reduces because of the SPF.

Areas where there would be uplift beyond current initiatives of entities in the banking sector are summarised in Table 5.

[37] APRA, *Monthly Authorised Deposit-Taking Institution Statistics: Table 4, Deposits on Australian books of selected individual ADIs* (June 2024)

[38] Further details in Appendix 2. This list is illustrative and is not intended to represent the intended scope of the definitions for the designation of these services, which would require further development after the SPF is legislated. Providers of purchased payment facilities and restricted ADIs have been assumed to be out of scope of SPF obligations.

Table 5 – Banking sector initiatives and uplift required for the Scams Prevention Framework

Obligation	Current initiatives	Uplift required
Anti-scam activity	Voluntary Scam-Safe Accord standards for ABA and COBA members	Anti-scam activity improvements, governance operations
Information sharing and reporting	ABA/COBA members committed to participation in AFCX	Higher standards of information sharing would be required, including beyond the banking sector
Dispute resolution	AFCA membership and IDR requirements for consumer banking	Likely increase in complaints, required membership of AFCA for branches of foreign banks

As outlined in Table 6, the estimated regulatory costs of Option 2 additional to the status quo for the banking sector would be $100.9 million in the initial year, and $31.8 million on an ongoing basis each following year. Most of this regulatory cost would be on banks which are not affiliated with the ABA or COBA, which would be required to invest in capabilities to meet the Scam-Safe Accord level of anti-scam activity and additional requirements of the proposed option. However, there would also be a need for investment in improvement of capabilities for Scam-Safe Accord signatories. While almost all ADIs are members of AFCA, banking EDR costs are expected to increase due to an initially increased number of scam complaints each year.

Table 6 – Option 2 Estimated annual regulatory burden on banks ($m)

Entity type	Entities	Initial cost	Ongoing cost
Major banks	4	$6.2	$1.0
Other ABA/COBA	72	$22.9	$2.7
Non-affiliated/AFCA	40	$51.1	$20.0
Non-affiliated/non-AFCA	16	$20.6	$8.1
Total	**132**	$100.9	$31.8

4.1.2 Telecommunication providers

Option 1 – Status quo

Telecommunications providers are already subject to mandatory obligations under their existing industry code. The 2022 *Reducing Scam Calls and Scam SMs* industry code requires telecommunications providers to:

- provide up-to-date guidance for consumers on how to manage and report scam calls and texts;
- monitor, identify, trace and block phone calls and SMS from recognised scammers; and
- report identified scam calls and SMS to the ACMA and any involved telecommunications providers.

These actions demonstrate providers have the infrastructure and are responding to existing expectations that businesses in the sector lift consumer protections.

Information sharing arrangements in the telecommunication sector are progressing. Major telecommunications providers participate in the AFCX Intel Loop. The AFCX has expressed interest in expanding inclusion of non-banking sector entities such as the telecommunications and payments system providers, with Optus and Australian Payments Plus already AFCX members. In July 2023, Optus announced its Call Stop technology to automatically block calls to scam numbers, linking to intelligence gained in partnership with the banking sector and AFCX.[39]

Telecommunications providers would maintain their existing mechanisms in relation to IDR and EDR, which includes compliance with complaints handling requirements under the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* and membership with the TIO. The TIO receives and manages all complaints in relation to the telecommunications sector, including scam complaints.

Option 2 – Scams Prevention Framework

Under Option 2, there are unlikely to be significant additional costs for telecommunications providers who are compliant with current obligations. Actions previously taken or planned to be taken to implement anti-scam activities in response to *Reducing Scam Calls and Scam SMs* industry code obligations would mitigate the costs required for meeting the SPF's regulatory requirements.

All telecommunication providers would have additional governance obligations to document and review their anti-scam activity, as detailed in the section for banks. Although the industry does not have an explicit sector-wide commitment to specific governance activities related to scams, impacts are similarly likely to be variable and mitigated by existing governance activities.

Telecommunications providers would need to invest in their capabilities to share scam information potentially more frequently and in new formats. This burden would be mitigated by the current capabilities required to share data with ACMA and other providers under the *Reducing Scam Calls and Scam SMs* and involvement by the major telcos in AFCX.

Telecommunication service providers would largely be able to leverage existing complaints handling processes to meet IDR requirements under the SPF. In relation to EDR, telecommunication service providers would be required to join an AFCA-led single EDR scheme for the purposes of scam complaints, in addition to maintaining their existing required membership with the TIO for non-scam complaints.

The requirement to join AFCA would also apply to transit carriers and carriage service providers (CSPs) that may currently be exempt from the requirement to join TIO because they do not have individual or small business customers. This is because transit carriers and CSPs could be responsible for carrying scam calls and texts between two providers prior to reaching a consumer.

Under Option 2, most telecommunication service providers would be required to maintain membership of two EDR schemes – TIO and AFCA. In addition to costs associated with TIO's EDR process under the status quo, telecommunication service providers would incur costs to join and participate in AFCA's EDR processes.

Areas where there would be uplift required additional to current initiatives of entities in the telecommunications sector are summarised in Table 7Table 7 – Telecommunications sector initiatives and uplift required for Scams Prevention FrameworkTable 7.

39 Optus, *Optus Call Stop to fight off SMS scams*, 17 July 2023.

Table 7 – Telecommunications sector initiatives and uplift required for Scams Prevention Framework

Obligation	Current initiatives	Uplift required
Anti-scam activities	Mandatory *Reducing Scam Calls and SMs* Code obligations	Mainly new governance processes, and possible uplift in obligations
Information sharing and reporting	AFCX for major telcos, sharing with ACMA under *Reducing Scam Calls and SMs* Code	Higher standards of information sharing would be required, including across sectors
Dispute resolution	TIO membership and IDR requirements, except for transit carriers and CSPs	AFCA membership, likely increase in complaints

As outlined in Table 8, the estimated additional regulatory costs of Option 2 for the telecommunications sector would be $22.0 million in the initial year, and $14.1 million on an ongoing basis each following year. There would be a need for investment to comply with new governance, information sharing and EDR arrangements. There would also be costs associated with an increased number of scam complaints each year, with a higher level of fees required by AFCA.

Table 8 – Option 2 Estimated annual regulatory burden on telecommunications providers ($m)

Entity type	Entities	Initial cost	Ongoing cost
Major telcos	4	$5.4	$4.5
Medium CSPs	18	$1.8	$1.4
Small CSPs	150	$5.2	$2.8
Very small CSPs	241	$8.3	$4.6
Transit carriers / CSPs[40]	32	$1.3	$0.8
Total	**445**	**$22.0**	**$14.1**

4.1.3 Digital platforms

Option 1 – Status quo

Some major digital platforms in Australia have agreed to voluntary measures to address online scams through the AOSC. DIGI, the industry body representing the digital industry in Australia, has voluntary industry anti-scams standards and is developing internal dispute standards in response to a request from the government.

Under the status quo the AOSC would see a voluntary uplift in anti-scam activities in signatory digital platforms. It would encourage progress on anti-scam measures including verification measures for advertisers, mechanisms for user reporting of scam content, and agreements to co-ordinate actions with the NASC.

[40] Transit carriers/CSPs are included in this entity type category, and not under the other categories above.

As a voluntary code, industry actions are not enforceable and there are no obligations if signatories fail to meet commitments under the AOSC. Other observed limitations to the application of the AOSC include that:

- There are no defined timelines for full implementation of commitments or details on how DIGI will monitor and evaluate the effectiveness of actions taken by signatories to consider compliance with the AOSC, beyond processes for AOSC review and amendment.
- The AOSC contains principles limited by other terms of use, policies or conduct rules of the entity. Whilst signatories are also committed to address initiating scams in these instruments, it gives latitude to industry to define what content would attract the operation of the AOSC.

Information sharing arrangements across industry to address scams in Australia is nascent, with some digital platform membership of the AFCX and Intel Loop. The AOSC provides a general commitment to work with relevant stakeholders to share information and respond to information requests with Government agencies, law enforcement and industry. However, due to limited details on these commitments including specifics on the nature of collaboration and information sharing, the AOSC may leave inconsistent ways in which digital platforms are interacting with them.

While options for a mandatory IDR and EDR regime for digital platforms are being developed for future consideration by Government, currently the sector is not subject to any such mechanisms. As a result, the status quo options would leave consumers with limited options to seek support or redress from digital platforms where they have been subject to a scam on their service.

Option 2 – Scams Prevention Framework

The SPF would designate digital platform services, initially offering social media, direct messaging and paid search advertising services, comply with principles-based obligations. A snapshot of potentially regulated digital platforms is outlined in Table 9.[41]

Table 9 – Potential regulated digital platform services[42]

Known services	Examples
~10 social media services	Facebook, Instagram, YouTube, TikTok, Pinterest, Twitter, Reddit, LinkedIn, BeReal
~19 direct messaging services	Facebook Messenger, WhatsApp, SnapChat, Signal, iMessage, Zoom, Slack, Discord, WeChat
~2 paid search advertising services	Google Search, Bing Search

Due to the broad range of regulated services in this sector, and that sector-wide action to combat scams has not been as co-ordinated to-date as in other sectors, greater uplift can be expected to meet compliance with the SPF. Whilst the voluntary AOSC would encourage the uplift of anti-scam activities in relation to services covered by the AOSC that are offered by the signatories, the SPF would mandate a stronger uplift to address scam activity in designated services provided by digital platforms. In addition to general obligations relating to governance and information sharing, businesses may undertake the following actions to demonstrate compliance with the SPF:

- Prevention activities, including greater verification of user accounts, and clear information and warnings to service users about scam activity and providing users with the options to manage their exposure to content at a higher risk of being a scam, such as receiving messages from unknown accounts.

41 Further detail on assumptions used to estimate the number of relevant services is included in Appendix 2 – Regulatory cost calculations.
42 This list is illustrative and is not intended to represent the intended scope of the definitions for the designation of these services, which would require further development after the SPF is legislated. These definitions would involve further consultation before designation of the sector by the Minister.

- **Detection activities**, including the use of appropriate tools and technologies to proactively identify accounts, content and advertisements that are likely to be associated with scam activity.
- **Disruption activities**, involving greater content moderation including suspension of accounts, content and advertisements reported by users, other entities, and regulators, and removing those accounts and content within a reasonable period if verified as a scam.
- **Responses to scams**, including to have an accessible mechanism for consumers to report scams, an accessible and transparent IDR mechanism and membership of an EDR scheme.

Under Option 2, designated digital platforms would be required to have in place an IDR mechanism that is accessible and transparent for users, and comply with any requirements related to IDR set out in the sector codes (including timeframes for response to a consumer complaint). Designated digital platforms would be required to become a member of AFCA if they are providing a service that is regulated by the SPF.

Areas where there would be uplift required additional to current initiatives of entities in the digital platforms sector are summarised in Table 10.

Table 10 – Digital platforms sector initiatives and uplift required for Scams Prevention Framework

Obligation	Current initiatives for AOSC signatories	Uplift required
Anti-scam activities	Voluntary AOSC commitments to develop internal anti-scams strategy and procedures	Develop anti-scams activities, with oversight and governance measures for continuous improvement
Information sharing and reporting	Commitments to share information and respond to requests under the AOSC and engage with the NASC	Higher standards of information sharing would be required, including with other sectors
Dispute resolution	No mandatory requirements	Accessible and transparent IDR mechanism available to consumers and AFCA membership

As outlined in Table 11, the estimated regulatory costs of Option 2 additional to the status quo for the digital platforms would be $106.0 million in the initial year, and $42.1 million on an ongoing basis each following year. Most of this regulatory cost burden would be on the major digital platforms offering social media, paid search advertising and direct messaging services. Digital platforms would be required to undertake investment in anti-scam activities to comply with new obligations under the SPF, beyond activities committed to under the AOSC including governance, information sharing, IDR and EDR arrangements. Digital platforms which are not signatories to the AOSC would be expected to incur a higher level of costs to implement anti-scam activity improvements.

Table 11 – Option 2 Estimated annual regulatory burden on digital platforms ($m)

Entity type	Entities	Initial costs	Ongoing costs
Major platforms - AOSC	5	$43.7	$16.8
Major platforms - non-AOSC	2	$21.8	$9.6
Medium platforms - AOSC	2	$5.0	$1.8
Medium platforms - non-AOSC	12	$35.4	$14.0
Total	**21**	$106.0	$42.1

4.1.4 Consumers

Consumers need to engage with new or changed processes that entities often introduce in their services to strengthen protections from scams.

These processes, referred to as frictions, are intended to make services safer or slow the pace of services to make it more difficult for scammers to succeed in causing harm to consumers. For example, for the banking sector frictions involve the use of limits, holds, and delays to reduce risk in transactions, including those to new payees. For digital platforms, such similar process which create frictions for consumers could include account holder verification, two-factor account identification and delays in sending messages, posting advertisements or social media content.

There are known inconveniences and issues regarding frictions as not all consumers will perceive the value or benefit of the friction. These frictions can create costs for doing business through the introduction of inconvenience and delays in using regulated services or platforms, including administrative impost for users and may reduce the efficiency of urgent digital interactions. However, survey responses from Treasury and Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)'s public consultation and industry sentiment suggests that consumers may be willing to accept additional frictions in order to be better protected from scams.

Option 1 – Status quo

Under the status quo, the accountability for scam activity would fall inequitably across the scam ecosystem with banks and payment providers (the point where the financial loss is most frequently recognised) giving rise to greater risk-aversion in undertaking banking with customers or introducing more excessive frictions in their consumer services.

Absent clear obligations or controls, entities may use measures at their disposal to mitigate risks in ways undesirable to consumers in terms of access to and efficiency of their services more generally, but particularly in banking services. This may involve banking and other services imposing higher costs on higher risk consumers and businesses, including additional fees and in some cases stricter limitations on service offerings.

Option 2 – Scams Prevention Framework

The costs on consumers of frictions may increase due to entities uplifting their anti-scam activities to comply with their SPF obligations under option 2. Such anti-scam actions may result in additional time, cost, resources and effort required to use services of banks, telecommunications providers and digital platforms. However, the relative impact compared to frictions expected under the status quo is uncertain and difficult to quantify.

Frictions may be affected in each sector as follows:

- In banking services there could be minimal impact given the prominence of existing anti-scam measures. In comparison to the status quo option 2 may lead to either an increase or

reduction in prominence of frictions; as a result of clearer accountability and coordination across the ecosystem altering the need for delays and verification in banking activities.

- In telecommunications services there may only be minor impacts on consumers compliance costs given the current and planned levels of anti-scam actions.
- For digital platform services in social media, paid search advertising and direct messaging there may be a greater level of frictions for consumers, potentially relating to obligations to improve identification verification processes or user verification requirements on platforms which do not currently have these in place.

Many services which would be directly regulated by the SPF such as digital platforms and bank transaction accounts do not involve direct prices on consumers. Regulated entities may pass on a share of the costs of complying with increased regulation potentially through higher consumer prices or onto other users of the service such as businesses. As costs would be spread across various entities and industries the overall effect on prices experienced by consumers may be negligible, and outweighed by lower burden on consumers to engage in their own administrative or external security measures to help them avoid falling victim to a scam.

Given the high level of uncertainty over whether the net change in consumer costs would be an increased or decreased burden, they are assumed to be negligible under option 2.

Under option 2, consistent with status quo, consumers would not be charged any fees for taking their scam complaints to AFCA and would not incur costs for EDR.

4.1.5 Overall regulatory costs

Option 1 – Status quo

As Option 1 represents the status quo it does not involve additional regulatory costs relative to current commitments across industry.

Option 2 – Scams Prevention Framework

In the initial year implementing Option 2 would involve $228.8 million in regulatory costs including $100.9 million for banks, $22.0 million for telecommunications providers and $106.0 million for digital platforms. Each following year ongoing these regulated entities would incur $88.0 million of regulatory costs including $31.8 million for banks, $14.1 million for telecommunications providers and $42.1 million for digital platforms.

Table 12 outlines the overall regulatory costs expected to be involved in implementation of Option 2. On average over the first 10 years industry would be expected to incur $102.1 million in annual regulatory costs across the 3 sectors designated under the SPF (($228.8 million + 9 x $88.0 million)/10). Individuals and community organisations would not be expected to incur a net change in costs as these impacts are assumed to be negligible.

Regulatory burden estimate (RBE) table

Table 12 – Annual regulatory costs (from business as usual) over first 10 years of implementation

Change in costs ($ million)	Business	Community organisations	Individuals	Total change in costs
Total, by sector	$102.1	Nil	Nil	$102.1

4.2 Government costs

Option 1 – Status quo

As Option 1 represents the status quo it does not involve additional costs for government relative to the current arrangements. However, from the government's perspective, as the scams problem grows, the resources required to address issue at a later point in time will also grow.

Option 2 – Scams Prevention Framework

As announced in the 2024-25 Budget, the government would provide $37.3 million for the introduction of mandatory industry codes to be established under a SPF over four years from 2024–25.[43] This includes $8.6 million per year ongoing for government regulators to administer and enforce mandatory industry codes for regulated businesses to address scams on their platforms and services, initially targeting telecommunications, banks and digital platforms services relating to social media, paid search engine advertising and direct messaging.[44]

To implement a single EDR scheme for scam disputes for the three initial regulated sectors under the SPF would involve seed funding of $14.7 million over two years from 2024-25 for AFCA to expand its jurisdiction and establish its capacity to handle SPF disputes. There would no ongoing government costs. Once established, AFCA would recover its operating costs from its members.

As outlined in Table 13, government costs for the initial year would be $26.2 million for establishing the SPF and AFCA's expanded jurisdiction, followed by $8.6 million each year to administer the SPF.

Table 13 – Annual government costs ($ millions)

	Initial	Ongoing
Administering and enforcing SPF obligations	$11.5	$8.6
AFCA – establish single EDR scheme for 3 initial sectors[45]	$14.7	$0.0
Total	**$26.2**	**$8.6**

4.3 Benefits

4.3.1 Reducing exposure to scams

Option 1 – Status quo

There would be two key factors limiting future reductions in exposure to scams under the status quo policy settings: lack of clear industry obligations and lack of co-ordination across the economy.

Option 2 – Scams Prevention Framework

Clear obligations on regulated entities

The primary objective of the SPF is to set clear roles and responsibilities for the Government, regulators, and the private sector in combatting scams. The key benefit of the SPF is that mandatory

43 Treasury (2024) Budget 2024-25 Paper 2, Part 2: Payment Measures, Page 180

44 Prior expenditure announced in the Budget 2023-24 for Fighting Scams (Budget Paper 2, page 211) included "$58 million over years from $86.5 million to establish the NASC within the ACCC to improve scam data sharing across government and the private sector and to establish public-private sector Fusion Cells to target specific scam issues." Although this prior investment would facilitate information sharing and coordination activities under the SPF, these activities are not wholly dependent on the SPF being implemented and therefore not calculated as a direct government cost related to implementing the SPF.

45 AFCA will receive $14.7 million over two years from 2024-25. That is, $5.2 million in 2024-25 and $9.2 in 2025-26.

and consistent standards across industry sectors will uplift anti-scam activities and in turn reduce exposure to scams for consumers.

Uplifting these anti-scam activities to a consistent standard across the designated sectors of banking, telecommunications and digital platforms would result in more consistent consumer protections across the Australian economy. This would result in lower frequency of scam activity reaching consumers and reduced losses to scams, as has been demonstrated by industry activities including:

- Under the Reducing Scam Calls and Scam SMs industry code telecommunications providers have blocked 1.5 billion scam calls and 668 million scam SMS between July 2022 and June 2024.[46]
- Google reported blocking or removing 206.5 million advertisements which violated their misrepresentation policy in 2023, including many scams.[47]
- Meta conducted a targeted search for scam investment ads in July 2024 which resulted in nearly 20,000 such scam ads being identified and removed.[48]

Ensuring consistency across the sectors in which scams operate would also reduce the potential movement of scam activity to other sectors. The use of mandatory obligations would deliver a benefit over the status quo as there are recognised gaps in existing anti-scam policies and procedures.[49]

Coordination of anti-scam actions

The SPF would enhance information sharing arrangements to enable more efficient and timely sharing of information critical to support government regulators and industry to effectively protect consumers against scams. Sharing information would enable regulators and businesses to act quickly to prevent and disrupt the scam occurring, to mitigate the impact of the scam and/or prevent future scams. This would also include information sharing with law enforcement and government agencies via the government regulator.

For example, the SPF would enable a bank that is notified it has facilitated the transfer of funds through a scam into an account at another bank to report details about both the sending and receiving account holders to the regulator. The information would then be provided to other regulated entities so that prompt action can be taken to disrupt other transfers to the scammers receiving account and attempt to recover the funds. Sharing scam information across the ecosystem could also enable a social media service provider to quickly remove an advertisement or suspend an account suspected to be associated with scam activity reported by the bank to prevent further consumers from being impacted.

These capabilities would build on other coordination activities which have been effective in reducing scam exposure, including the following:

- ASIC's website takedown service has worked with other government agencies and industry to coordinate the removal of over 5,530 fake investment platform scams, 1,065 phishing scam hyperlinks and 615 cryptocurrency investment scams between July 2023 and August 2024.[50]
- The Optus 'Call Stop' program targets call back scams by diverting calls to scam phone numbers identified by banks and their customers, operated through the AFCX.[51]
- The NASC investment scam Fusion Cell brought together 43 organisations to identify and block investment scams including banks, social media platforms, payment platforms, trading

46 Calculated from ACMA's "Action on telco consumer protection" quarterly reports from the July to September 2022 to April to June 2024.
47 Google 2023 Ads Safety Report, 27 March 2024
48 Meta's Submission on the Scams Prevention Framework Bill 2024, 4 October 2024.
49 An outline of these identified gaps in regulator investigations into industry practices in the banking and digital platforms sector is included in **Appendix 1.**
50 ASIC, *Online investment trading scams top ASIC's website takedown action,* 19 August 2024.
51 Optus, *Optus Call Stop to fight off SMS scams*, 17 July 2023.

platforms, investment services, telecommunications providers and government agencies. Between August 2023 and February 2024, the Fusion Cell's information sharing activity resulted in 1,000 instances of scam advertisements, advertorials, and videos being removed by digital platforms, takedown of 220 scam websites and diversion of 113 call back scams.[52]

- Between April and May 2024 Meta engaged in an intelligence sharing initiative with the banking industry through the Fraud Intelligence Reciprocal Exchange, via the AFCX. Meta was able to act on 102 scam reports to conduct a wider investigation, resulting in the removal of over 9,000 pages and over 8,000 AI-generated celeb-bait scams.[53]

4.3.2 Reducing scam losses

Option 1 – Status quo

Inaction from Government to close gaps in the ecosystem targeted by scams would continue to expose Australians to vulnerabilities and high volumes of scam activity and resulting financial, psychological and social detriment.

Option 2 – Scams Prevention Framework

Reducing exposure to scams under option 2 would result in reduced scam losses. In addition to the benefit of Option 2 in reducing exposure to scams resulting in reduced losses to scams, there are particular actions related to the SPF principles which would result in lower amounts being lost to scams once a consumer has been exposed to a scam or a scam is underway. Option 2 would uplift the capability of regulated entities across the chain of services involved in a scam, improving the likelihood scam activity can be prevented, disrupted and potentially amounts recovered. This would result in reduced losses in the Australian economy.

There is evidence that uplifts to anti-scam activities consistent with potential obligations under the SPF have resulted in measurable benefits to industry and consumers, indicating that creating consistent standards for these uplifts in capacity through mandatory obligations would result in further reductions in scam losses. In the banking sector, major banks have announced that their existing measures have diverted millions of dollars from being lost to scams and fraud.[54] Table 14 outlines a summary of reported scams losses prevented due to anti-scam activities in the banking sector.

Table 14 - Reported banking sector savings due to disruption of payments to scammers

Bank	Measure	Description	Value
ANZ	Overall	Jan 2023 – Oct 2023	$100-120 million[55]
Bendigo Bank	Blocks	2022 – 2023	$39 million[56]
Commonwealth Bank	Customer verification	Mar 2023 – May 2023	$11 million[57]
NAB	Overall	Jan 2023 – Apr 2023	$270 million[58]
Westpac	Blocks	Jan 2022 – May 2023	$131,000[59]

52 NASC, Investment scam fusion cell, Final report, May 2024.
53 Meta, *Meta partners with the Australian Financial Crimes Exchange (AFCX) and Australian banking sector to combat scams*, October 2024. https://medium.com/meta-australia-policy-blog/meta-partners-with-the-australian-financial-crimes-exchange-afcx-and-australian-banking-sector-to-7b7b26227360
54 ANZ, *The price of security is vigilance,* 2023; Commonwealth Bank, *Annual Report 2023*
55 ANZ, *We are in the fight against scammers together* (26 October 2023); *The price of security is vigilance* (27 November 2023)
56 Bendigo Bank, *Bendigo Bank says collaboration is key to fight against scams and fraud* (24 November 2023)
57 Commonwealth Bank, *CBA steps up national battle against scams* (30 May 2023)
58 NAB, *NAB's scam alerts intervene in $270 million worth of payments* (17 June 2023)
59 Westpac, *Westpac trials new cryptocurrency blocks to prevent scam losses* (18 May 2023)

Westpac	Customer verification	Mar 2022 – May 2023	$250,000[60]

As an example, the Commonwealth Bank introduced a NameCheck confirmation of payee system in February 2023[61] which diverted 10,000 scam payments valued at over $38 million between March to September 2023.[62] This technology, which is licensed to other entities, has led to benefits reflected in reducing customer losses by a third over 6 months.[63]

There is also evidence that Government and regulator intervention is reducing the trajectory of scam losses as outlined in section 2.2.1.

4.3.3 Improving redress of scam losses

Option 1 – Status quo

This option would not achieve an economy wide understanding or agreement on responsibilities in responding to scams. As a result, consumers will continue to be subject to the imbalance of power they face in requesting a service provider investigate or accept a proportion of accountability for a scam loss.

Option 2 – Scams Prevention Framework

The SPF would impose clear obligations on regulated entities, provide clear pathways for consumers to seek redress and ensure consistency in consideration of scams complaints. Under the SPF, responsibility for redress will sit with all regulated entities where they have not taken appropriate action. This would ensure the liability for scam losses is appropriately allocated across the ecosystem.

Mandatory IDR

Under the SPF, regulated entities operating designated digital platforms would be required to have an accessible and transparent IDR mechanism for consumers to complain about scams on its services (including the entity's conduct relating to such scams) consistent with standards for banks and telecommunications providers. Effective IDR mechanisms benefit both consumers and businesses by providing regulated entities an opportunity to assess its conduct and resolve the complaints in a timely and efficient manner. The IDR obligation would encourage the early resolution of complaints, including for compensation or other remedies to be provided to consumers where there has been a breach of their obligations under the SPF.

Mandatory EDR

Entities that are providing a service that is regulated by the SPF will be required to become a member of the EDR scheme for their sector. An EDR scheme offers a no-cost, independent and fair mechanism for consumers to escalate their complaint when they are not resolved at the IDR stage or if the IDR outcome is unsatisfactory. An effective ombudsman also incentivises regulated entities to meet their obligations, knowing that consumers have an accessible pathway to seek redress.

As scammers often operate across multiple entities and sectors in their deception of consumers, a single EDR scheme offers SPF consumers a holistic experience where there are multiple regulated entities involved in complaints. It would also bring consistency in consideration of complaints and be less burdensome for SPF consumers and industry when compared with multi-scheme alternatives.

60 Ibid
61 Commonwealth Bank of Australia, *New scam detection, prevention and education initiatives to keep more customers safe,* 2023
62 Commonwealth Bank of Australia, *CBA extends scam disruption technologies as part of 'whole of ecosystem' national approach,* 2023.
63 Commonwealth Bank of Australia, *Research shows Australians are more scam-aware than 12 months ago as losses fall,* 2023.

4.4 Comparison of benefits and costs

Assessment of the of Options 2 is based on both break-even analysis and assessment of the expected relative level of benefits from each option. As previously discussed, the status quo would involve persistence of harmful costs of scams associated with personal data breaches, financial losses, psychological damages with broader socioeconomic consequences. Therefore, the net benefit is an assessment of whether their implementation costs are outweighed by the level to which they reduce these scam harms.

Option 2 – Scams Prevention Framework

Break-even analysis

As outlined in the **4.1.5 Overall regulatory** costs and **4.2 Government** costs sections, the average annual costs to implement Option 2 over the first 10 years will be $112.5 million ($102.1 million in regulatory costs plus $10.4 million in government costs). Given the average scam victim in Australia reported losing $16,000 in 2023,[64] for Option 2 to result in a net benefit to society (based on reduced financial losses to scams alone) the number of instances of consumers experiencing a scam loss would need to reduce by 7,028. This is equal to 4.6 per cent reduction of the $2.7 billion of reported scam losses in 2023.[65]

Likelihood of achieving a net benefit

As Option 2 would substantially improve the regulatory framework for industry anti-scam activities and improve industry practices in responding and sharing scam information, it would be broadly expected to reduce instances of scam losses by at least 7,028 resulting in the benefits of this option outweighing the costs associated with its implementation.

As outlined above, there is evidence that uplifts to anti-scam activities have resulted in reduced measured scam losses. Although the level of further scam losses which could be avoided is uncertain, it is reasonable to assume that strengthening of scam protections, including coordination across the scam ecosystem, would result in further reductions in scam losses. Therefore, although quantification of the level of benefit is not possible given the current level of evidence available, it would be more than that likely Option 2 would result in a net gain for Australian society.

In addition, Option 2 is highly likely to reduce exposure to scams, improve redress of scam losses and provide benefits in addition to those directly related to reducing scam losses. Although these additional benefits are also unquantifiable for the purposes of this analysis, they would likely substantially increase the level of net benefit associated with Option 2.

64 ACCC, Targeting Scams report 2023.

65 Note the of scam losses in Australia may be expected to change in the future under Option 1 - status quo. If the number of scam victims would rise under the status quo (as is likely given assessment outlined in the Section 1) this percentage represents an overestimate of the reduction in scam losses required to result in a net benefit.

5. Consultation

Extensive consultation was undertaken to inform the design, objectives and challenges policy interventions on scams may encounter, as well as to gauge industry and civil society's attitudes toward the proposed options.

5.1 Initial public consultation

Treasury and DITRDCA consulted on a comprehensive scams framework from 30 November 2023 to 29 January 2024.[66] Consultation involved seeking feedback on a paper that outlined a Scams Code Framework with proposed principles, features and sector-specific obligations for banks, telecommunication providers and digital platforms to adhere to in an effort to combat scams. To complement the consultation paper, a survey was released to seek feedback from members of the public on their personal experience with scams, as an alternative to providing a written submission.

As part of consultation, roundtables and bilateral meetings were held with key stakeholders. This included digital platforms, telecommunications, consumer and banking roundtables; and a regulator workshop with the ASIC, the ACCC and the ACMA.

There were 67 written submissions received (including 13 confidential submissions) from banks and financial services, digital platforms, telecommunication providers, consumer and other advocacy organisations, external dispute resolution bodies and regulators. Non-confidential submissions are published on Treasury's website. The public survey received 203 responses.

In response to consultation, businesses did not provide estimates of the quantum for anticipated costs to meet the standard of the proposed policy. Reasons for this include a reluctance to provide estimates or commit funding without greater detail on expectations from Government and guidance from regulators.

Key themes and findings

Consultation paper

Stakeholders generally supported the policy intent and design of the Framework. This included general support for a two-tiered model characterised by an overarching framework with principles-based obligations and mandatory sector-specific codes. Stakeholders generally agreed the definition of a 'scam' and 'consumer' should be legislated, with suggestions for refinement in order to capture the appropriate consumer and scam activity.

Stakeholders agreed that banks, telecommunication providers and digital communication platforms be captured in the initial scope, noting it will be expanded to other sectors later and suggesting rapid integration of several further sectors. Given the complexity of multiple regulators enforcing different sector-specific codes, stakeholders noted how regulation and enforcement across the ecosystem may differ. Banks and telecommunication providers supported an anti-scam strategy requirement and other stakeholders recommended making certain changes to the obligations, to reduce the reporting burden on businesses. Digital platforms expressed a desire for the creation of industry-developed codes and suggested voluntary approaches. Through DIGI, entities expressed encouragement for further engagement to clarify the scope of services relevant to the framework and associated definitions.

Industry stakeholders welcomed dispute resolution processes, particularly banks and telecommunication providers with existing EDR regimes. Some stakeholders including digital platforms

[66] The Department of Treasury, *Scams – mandatory industry codes,* 30 November 2023 – 29 January 2024

noted further work would be required on determining the requirements on businesses and scope for stakeholders to seek redress, as well as determining an appropriate external dispute resolution body. Consumer advocates generally supported the intent of dispute resolution processes, although expressed a desire to streamline the consumer journey through dispute resolution and avoid complexity or delay with disputes. In terms of penalties and enforcement, stakeholders largely supported a consistent approach to enabling regulators with appropriate tools and penalties for non-compliance.

Consumers and consumer advocates recommended obligations on banks be introduced for mandatory reimbursement of consumer losses in addition to the proposed framework of mandatory and enforceable industry codes. The recommendation was proposed as a way to incentivise primarily the banking industry to take greater steps to reduce scam-related risks in the banking and payments system to mitigate the impacts of losses stolen from Australians by scammers. For instance, a joint submission by the Consumer Action Law Centre, CHOICE and The Australian Communications Consumer Action Network recommended a strong presumption of reimbursement for consumer losses by the bank apply, with a corresponding mechanism for banks to seek to recover a portion of these costs from other regulated entities where those entities' actions have contributed to the scam occurring. This recommendation was considered in the policy development process, particularly as a partially related model has been adopted in the United Kingdom. The recommendation to introduce mandatory reimbursement by banks as an additional component to the framework of mandatory industry codes is not appropriate to be assessed as an additional component to option 2 in this IA as it would predominantly place an additional presumption of liability of scam losses and costs for resolution of redress apportionment onto one sector, with minimal corresponding additional incentives for other sectors to recognise liability for not meeting their obligations. This approach would not effectively address the key policy objectives to align industry responsibilities for scam prevention with the presence of scam activity on platforms and services across the economy and would not further incentivise co-ordination of anti-scam responses (see section 2.2.2). The design of the redress arrangements in government's framework will consider consumer advocates feedback to look to make the dispute resolution and redress process as consumer focused as possible, while maintaining the objective of aligning responsibility for liability and obligations for scam prevention across the economy.

Consumer survey

Respondents broadly expressed their challenges with reporting and managing scam complaints to businesses, such as delays in responses and poor visibility of actions taken by the businesses. Respondents were most exposed to and were victimised by phishing, false billing and online shopping scams. Phone calls and text messages were the most common medium for scams.

Respondents supported the need for greater industry accountability and suggested improvements in access to reporting, account authentication and verification and information sharing. Respondents support the current regulatory action, including the centralised approach to data reporting, compliance activities and co-ordination via the NASC. To supplement existing action, respondents recommended measures to improve consumer education and digital literacy and greater law enforcement.

In terms of sector-specific obligations, respondents called for banks to improve methods to create and verify new accounts and improve processes to recall user funds; for telecommunication providers to address scam texts and calls and prevent the registration of scam numbers; and for digital platforms to restrict reported accounts, such as accounts with false and misleading advertisements, and improve customer service responses.

5.2 Targeted consultation

Post-consultation in January, Treasury and the DITRDCA continued to lead the policy development process and sought feedback on the proposed features of the policy for the public consultation. The ACCC, ASIC and ACMA were also regularly engaged with Treasury in developing the regulatory and administrative aspects of the proposed SPF under option 2.

Treasury also engaged with key private sector stakeholder groups including the Communications Alliance, AFCX, ABA, COBA and DIGI on key aspects of the policy development throughout 2024.

Key themes and findings

Targeted discussions informed the policy development process. They represented opportunities for entities and representative bodies to explore initiatives in relation to the development of standards to prevent, detect, disrupt and respond to scams.

Input was specifically sought on the regulatory costs which were likely to be incurred by regulated entities in complying with new obligations under the SPF. Responses were received with reference to investments previously undertaken to initiate anti-scam procedures and information sharing systems, as follows:

- Obligations for information sharing with the government regulator were identified to be similar in nature to those required under the Consumer Data Right, which is also administered by the ACCC. However, the likely level of cost burden from information sharing for regulated entities was indicated to be of a smaller scale given the scope for information to be shared would be more limited to scam activity, in comparison to information on customers.
- Stakeholders noted the likely level of regulatory cost would be highly dependent on prior or planned investments in anti-scam activities. In particular, entities which are already constructing information sharing arrangements such as through the AFCX would have a lower administrative burden.

5.3 Consultation on draft legislation

Treasury and DITRDCA undertook consultation on the exposure draft of legislation that established the SPF from 13 September to 4 October 2024. This process involved direct engagement through roundtables and meetings with regulators, consumer groups, industry associations and banks, telecommunication providers, digital platforms (providing social media, direct messaging and paid advertising search services) and other relevant stakeholders.

To inform analysis of the regulatory impacts of option 2, consultation materials included a paper outlining consultation questions for stakeholder,[67] including the following requested input from stakeholders:

"If possible, please include a breakdown of the following including upfront and ongoing impacts:

- uplift in administrative processes (including staff capacity building),
- change management and education support costs,
- governance costs,
- technology uplift, including for data-sharing requirements,
- building and maintaining appropriate mechanisms to meet IDR and EDR requirements,
- additional costs, time, resources or effort for consumers, and
- any other expected compliance impacts."

67 Treasury, Scams Prevention Framework – exposure draft legislation, Summary of reforms document, page 12.

Key themes and findings

Direct engagement identified the following key issues with the design of the proposed SPF policy:

- Concern about the interaction between obligations under the SPF principles and sector specific codes, and coordination between the regulators.
- The legislative structure may not allow for adequate tailoring of obligations to specific sectors.
- Industry representatives discussed a desire to align obligations with existing industry codes or instruments, such as the Scam-Safe Accord, Reducing Scam Calls and SMs Code, and DIGI's AOSC.
- Concern that reporting obligations would drive a high volume of reports which in turn may not be useful to support disruption activities.
- Concern that consumer warning obligations may lead to a high volume of warnings and be ineffective.
- A lack of clarity regarding liability for compensation, including apportionment between regulated entities.
- Concerns about the effective operation of dispute resolution, including how regulated entities may work together at the IDR stage.

Stakeholders did not provide estimates of additional regulatory costs expected to be incurred by regulated entities or consumers. However, they provided qualitative feedback including:

- Expect to have increases in reporting and compliance costs for regulated entities. These costs would include implementing the new annual certification regime, system enhancements, additional resources for IDR, staff training and change management costs.
- Participants in existing industry initiatives were expected to have a lower level of regulatory burden. Entities that already have information sharing arrangements such as through the AFCX and ACMA would already be developing the infrastructure to support it under the SPF.
- There would be substantial burdens on smaller entities to implement SPF obligations, which have more limited personnel and technology resources. There were concerns this would put smaller entities at a competitive disadvantage.
- Entities may face overlapping obligations with existing IDR/EDR requirements, the Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) regime and existing industry codes.
- Increased costs are likely to be passed onto consumers, making it important initiatives are efficient and proportionate to scam risk. Stakeholders suggest existing frameworks be recognised to reduce inefficiencies and minimise additional compliance costs.
- Digital platforms discussed that completely new obligations, such as the development of pathways for dispute resolution arrangements, would have a disproportionately higher impact on the sector to develop and implement than other sectors with existing systems.
- Transitional arrangements would be required to enable entities to undertake uplifts in capabilities prior to obligations being enforced.

5.4 Future consultation

To proceed with option 2, following the finalisation of the legislation there would be several consultation processes undertaken to further refine the policy design:

- consultation on the instruments to designate the initial target sectors;
- consultation on the design and implementation aspects for EDR to be operated by AFCA to deliver whole-of-ecosystem external dispute escalation approach, and integrated with IDR processes;
- consultation on the obligations in the banking sector code;

- co-development between ACMA and the Communications Alliance of obligations in the telecommunications sector code, informed by experience with the current *Reducing Scam Calls and Scam SMs* code; and
- consultation on the obligations in the digital platform sector code.

5.5 Evaluation of the consultation process

How feedback was incorporated into policy design

In response to general support from stakeholders, key design aspects of the SPF under option 2 have been retained. Namely, the two-tiered model with its initial designated sectors (along with the intention of expanding of the framework to future sectors). Certain aspects of the SPF were modified in consideration of stakeholders' suggestions, for instance, stakeholders noted the importance information sharing and reporting and encouraged consideration of how to remove duplication between the multiple sectors and regulators involved in implementation of the SPF. As a consequence, the option has been adjusted to establish a streamlined overarching principles-based obligation for reporting and information sharing, with further details to be clarified outside of primary legislation.

The digital platforms sector has expressed concerns that the proposed definition[68] of "digital communication platforms" was too broad and may capture entities, such as news, music, audiobooks or podcast aggregators, on which scams may not occur. The SPF has been subsequently modified to capture social media, messaging and search advertising services.

Concerns about risks of burdens on smaller regulated entities identified by stakeholders are to be mitigated by enabling the SPF the flexibility to tailor obligations to the size, structure and operations of the entities. Differences in capabilities would be accounted for when providing further detail on obligations under the SPF principles and sector-specific code obligations. Similarly, transitional arrangements for penalty provisions across the framework would also be considered, noting the uplift that is required in capability and infrastructure to adhere to obligations. This must be balanced against the need for immediate and coordinated action to respond to the threat of scam activity and protect SPF consumers.

Feedback on the primary areas for expected additional regulatory costs has been checked against IA assumptions. Stakeholder feedback broadly aligns with assumptions used for costs for regulated entities.

Limitations

The design of the public consultation paper was high-level in nature as it aimed to assess the capabilities of and sought broad advice on a comprehensive model. Similarly, consultation on exposure draft legislation focused on the over-arching design of the SPF legislation. Subsequently, the opportunity to ask more specific questions to refine details on certain elements, like sector-specific codes' details and their impacts, was limited. Regulatory costs estimated in this IA were not able to be tested with stakeholders and industry was also not able to quantify their compliance costs which may be a result of the range of questions raised that diverted capacities.

The public consultation begun on 30 November 2023 and concluded on 29 January 2024 which coincided with major holiday celebrations that may have influenced stakeholder capacities. Likewise,

68 It was initially proposed for digital communication platforms to cover content aggregation, connective media and media sharing services.

the consultation on exposure draft legislation ran for 3-weeks due to time constraints in the legislative development process.

6. Preferred option

6.1 Comparison of options

Option 2 is preferred. The benefits of implementing a coordinated approach to mandatory industry codes, information sharing and a single EDR scheme under option 2 have been assessed as making it the preferred option in comparison to the status quo under option 1. Option 2 is preferred as it has been assessed to result in better outcomes for the 2 core objectives of government action outlined in section 2.2.2: reduce scam harms and align benefits and costs of scam prevention.

1) Reduce scam harms

The key benefit of option 2, is that mandatory and consistent standards across industry sectors will uplift scam prevention activities and in turn reduce exposure to scams for businesses and consumers.

Under the status quo there may be some improvement in actions from entities to reduce exposure to scams, but inaction from Government to close gaps in the ecosystem targeted by scams would continue to expose Australians to vulnerabilities and high volumes of scam activity.

Option 2 would provide substantial improvement toward creating clear obligations on regulated entities and coordination of scam prevention activities. Option 2 would uplift the capacity for regulated entities across the chain of services involved in a scam, improving the likelihood scam exposure does not lead to financial loss. Uplifts to scam entity disruption activities and information sharing between entities would result in more scam activity being circumvented before amounts are transferred to a scammer.

While there may otherwise be continued progress on voluntary information sharing and anti-scam activities, the status quo would not involve the level of uplift or coordination of option 2. Similarly, under the status quo there would not be the benefit of ecosystem-wide improvements and it may involve risks of such a system being exploited by scammers.

The proposed SPF under option 2 addresses a variety of socioeconomic challenges which arise from scams through introducing a cohesive overarching structure to Australia's response to scam activity supported by government. Establishing a coherent government framework would provide a consistent message in relation to consumer protections for scams (see section 2.1.3). This would assist in improving confidence for engaging in communications and economic activity, and understanding there are structures in place for acting on evolving scam activity into the future.

2) Align benefits and costs of scam prevention

Given the role of different types of entities offering services vulnerable to scams across the Australian economy, it is preferable to pursue an approach which does not inequitably burden one sector with the regulatory burden of complying with scam prevention and response obligations. Allocation of incentives across the scams ecosystems associated with option 2 make it preferable to the status quo Option 1 would not result in alignment of the benefits of anti-scam activity as protections, with incentives currently more concentrated on banking services and major entities rather than across entities in the scam ecosystem.

Option 2 involves aligning the imposition of costs across the economy with where there would be benefit from scam prevention activity. Option 2 would involve regulatory burden improving anti-scam activities and complying with mandatory obligations spread across the initially designated sectors of banking ($38.7 million average over the first 10 years), telecommunications ($14.9 million) and digital platforms ($48.5 million), and then potentially onto designated future services where scams are occurring. Within these sectors, costs are expected to be aligned with the extent there are

opportunities for certain categories of entities to uplift their anti-scam activities and engage in improved information sharing arrangements and EDR.

The single EDR scheme proposal under option 2 takes a whole-of-ecosystem approach. This ensures responsibility for redress will sit with all entities regulated under option 2 where they have not taken appropriate action. This would ensure the liabilities for redress for scams are allocated across the ecosystem, including digital platforms who currently do not have EDR arrangements in place and remain a point of vulnerability in the scams ecosystem.

6.2 Implementation of Option 2 – Scams Prevention Framework

To implement option 2 legislation would need to be passed to establish the legal status of the SPF and enable the establishment of mandatory industry codes for scam prevention. The SPF would introduce mandatory requirements to combat scams in all sectors in the economy, initially applying to designated sectors in telecommunication providers, banks and digital platform services relating to social media, paid search engine advertising and direct messaging. Future sectors will be considered as scam methods and trends adapt and the SPF matures.

The SPF would be introduced as part of a broader effort to modernise Australia's laws for the digital age, including reforms to Australia's privacy, money laundering and cyber settings, the modernisation of the payment system, introduction of online safety measures, as well as the rollout of Digital ID and eInvoicing infrastructure for businesses.

Detailed obligations relating to scam prevention activities, governance, reporting and dispute resolution would be further refined to ensure compatibility with other regulatory regimes and industry initiatives. Obligations would be designed to minimise inefficiencies and regulatory burdens where appropriate.

Designation of sectors

With the SPF legislation, a designation instrument would be issued to outline the scope of entities providing services in the banking, telecommunications and certain digital platforms (social media, direct messaging and paid search advertising services) which would be obligated to comply with the SPF. This would introduce mandatory anti-scam obligations on services through which most scam activity is occurring.

Designation instruments for the first three sectors would be developed by Treasury and DITRDCA, in collaboration with industry stakeholders and other government agencies. Public consultation on the designation instruments would occur prior to instruments taking effect, to minimise risk the scope of entities covered under the SPF does not match the policy intent. The instrument may specify an application or a transition period before the SPF comes into effect to manage implementation risks.

The SPF's flexible design would enable additional sectors to be designated in the future. Prior to designating a sector, there would be consideration by Treasury and the Government of the scam activity in the sector, effectiveness of existing industry initiatives to address scams, interests of SPF consumers of the service, consequences and any other matters such as regulatory costs.

Sector-specific codes

Sector-specific codes would be developed to outline sector-specific prescriptive obligations for each sector that are consistent with the principles-based obligations. This would enable the codes to provide specific obligations tailored to the scam activity in different sectors. The codes would also

provide flexibility to adapt to new and emerging scams, reflecting the fast changing and dynamic nature of scam activity in the digital economy.

Code-making may be conducted by a Minister or a government regulator, to provide flexibility for appropriate responsibilities across relevant sectors. Consultation would be undertaken on the specific obligations in the sector-codes before they are made mandatory to ensure they are appropriately designed.

Treasury would develop the codes for banks and digital platforms. The Treasury Minister intends to delegate code making for the telecommunications sector to ACMA. ACMA would work closely with the telecommunication industry on the telecommunications sector code with DITRDCA being the relevant policy agency.

Enforcement of the code

The tiered regulatory design of the SPF would be administered and enforced via a multi-regulator model. This would deliver a whole-of-ecosystem approach to enforcement, and leverage existing regulatory relationships, monitoring and investigation frameworks already established by regulators.

The intent is that ACCC will enforce the obligations in the primary law of the framework and the digital platform service provider code; the ACMA will enforce the telecommunications code; and the ASIC will enforce the banking code.

The ACCC as facilitators of information sharing would develop appropriate guidance for reporting by regulated entities, to align with their systems, operational objectives and capabilities. Sector regulators would also develop guidance appropriate for each sector in relation to obligations under the sector codes.

Transitional arrangements for penalty provisions across the framework would be considered to enable uplift in regulated entities capabilities to be conducted. Consideration of transitional arrangements would be balanced against the need for immediate and coordinated action to respond to the threat of scam activity and protect SPF consumers.

7. Evaluation

As outlined in the need for Government action (see section 2.2.2), the objectives of the SPF are to uplift industry efforts to address scams by mandating improvements in business practices, policies, and procedures to address scams. The intended outcomes are that improvements in industry standards will reduce the impact of scams on Australians and improve industry responses and scam supports.

Evidence to inform evaluation of the SPF and success measures will include information from Government and industry sources. Industry sources include existing reporting and monitoring mechanisms undertaken by agencies and regulators to monitor of scams on regulated platforms. Metrics for success will include information through the following mechanisms:

- The NASC regularly monitors and publishes information on consumer and industry reports about scams under the Quarterly Report and Targeting Scams report.
- Agencies monitor consumer victimisation to scams, including the Australian Bureau of Statistics Personal Fraud report and Australian Institute of Criminology Cybercrime in Australia report.
- Under the current industry codes regime, the ACMA is already monitoring and evaluating telecommunications industry compliance under the Reducing Scam Calls and Scam SMs code. The SPF will enhance the current evidence base by providing greater regulatory oversight and compliance reporting that provides transparency on measures businesses are undertaking to address scams. Regulators will monitor and evaluate how regulated entities in their sector implement mandatory obligations.

Reports from government regulators including many of these metrics are published annually or quarterly which would enable evaluation of the intended objectives to reduce scam harms to be undertaken and analysis to be conducted on areas for improvement. More details on these measures and their value for evaluation of the SPF is provided in *Appendix 3*.

Due to the multi-faceted, changing nature of scams, there are risks that the above metrics for success may not be reflected by the evidence base used to evaluate the SPF. There are many factors that underpin changes in consumer reporting and losses that require proper recognition and analysis. As the lead regulator and overarching agency operating the NASC program, the ACCC has experiencing in monitoring and interpreting changes in the scams ecosystem and is best placed to consider these factors when using data and evidence to evaluate the outcomes of the SPF.

Glossary of acronyms

ABA	Australian Banking Association
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ADI	Authorised deposit-taking institution
AFCA	Australian Financial Complaints Authority
AFCX	Australian Financial Crimes Exchange
AIC	Australian Institute of Criminology
APRA	Australian Prudential Regulation Authority
AOSC	Australian Online Scams Code
ASIC	Australian Securities and Investments Commission
CDR	Consumer Data Right
COBA	Community Owned Banking Association
CSP	Carriage Service Provider
DIGI	Digital Industry Group Inc.
DITRDCA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
EDR	External dispute resolution
FTE	Full-time equivalent
IA	Impact Analysis
IDR	Internal dispute resolution
NASC	National Anti-Scam Centre
OIA	Office of Impact Analysis
RBE	Regulatory burden estimate
SMs	Short messages
SMS	Short message service
SPF	Scams Prevention Framework
TIO	Telecommunications Industry Ombudsman

Status during policy development

Point in policy development	Timeframe	Status of the IA
Government elected with commitment to implement mandatory industry codes for scam prevention	May 2022	Undeveloped.
Public consultation on a mandatory industry code framework	November 2023 - January 2024	Began collating information for analysis in IA.
Government allocates funding in the 2024-25 Budget to establish a scams code framework	May 2024	Decision informed by Draft IA. OIA reviewed the Draft IA, providing comments which were addressed prior to the decision. An OIA assessment of the Draft IA was not required.
Ongoing targeted consultation with stakeholders	May 2024 - September 2024	Further collation of information for policy design and analysis in IA. Draft IA not used as basis for this consultation.
Internal interim decision on draft legislative design	September 2024	Draft of IA sent to OIA for comments.
Consultation on exposure draft legislation for the SPF	September 2024 - October 2024	Questions related to policy design and regulatory impacts outlined in consultation documentation. Further collation of information for analysis in IA. Draft IA not used as basis for this consultation.
OIA 1st Pass Final assessment	October 2024	1st pass assessment IA completed and presented to OIA.
OIA 2nd Pass Final assessment	October 2024	OIA 1st pass assessment comments addressed. 2nd pass assessment IA completed and presented to OIA.
Final policy decision to proceed with proposal	October 2024	To be informed by IA that has been through final assessment by OIA.

Appendices

Appendix 1 – Recent anti-scam actions and dispute resolution arrangements

Banks

Examples of initiatives announced by major banks include improved approaches to confirmation of payee such as account matching and consumer alerts; new technologies and analytics to detect and disrupt unusual behaviours; and the introduction of new holds, limits and declines on payments to cryptocurrencies. Banks are also monitoring scam activity and providing consumers with pathways to report and seek support from scams.

ASIC has periodically reviewed the anti-scam policies and procedures of banks, producing two reports: the first in April 2023 reviewing the four major banks, and the second in August 2024 reviewing fifteen non-major banks.[69] In its analysis, ASIC identified that the approach to scams strategy and governance were variable between the banks. There were inconsistencies in detecting and stopping scam payments and determining liability and that victims were not always well supported.

ASIC's findings indicate areas for improvement for both major and non-major banks, but highlight the asymmetry of scam-related supports for consumers, including dispute resolution, outside the major banks.

As an industry, there has also been collective action to addressing scams. On 24 November 2023, the ABA and the COBA launched the Scam-Safe Accord[70]. The Scam-Safe Accord has six priority initiatives based on the principles of 'disrupt', 'detect' and 'respond' (outlined in Table 15) and aims to align the banking industry's approach to addressing scams. The Scam-Safe Accord applies to all members of the ABA and COBA including large commercial Australian banks, building societies and credit unions.

Table 15 – Priorities for the Scam-Safe Accord

Disrupt
Banks will deliver an industry-wide confirmation of payee solution to customers – All banks will roll out this name-checking technology so their 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 to check names is to have commenced, with rollout to occur over 2024 and 2025.
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 use behaviour detection or involve a check of a customer's face or fingerprint, enabling banks to use these characteristics to verify their customer's identity.
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, banks will ask more questions, and provide warnings and delays to reduce the risk of customers falling victim to a scam. It will act as a mitigant when scammers put customers under

69 ASIC, *Scam prevention, detection and response by the four major banks, Report 761,* April 2023; *Anti-scam practices of banks outside the four major banks, Report 790*, August 2024.
70 ABA, *Banks unite to declare war on scammers*, 24 November 2023.

pressure to act quickly to transfer funds. – Banks will work to introduce enhanced warnings and delays by the end of 2024.
Detect
Banks will invest in a major expansion of intelligence sharing across the sector – All ABA and COBA members will join the AFCX to be ready to use scams intelligence to fight scams from mid-2024, and to the Fraud Reporting Exchange over 2024-25 to help customers recover money faster. – This will allow scams intelligence to be shared at speed between banks, helping banks prevent more scams and recover funds for customers faster where possible.
Respond
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. – More banks will limit payments to high-risk channels such as some crypto currency platforms to protect customers from possible theft.
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.

Under section 912A of the Corporations Act 2001, banks are required to have in place IDR procedures that meet certain requirements and procedures approved by ASIC (see ASIC's Regulatory Guidance 271[71]), and additionally to be a member of AFCA. Having an IDR mechanism in place allows consumers to make a complaint to a bank (including where the consumer has been subject to a scam). Where a complaint involving a scam is not resolved at the IDR stage or the IDR outcome is unsatisfactory, consumers can escalate their complaints to AFCA.

Telecommunication providers

The telecommunications industry has taken a number of steps in developing codes to reduce the frequency and impact of scam SMS and telephone calls. The networked nature of telecommunications means that scam calls and SMS usually travel across multiple networks owned by multiple telecommunications providers - both compliant and non-compliant - to reach their target. Scammers are able to exploit vulnerabilities in the ecosystem via providers who are not compliant with the rules.

The first *Reducing Scam Calls and Scam SMs* industry code was developed by Communications Alliance, the peak body for the Australian telecommunications industry and registered by the ACMA in December 2020. In 2022, the Communications Alliance led revision of the *Reducing Scam Calls and Scam SMs* industry code, which was registered by the ACMA in July 2022.[72] The revised Code features improved tracing and reporting measures, along with a new section dealing with the identification, tracing and blocking of numbers associated with Scam SMs.

The 2022 *Reducing Scam Calls and Scam SMs* industry code requires telecommunications providers to:

- provide up-to-date guidance for consumers on how to manage and report scam calls and texts;
- monitor, identify, trace and block phone calls and SMS from recognised scammers; and

71 ASIC RG 271: https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-271-internal-dispute-resolution/
72 Register of telco in...~https://www.acma.gov.au/register-telco-industry-codes-and-standards

- report identified scam calls and SMS to the ACMA and any involved telecommunications providers.

Telecommunications providers who are found to be in breach of the code can be issued with a direction to comply by ACMA in the first instance. This is the strongest enforcement outcome currently available to the ACMA for initial breaches of the code. Telcos may face penalties of up to $250,000 for breaching ACMA directions to comply with the code.

In addition to the code, telecommunications providers are subject to other rules introduced by the ACMA to combat scams, including:

- stronger identity verification processes before mobile numbers can be transferred between providers – aimed at stopping scammers from hijacking mobile phone numbers for the purpose of gaining access to other people's personal accounts including bank accounts and social media accounts, and
- authorisation processes for sensitive transactions via the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* to provide a high level of assurance to prevent malicious actors gaining access to a device and the personal information held on it.

The ACMA regularly conducts audits and investigations to test industry compliance with the code. Since 2023, the ACMA has acted against seven telcos that send bulk SMS for failing to comply with multiple anti-scam and public safety rules. In 2023, the ACMA reported that despite the significant inroads made by the new code rules, some telcos were not conducting sufficient checks to ensure customers using text-based sender IDs have a legitimate right to do so. The ACMA noted there are strong indications scammers have used these vulnerabilities to send SMS scam campaigns[73].

Individual telecommunications providers are also continuing to implement new technologies and processes to protect consumers. Several larger telecommunications providers have developed their own internal processes, such as 'trusted source' arrangements to protect phone numbers associated with well-known Australian companies.

The telecommunications sector has a mature external dispute resolution scheme, administered by the TIO. The TIO has jurisdiction to handle complaints about phone and internet services and can handle a complaint about a scam if part of the complaint related to the actions (or inactions) of a telecommunications provider who is a member of TIO. The TIO can also consider a telecommunication service provider's compliance with the *Reducing Scam Calls and Scam SMs* Code. However, there are certain matters the TIO cannot consider (e.g. contents of a scam calls or text, situations where a scammer pretends to be acting for the telecommunication service providers).[74] Certain transit carriers and CSPs may be exempt from the requirement to join TIO as they do not have individual or small business customers.

The TIO can also only take action against a consumer's contracted telecommunications provider. A common scenario is where a consumer receives a scam SMS or phone call that originated from a non-compliant provider and was transmitted to their device via a network operated by a compliant provider. In this scenario, the consumer has no right of action against their own telecommunications provider or the non-compliant originating provider.

In relation to IDR, a carriage service provider that is offering to supply a telecommunications goods or service is required to establish and implement a complaint handling process that meets certain minimum requirements set out in the *Telecommunications (Consumer Complaints Handling) industry Standard 2018.* This provides an avenue for consumers to make complaints to telecommunication service providers about their products and services (including a scam on their service).

73 ACMA, *Action on scams, spam and telemarketing: January to March 2023,* 15 May 2023.
74 TIO's Submission to the Department of Treasury, 1 February 2024.

Digital platforms

In 2022, the ACCC identified the failure of digital platforms to take sufficient steps to prevent online harms as a key consumer harm throughout its digital platform inquiries. The ACCC recommended that digital platforms be required to implement measures to prevent and remove scams, including a notice and action mechanism (for businesses to take timely action on reports). At a minimum, the ACCC recommended these measures be applied to search, social media, online private messaging, app store, online retail marketplace and digital advertising services.[75]

On 8 December 2023, the Government provided in-principle support for the recommendations made by the ACCC in its fifth interim report of the Digital Platform Services Inquiry that aim to address competition and consumer harms on digital platforms.[76] As part of the response, the Assistant Treasurer and Minister of Communications wrote to digital platforms to develop a voluntary IDR code by July 2024. Digital platforms are not currently subject to industry-specific mandatory IDR or EDR requirements in relation to their services in Australia.

DIGI is an industry association representing twelve large digital platforms with a presence in Australia. The digital sector also includes companies in the technology sector, represented by the Tech Council of Australia. DIGI has previously led self-regulated industry codes to address online harms, including development of the Australian Code of Practice on Disinformation and Misinformation in response to the Government's response to the ACCC's 2019 Digital Platforms Inquiry[77].

In February 2024, DIGI expressed interest in developing a voluntary scams code of practice for the digital industry and launched the AOSC on 26 July 2024. The AOSC, signed by 9 DIGI members to date,[78] proposes several voluntary measures for signatories to implement when providing online services. The code applies to the provision of services including social media, peer-to-peer marketplaces, email, messaging, video sharing and paid advertising on digital platforms.

The AOSC sets out guiding principles to inform commitments to undertake specific measures, depending on the applicable services operated by the signatory. These guiding principles include consideration of the diversity of services, proportionality, the protection of user privacy and freedom of expression, and the need for collaboration and co-operation among all relevant stakeholders. Table 16 details the specific commitments set out under the AOSC for signatories (outlined in Table 16)

Table 16 – High-level summary of key priorities under the Australian Online Scams Code

Priority	Services
Blocking	
Deploy measures to detect and block suspected scams, including to ensure scams are addressed as non-compliant activity in community standards, guidelines or terms of service, have or adopt effective internal processes to detect, flag or remove content suspected to be a scam, block or terminate users for creating new accounts when the original accounts were removed for scams, offer appropriate login authentication methods and encourage the adoption of strong security measures such as two-step verification.	Social media services, peer-to-peer marketplaces and video sharing services

75 Australian Competition and Consumer Commission, Digital Platform Services Inquiry, *Interim report No. 5 – Regulatory reform,* September 2022
76 The Hon Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, *Government's response to the ACCC's major competition and consumer recommendations for digital platforms,* 8 December 2023
77 Treasury, *Regulating in the digital age: Government response and implementation roadmap for the Digital Platforms Inquiry,* 12 December 2019.
78 Signatories include Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo.

Provide guidance to users on how to stay safe when buying and selling items from other users, and commit or move towards introducing reasonable and targeted measures for the verification of users using peer to peer marketplaces.	Peer-to-peer marketplaces
Reporting	
Have a simple and quick route to report possible scams, including having or adopting simple in-product mechanisms for users to report suspected scam content, action those reports as swiftly as possible if suspicious, have or adopt a simple and direct process for law enforcement and agencies to report suspected scam activity, and indicate to users that they may report scams to law enforcement and their bank.	Social media services, peer-to-peer marketplaces and video sharing services
Provide or develop appropriate protections, which may include displaying warnings or allowing users to control or block messages.	Social media services
Takedowns	
Take quick action against verified scam content and scammers, including to expeditiously remove scam content once found by the signatory that violates applicable terms or service or policies, take appropriate enforcement action against users that post, send or share scam content, once found to be in violation, and have a clear process for users to request reinstatement of access following account takeover or scam.	Social media services, peer-to-peer marketplaces and video sharing services
Advertising	
Deploy measures to protect people from scam advertising, including to offer or develop verification or authentication measures for new advertisers, commit or move towards introducing measures to confirm advertisers hold necessary financial services, have or introduce measures to screen advertisements, deploy processes to combat URL cloaking, and commit to or move towards a simple scam reporting mechanism.	Paid advertising services
Email and messaging	
Deploy specific measures to protect people from scams in email and messaging, requiring service providers to make guidance available to users on scams, clarifying standards, guidelines and terms of service to ensure initiating scams is a breach of them, and have systems or processes in place to monitor for and identify scams, take appropriate action and identify trending or changing behaviour associated with scams.	Email and messaging services
Law enforcement	
Engage with law enforcement efforts to address scams, including responding to valid Australian law enforcement requests for user information or to provide information on persistent and prolific serious and organised crime as soon as practicable, and considering other ways to support crime prevention such as the provision of training, law enforcement reporting channels or public-private partnership initiatives.	All entities

Intelligence sharing	
Contribute to public-private and cross sectoral initiatives to address scams, including working with the NASC, regulators and industry partners to contribute to the work of the NASC, explore data and share best practice, as well as responding to valid regulator information requests.	All entities
Communications	
Provide information about scam risks and support counter-scam efforts., including committing to the NASC and ACCC to share information and learnings, support regulator and consumer organisation communications campaigns, and continue engaging users with messaging on risks, such as through in-product messages, help pages or links to third-party resources.	All entities
Strategy and future proofing	
Contribute to strategy development and future proofing exercises to stay ahead of the threat, including developing an internal anti-scam strategy, analyse established and emerging scam types on relevant services, undertake internal co-ordination to assess risks of future technologies on those services, share findings with the NASC and appropriate entities.	All entities.

Appendix 2 – Regulatory cost calculations

Under options 2 regulated entities would need to implement new systems or improve existing systems to adhere to mandatory industry codes. These changes would impose implementation and ongoing costs on businesses in adhering to obligations and respond to changed levels of liability related to scams.

For the purposes of this IA, the types of activities undertaken by entities incurring regulatory costs due to implementation of option 2 are grouped into three categories:

1. Anti-scam activities - Activities needed would include scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem. This includes complaints handling and IDR obligations, and would also include governance operations to comply with new regulations.
2. Information sharing and reporting – Sharing, receiving and acting on information, to ensure that entities within the scams ecosystem have information to enable detection and prevention of scams.
3. External dispute resolution – Engagement in schemes to provide pathways for redress to consumers.

Increased regulatory costs from these activities are assumed to be either incurred for administrative improvements or technology, as outlined in Table 17.

Table 17 – Regulatory cost implications for relevant entities

Potential business costs in compliance with options 2	
Administrative improvements	Entities would need to make changes in administrative procedures to give effect to new mandatory obligations and improve anti-scam activity in response to changed incentives. This may include detecting patterns of potential scam activity, responding to reports or complaints from consumers and establishing procedures for sharing information and engaging with regulators and other businesses to respond to scams. Training may need to be provided to operational and executive staff in terms of their compliance and reporting responsibilities. New policies, procedures and risk analysis may need to be completed to give effect to new anti-scam activities. Businesses may be required to resource greater operational staffing or engage third party service providers to perform anti-scam activities, including for internal and customer-facing roles.
Technology	New or improved technology builds may be required to implement measures to facilitate detection, analysis and disruption activities, or set up infrastructure for data and information sharing.

Compliance costs would vary depending on several factors, including the maturity of voluntary protections being taken in a sector or individual business. The size and complexity of a business, its services, customer base, nature of the scam-related risks, and current and potential staffing and anti-scam infrastructure would also each shape expected costs. Across each activity, the assessment of regulatory costs for this IA has been based on benchmarks applied to the number of entities classified into categories across these factors.

Costs assumptions

Anti-scam activity

Uplifts in anti-scam strategy have been estimated based on benchmark assumptions for entities at different stages of capacity, assumed to be linked to their current participation in anti-scam initiatives such as industry codes, information sharing systems and EDR schemes. Entities whose existing or planned policies and procedures are better aligned with optimal practice are expected to incur lower additional costs compared to those that are not.

In constructing these assumptions, we have considered that regulated entities have already invested resources into similar or consistent consumer protection activities. These entities are likely to make further investments under the status quo. Uplifts would involve enhancements and managing higher volumes of activity for existing system and processes.

Table 18 outlines the benchmark regulatory cost assumptions for a medium sized entity. These estimates are based on assumptions of the required staff resources required to achieve a type of uplift, in terms of full-time equivalent (FTE) or weeks work required from staff.

Table 18 – Benchmark assumptions for required anti-scam activity uplift – for a medium sized entity

Uplift needed	Types of entities	Technology ($m)		Administration ($m)		Estimation assumptions
		Initial	Ongoing	Initial	Ongoing	
Minor anti-scam activity improvements	ABA/COBA member banks	0.22	0.00	0.02	0.00	Technology: 1.0 FTE technology staff in initial year, none ongoing Administration: 0.1 FTE admin staff in initial year, none ongoing
Moderate anti-scam activity improvements	AOSC signatory digital platforms	0.45	0.04	0.21	0.10	Technology: 2.0 FTE technology staff in initial year, 0.2 FTE ongoing Administration: 1.0 FTE admin staff, then 0.5 FTE ongoing staff.
Material anti-scam activity improvements	Non-affiliated banks, non-AOSC digital platforms	0.67	0.22	0.42	0.21	Technology: 3.0 FTE technology staff in initial year, 1.0 FTE ongoing Administration: 2.0 FTE staff, 1.0 FTE ongoing staff
SPF Governance operations	All regulated entities	0.00	0.00	0.02	0.01	Administration: 0.1 FTE admin staff in initial year, 0.05 FTE ongoing
Initiating IDR processes	Digital platforms	0.00	0.00	0.83	0.42	Administration: 4.0 FTE admin staff, 2.0 FTE ongoing

Full-time equivalent is assumed as 37.5 hours per week and 52 weeks per year, with labour costs at the rates per hour outlined in Table 19. Different labour cost rates are assumed for technology staff and administrative staff. These are calculated as per OIA guidelines with a 1.75 multiplier[79] applied to Australian Bureau of Statistics average earnings figures.[80]

Table 19 – Hourly labour cost assumptions

	Rate/hr	ABS category
Administrative staff	$106.75	224 Information and organisation professionals
Technology staff	$115.33	261 Business and systems analysts, and programmers

Large entities are assumed to require 5 times the resources of medium entities, and small entities are assumed to require half the resources of medium entities.

79 OIA - regulatory burden framework, page 13
80 ABS Employee Earnings and Hours, Australia, Data cube 13, May 2023. Full-time non-managerial employees paid at the adult rate.

These uplift cost assumptions can be interpreted in comparison to past industry activity, such as domestic banking sector members of ABA and COBA that have previously invested in a confirmation of payee system with total sectoral costs estimated at $100 million, around $1.3 million per bank.[81] This is comparable to the assumed regulatory costs incurred by a medium sized entity to initiate anti-scam activities over 2 years.

Information sharing and reporting

Regulatory costs of information sharing arrangements under option 2 are challenging to estimate due to uncertainty of the required systems for entities to communicate with the government regulator and other factors such as the frequency of communication and the information required.

However, expected entity investments for compliance with information sharing obligations under the consumer data right (CDR) are a comparable basis for estimated regulatory costs. Although, the SPF information sharing arrangements would be less complex and lower in volume and frequency than required under CDR.

Regulatory costs of CDR by type of entities regulated were conducted in 2021 for coverage of the telecommunications sector[82] and in 2022 for the non-bank lending sector.[83] Table 20 outlines the estimated annual regulatory costs in the first year and ongoing, by type of entity from these previous reports, which have been inflated to current dollar values to use as benchmarks for regulatory costs under option 2.[84]

Table 20 – Estimated annual CDR compliance costs by types of entity (in 2024 dollars)[85]

Type of entity	Year 1	Ongoing	Source
Small telco	$394,000	$186,000	CDR telecommunications sectoral assessment (Treasury 2021)
Large telco	$4,986,000	$1,484,000	
Medium non-bank lender	$826,000	$330,000	CDR non-bank lending sectoral assessment (Treasury 2022)
Large non-bank lender	$3,302,000	$1,101,000	

As information sharing for option 2 under the SPF would be less resource intensive than the CDR, it is assumed a regulated entity would incur 20 per cent of the CDR benchmark costs if needing to develop information sharing capabilities with the government regulator without similar prior or intended activities. Given many entities are already undertaking information sharing without the SPF, such entities would only be assumed to need to incur around 5 per cent of the CDR cost benchmark.

External dispute resolution costs

Costs to regulated entities for engaging in EDR programs are estimated based on the fee structures and experiences of entities engaged with AFCA's EDR process.[86]

AFCA is a not-for-profit body and recovers its cost from members. It relies on three funding streams to support its business operations:

- annual membership fees,
- fees collected from members subject to a complaint (complaint fees), and

81 Australian Banking Association, *Banks unite to declare war on scammers*, 24 November 2023.
82 Treasury (2022) Consumer Data Right – Telecommunications Sectoral Assessment, available on the OIA website: https://oia.pmc.gov.au/published-impact-analyses-and-reports/consumer-data-right-telecommunications-sectoral-assessment
83 Treasury (2022) CDR – Non-bank lending sectoral assessment, available on the OIA website: https://oia.pmc.gov.au/published-impact-analyses-and-reports/cdr-non-bank-lending-sectoral-assessment
84 Using Consumer Price Index values for Australia from the Australian Bureau of Statistics, from September 2021 to June 2024 for telecommunications estimates and from June 2022 to June 2024 for non-bank lender estimates.
85 Rounded to the nearest $1,000.
86 AFCA Complaint Fee Guide.

- a proportionate charge to members who have had six or more complaints brought against them during the period (user charge).

AFCA's annual membership fee for financial firms is expected to be around ~$389 in FY2024-25. Complaint fees and an proportionate user charges are calculated based on prior year's AFCA dispute handling data.

AFCA's fee schedule incentivises early resolution of disputes by regulated entities. EDR costs will be minimised if they meet their mandatory obligations, resolve complaints directly with their customers at the IDR stage or resolve complaints early where they are escalated to EDR. AFCA does not charge for the first five complaints in a financial year against a member. After that, AFCA's complaint fees depend on where in the process that the relevant complaint gets resolved. Fees are smaller at the earlier stages and increase if the complaint requires a decision. The fee schedule encourages earlier resolution of complaints and for firms to improve their IDR process, which decreases the need for the complaints to come to AFCA.

The user charge is a proportionate annual charge which is calculated at the start of the financial year and is based on AFCA's prior year dispute handing data. More frequent users of AFCA's service pay higher user charges.

In 2023-24, AFCA received 10,928 scam complaints, with 67% of the complaints closed at the 'registration and referral' stage.[87] Under the 2024-25 fee schedule, AFCA has a complaint fee of $96 for cases at the 'registration and referral' stage.[88]

As a conservative estimate of regulatory costs for the purposes of this IA it is assumed that entities which are not currently a part of an EDR scheme would incur approximately costs of $924 per complaint (inclusive of GST). This is based on AFCA 2023-24 data on distribution of the stage AFCA scam complaints are closed and the approximate 2024-25 fee associated with complaints at that stage.

The annual AFCA fees for scam complaints per entity is estimated by apportioning the approximately 11,000 complaints received each year across types of banks and other ADIs according to the market share of total residential deposits.[89] These estimates are outlined in Table 21 (covers major banks, non-major ABA member banks and other ADIs) and are used as benchmarks for EDR costs for regulated entities in the banking sector, as well as telecommunications and digital platforms.

Table 21 – Estimated annual EDR costs for scam complaints by type of entity[90]

Type of entity	Number	Market share	Assumed scam complaints per entity	AFCA fees for scam complaints per entity
Major banks	4	73.6%	2,025	$1,818,000
Non-major ABA member banks[91]	16	17.5%	121	$109,000
Other ADIs - AFCA members	115	8.8%	8	$8,000

For telecommunications providers which are currently members of the TIO, enrolment in a single EDR scheme under the SPF would involve an uplift in fees given they would need to be members of two

87 AFCA Annual Review 2022-23, Scam complaints, https://www.afca.org.au/annual-review-scams
88 AFCA Fee Structure FY25, https://www.afca.org.au/members/funding-model/fee-structure
89 APRA, Monthly Authorised Deposit Taking Institution Statistics, Key Statistics, July 2024. Although some complaints may not be related to ADIs, the market share of scam complaints have been calculated based on the assumption all complaints are made to ADI members in the proportion equivalent to their market share of total residential deposits. This benchmark may be conservatively higher than AFCA fees actually incurred.
90 Rounded to the nearest $1,000.
91 Identified based on Australian Banking Association website list of 20 members, as at September 2024, https://www.ausbanking.org.au/about-us/aba-members/

EDR schemes. TIO would continue to operate its existing EDR jurisdiction in relation to non-scam complaints about telecommunications service providers. However, as there is no publicly available data on TIO fees for complaints involving scams it is not possible to estimate current levels of TIO fees which are expended by TIO members on scam complaints.[92] For the purposes of this analysis, it is assumed the increase in EDR fees from the Framework would be 50 per cent of the estimated fees of similar scale entities in the financial sector.

Under option 2, demand for EDR would be higher as consumers seek to take action to exercise their rights to protection under the Framework or mandatory reimbursement. This is assumed to be a 10 per cent uplift from the current volume of scam complaints made against AFCA members (with the uplifted cost assumption carried across to telecommunications and digital platform sector entities).

It is assumed other internal costs and resources required to undertake EDR obligations in addition to AFCA fees are incorporated costs of overall anti-scam activity. Costs incurred by regulated entities in paying redress to scam victims are not accounted for as a cost of either option 2, as these payments represent a transfer from the entity to the consumer with no overall net cost or benefit.

Assumptions on number of regulated entities

Banking

Full membership of the AFCX is not publicly disclosed, however participants include the four founding major banks, Macquarie and Bendigo Bank, and COBA. In May 2023, the ABA reported that 14 of its 20 members were, or were in the process of, entering membership with the Fraud Reporting Exchange.

Table 22Table 22 outlines the estimated number of ADIs which are currently a part of voluntary industry codes, information sharing arrangements and EDR schemes. Almost all domestic ADIs are a member of an external dispute resolution scheme. According to APRA's register of ADIs and AFCA's member register, only 1 of the 80 Australian-owned authorised ADIs are not AFCA members.[93] This extends to 19 of the 49 Australian branches of foreign-owned banks on the APRA register.

Table 22 – Number of assumed regulated banking entities by current activity category

Category	Number of entities	Voluntary code membership	Information sharing	EDR membership
Major banks	**4**	ABA Scam-Safe Accord	AFCX members	AFCA members
ABA/COBA members	**72**		Soon to all be AFCX members	
Non-affiliated[94]/ AFCA members	**40**	No applicable code	No information sharing arrangements	
Non-affiliated/ non-AFCA	**16**			No EDR scheme

Telecommunications providers

For regulatory cost calculation purposes the SPF would be assumed to apply to carriers and carriage service providers as those terms are defined in s 7 of the *Telecommunications Act 1997* (Telco Act). Carriers require a license under the Act and are published under an ACMA register. Currently, there

92 According to the 2023 TIO Financial Report "funding requirement is allocated to members based on the percentage of the number of complaints (referrals) the member had in the previous calendar year compared to the total complaints (referrals) received in that year." However, data on the number of complaints by member is not available.
93 Identified through https://my.afca.org.au/ff-search/, September 2024
94 Not a member of the ABA or COBA.

are 342 ACMA licensed carriers.[95] Carriage service providers represent a far wider market, with ACMA estimating there are around 1,500 'eligible CSPs' under the *Telecommunications (Consumer Protection and Service Standards) Act* (TCPSS Act).[96]

The TCPSS Act requires eligible CSPs to be members of, and comply with, the TIO Scheme. Under s 128 of the TCPSS Act, each *carrier* and each *eligible carriage service* provider must join the TIO Scheme.

- A "carrier" is a holder of a carrier licence granted under s 56 of the Telco Act.
- Under s 127, an "eligible carrier service provider" is a carriage service provider who supplies or arranges the supply of:
    - A standard telephone service to residential or small business customers
    - Public mobile telecommunication service
    - Access to the internet

Under option 2 a potentially broader group of entities would be required to join an EDR scheme than are currently required to join the TIO. Transit carriers and CSPs may be exempt from the requirement to join the TIO scheme as they do not have individual or small business customers,[97] but would be required to join the AFCA scheme under the SPF. As at the end of 2022-23 there were 1,686 TIO members,[98] and 32 transit carriers and CSPs with TIO membership exemptions.

ACMA published a regulation impact statement, *Reducing the impact of scam calls*, that estimated 413 carriers/CSPs provide public numbers to ACMA for mobile and local services in 2020.[99] The report noted that multiple carrier and/or CSP licences can be held by a single telecommunications provider entity. The IA provides the following estimates of the number of telco entities impacted by the scam calls code holding relevant licences as follows:

- large carriers: 4 (over 10 million numbers)
- medium CSPs: 18 (1 million to 10 million numbers)
- small CSPs: 150 (100,000 to 1 million numbers)
- very small CSPs: 241 (1 to 100,000 numbers)

These figures are used as the basis for the number of entities which would be regulated entities under option 2's SPF, with the addition of 32 transit carriers/CSPs. Table 23 outlines the number of entities in each category.

Table 23 – Number of assumed regulated telecommunications entities by current activity category

Category	Number of entities	Mandatory code obligations	Information sharing	EDR membership
Major telcos	4 (Telstra, Optus, TPG)	*Reducing Scam Calls and Scam SMs* code	*Reducing Scam Calls and Scam SMs* code & AFCX members	TIO members
Medium CSPs	18		*Reducing Scam Calls and Scam SMs* code	
Small CSPs	150			
Very small CSPs	241			

95 ACMA, *Register of licensed carriers* (5 September 2024)
96 DITRDCA, *Registration or licensing scheme for carriage service providers: Discussion Paper* (September 2023)
97 Under s 129 of the TCPSS Act, ACMA may grant an exemption from the requirement to join the TIO Scheme. Before granting such an exemption, ACMA must have regard to the following matters (note, it can also have regard to other things): the extent to which the carrier or provider deals with residential customers or small businesses; the potential for complaints under the TIO about the services supplies by the carrier or provider; and, whether the carrier or provider is a statutory infrastructure provider (within the meaning of Part 19 of Telco Act).
98 TIO Financial Report 2023
99 ACMA, *Reducing the impact of scam calls: Regulation Impact Statement* (December 2020); *Reducing the impact of scams delivered by short message service (SMS): Regulation Impact Statement* (June 2022)

Category	Number of entities	Mandatory code obligations	Information sharing	EDR membership
Transit carriers/CSPs	32			TIO exempt

Digital platforms

The number of digital platform entities which would be regulated entities under option 2 has been estimated based on previous ACCC inquiries into the relevant services.

As the SPF would be intended to address where scams harms are most prevalent, the social media services that could be captured would include Facebook, YouTube, Instagram, Snap, TikTok, Pinterest, Reddit, LinkedIn, BeReal and X. This is based on the ACCC's 6th interim report of the Digital Platform Services Inquiry[100], which identified services of Meta (Facebook, Instagram), Google (YouTube), ByteDance (TikTok), Snap (Snapchat) and Pinterest having over 5 million monthly active users in 2022.

In the ACCC's 5th interim report of the Digital Platform Services Inquiry "online private messaging services" are defined as "services that enable users to communicate privately and in real-time with friends, family members, colleagues and other contacts, one-to-one and/or with a group using text, voice or video."[101] Based on Nielsen Digital Content Ratings the report identifies usage data for 17 direct messaging services, in addition to 3 services not captured by this ratings data.[102] The report identified Meta (Facebook Messenger, WhatsApp) and Apple (iMessage, FaceTime) as the 2 largest supplies of online messaging services, Snap (Snapchat) had over 4 million monthly active users, and Zoom, Microsoft (Skype) and Discord had services with around or over 2 million monthly active users.

In terms of search advertising service providers, Google (through its Google search service) and Microsoft (though its Bing search service) would initially be captured. This is based on the ACCC's 2021 Digital Advertising Services Inquiry[103] and more recently, the ACCC's 9th interim report of the Digital Platform Services Inquiry issues paper on revisiting general search services[104] which reported that these entities provide almost all search engine services used in Australia. The recent issues paper reported that Google Search had an 86 per cent market share in desktop search and 98 per cent market share in mobile search, and Microsoft Bing had a 12 per cent market share in desktop search.[105]

Table 24 outlines the number of entities in each category assumed for this IA. Digital platform entities are grouped by the scale of their entity (major or medium) and whether they are a signatory to the AOSC in order to estimate the relative level of regulatory cost required to be incurred under the obligations in option 2. Major platforms operate either a social media platform or direct messaging service with over 4 million active monthly users (in 2022), or a search advertising service with a greater than 10 per cent market share on either desktop or mobile (in 2024).

100 ACCC (2023) Digital Platform Services Inquiry, *Report on social media services,* March 2023. Page 31
101 ACCC (2022) Digital Platform Services Inquiry, Interim report No. 5 – Regulatory reform, September 2022. Page 23
102 Ibid. Page 202
103 ACCC (2021) Digital advertising services inquiry - final report, 28 September 2024
104 ACCC (2024) Digital Platform Services Inquiry – September 2024 report revisiting general search services, Issues Paper, 18 March 2024
105 Ibid. pages 6-7

Table 24 – Number of assumed regulated digital platform entities by current activity category

Category	Number of entities	Voluntary code membership	Information sharing	EDR membership
Major platforms – AOSC	**5** (Meta, Google, ByteDance, Snap, Apple)	Australian Online Scams Code (AOSC)	Engagement in NASC information sharing	No memberships of EDR schemes
Medium platforms – AOSC	**2** (X, Discord)			
Major Platforms – non-AOSC	**2** (Microsoft, Pinterest)	None	No current arrangements	
Medium platforms - non-AOSC	**12** (Reddit, BeReal, Zoom)			

Option 2: Regulatory cost assumption tables

Table 25 – Option 2 - Banking sector annual regulatory cost assumptions by entity type (medium sized entity)

		Description of impacts		Technology ($m)		Administration ($m)	
Obligation	**Entity type**	**Current actions**	**Uplift required**	**Initial**	**Ongoing**	**Initial**	**Ongoing**
Anti-scam activity	Major banks	Scam- Safe Accord standards	Minor anti-scam activity improvements, Governance operations	1.12	0.00	0.21	0.05
	Other ABA/COBA	Scam-Safe Accord standards	Minor anti-scam activity improvements, Governance operations	0.22	0.00	0.04	0.01
	Non-affiliated/AFCA	No identifiable consistent standards	Material anti-scam activity improvements, Governance operations	0.67	0.22	0.44	0.22
	Non-affiliated/non-AFCA	No identifiable consistent standards	Material anti-scam activity improvements, Governance operations	0.67	0.22	0.44	0.22
Info sharing & reporting	Major banks	AFCX intel loop participation	Minor investment in info sharing	0.04	0.02		
	Other ABA/COBA	AFCX intel loop participation	Minor investment in info sharing	0.04	0.02		
	Non-affiliated/AFCA	None	Likely significant investment	0.17	0.06		
	Non-affiliated/non-AFCA	None	Likely significant investment	0.17	0.06		
EDR	Major banks	AFCA members	10% increase in complaints			0.18	0.18
	Other ABA/COBA	AFCA members	10% increase in complaints			0.01	0.01
	Non-affiliated/AFCA	AFCA members	10% increase in complaints			0.00	0.00
	Non-affiliated/non-AFCA	None	EDR for complaints with AFCA			0.01	0.01

Table 26 – Option 2 - Telecommunications sector annual regulatory cost assumptions by entity type (medium sized entity)

		Description of impacts		Technology ($m)		Administration ($m)	
Obligation	**Entity type**	**Current actions**	**Uplift required**	**Initial**	**Ongoing**	**Initial**	**Ongoing**
Anti-scam activity	Major telcos	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.10	0.05
	Medium CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.02	0.01
	Small CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.01	0.01
	Very small CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.01	0.01
	Transit carriers/CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.01	0.011
Info sharing & reporting	Major telcos	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.25	0.07		
	Medium CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
	Small CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
	Very small CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
	Transit carriers/CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
EDR	Major telcos	TIO members	AFCA fee level, 10% increase in complaints			1.00	1.00
	Medium CSPs	TIO members	AFCA fee level, 10% increase in complaints			0.06	0.06
	Small CSPs	TIO members	AFCA fee level, 10% increase in complaints			0.00	0.00
	Very small CSPs	TIO members	AFCA fee level, 10% increase in complaints			0.00	0.00
	Transit carriers/CSPs	No current EDR scheme	EDR for complaints with AFCA			0.01	0.01

Table 27 – Option 2 - Digital platforms sector regulatory cost assumptions by entity type (medium sized entity)

		Description of impacts		Technology ($m)		Administration ($m)	
Obligation	**Entity type**	**Current actions**	**Uplift required**	**Initial**	**Ongoing**	**Initial**	**Ongoing**
Anti-scam activity	Major platforms - AOSC	Aus Online Scams Code	Moderate anti-scam activity improvements, Governance operations, IDR processes	2.25	0.22	5.31	2.65
	Major platforms - non-AOSC	None	Material anti-scam activity improvements, Governance operations, IDR processes	3.37	1.12	6.35	3.17
	Medium platforms - AOSC	Aus Online Scams Code	Moderate anti-scam activity improvements, Governance operations, IDR processes	0.45	0.04	1.06	0.53
	Medium platforms - non-AOSC	None	Material anti-scam activity improvements, Governance operations, IDR processes	0.67	0.22	1.27	0.63
Info sharing & reporting	Major platforms - AOSC	No current arrangements	Likely significant investment	1.00	0.30		
	Major platforms - non-AOSC	No current arrangements	Likely significant investment	1.00	0.30		
	Medium platforms - AOSC	No current arrangements	Likely significant investment	1.00	0.30		
	Medium platforms - non-AOSC	No current arrangements	Likely significant investment	1.00	0.30		
EDR	Major platforms - AOSC	None	AFCA membership			0.18	0.18
	Major platforms - non-AOSC	None	AFCA membership			0.18	0.18
	Medium platforms - AOSC	None	AFCA membership			0.01	0.01
	Medium platforms - non-AOSC	None	AFCA membership			0.01	0.01

Appendix 3 – Outcomes and evaluation matrix

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
Reduced demographic rates of exposure and victimisation of consumers to scams	Quantitative	ABS, *Personal Fraud* AIC, *Cybercrime in Australia* Treasury, *Australian Consumer Survey*	Consumer surveys in Australia have found that scam exposure is widespread. Estimates of exposure to scam attempts sit around 65% of the population, with victimisation between 2% to 3%.	Greater business anti-scam measures, particularly prevention and disruption measures, will contribute to lower rates of exposure and victimisation to scams. Increasing avenues for consumer redress may lead to a decline in average losses as the impacts of scams become less ruinous for the consumer.	Due to the nature and increasing prevalence of scam activity, it is impossible to eradicate overall exposure to scams. Figures relating to victimisation are more accurate assessments of the degree to which scam attempts 'break through' and impact Australians. Improvements should be analysed in context to short-term trends whilst accounting for the fact that scam activity can fluctuate, which the ACCC is well equipped to identify and account for.
Reduced consumer losses to scams reported to regulators		ACCC, *Targeting Scams*, *Scamwatch Dashboard* Treasury, *Australian Consumer Survey*	Consumers and businesses reported $3.1 billion in losses to scams in 2022, an increase of 80% from 2021. On average, a victim to a scam loses $20,000. There is evidence of recent Government and industry efforts leading to this figure to peak, but losses remain much higher than pre-pandemic levels.		Changes in average losses should be considered with caution as they may reflect changing patterns to overarching scam methods, such as low-yield shopping scams or high-yield investment scams, rather than a reduced overall prevalence of scams. The ACCC records other figures, including recording median losses, and disaggregates reports and losses by scam type, which can corroborate evidence of improvements.
Improved reporting and information sharing on scam cases affecting consumers	Quantitative and qualitative	ACCC, *Targeting Scams*, *Scamwatch Dashboard* ATO, *Scam Data*	Consumer reports to regulators remain high. In 2023, Australians made over 300,000 reports to Scamwatch, an increase of 26% from 2022. Reporting and information sharing arrangements to regulators under the NASC are currently voluntary or limited due to the scope of privacy or tipping-off provisions.	Increased access to complaints handling and reporting measures may increase the level of consumer reports being made to regulators from consumers. More reports can be leveraged by information-sharing infrastructure of the SPF and NASC.	Increases or decreases in reporting do not necessarily reflect a desirable outcome. Although fewer consumer reports may reflect less scam activity, increased reporting may reflect improved accessibility to and quality of reporting measures.

Increased rate of detection and disruption activities undertaken by the private sector	Quantitative and qualitative	ACCC, *Quarterly Report* ACMA, *Action on Scams, Spam and Telemarketing*	Outside of existing regulatory regimes including ACMA codes, there is little centralised evidence for sector-wide activities to address scams.	Potential monitoring of business action by regulators and subsequent reporting under the SPF will provide Government with clearer evidence on the extent of industry action on scams and in turn opportunities to identify regulatory gaps, effective actions, and ongoing trends.	Scam threats wax and wane over time. Quantitative information on industry action must be interpreted in the context of these trends; for instance, increases or decreases in blocked calls or numbers or account closures.
Increased assessment of quality in business anti-scam policies and procedures	Qualitative	ACCC, *Digital Platform Services Inquiry* ASIC, *Scam Prevention, Detection and Response*	Regulators have identified significant levels of variation in the quality of business anti-scam practices and procedures. Whilst some voluntary industry efforts such as the Scam-Safe Accord are in place, there will remain gaps in the voluntary framework for outsider participants.	Uplift of quality of anti-scam policies and procedures in the business sector, which will in term limit regulatory gaps and contribute to other improved outcomes.	This measure depends on future regulatory review and reporting mechanisms which remain unconfirmed.
Increased levels of consumer satisfaction with business policies and procedures relating to scams	Qualitative	Treasury, *Scams Consumer Survey*	Consumer advocacy bodies have expressed dissatisfaction with current business policies and procedures relating to scams. The widespread impact of scams is anecdotally leading consumers to be more risk-averse and distrustful of everyday business functions, including communications, notifications and transactions relied on by businesses.	Improved consumer protections will increase consumer satisfaction and trust in their communications and transactions with industry entities.	This metric is difficult to measure. Consumer satisfaction with business anti-scam policies and procedures are oriented towards positive resolution and redress of consumer disputes. An improvement in consumer satisfaction may not reflect the state of the overarching ecosystem and business impacts.
Consumer trust in the payments and communications system		Treasury, *Scams Consumer Survey*	The widespread impact of scams is anecdotally leading consumers to be more risk-averse and distrustful of everyday business functions, including communications, notifications and transactions relied on by businesses.	Improved consumer protections will increase consumer trust in their communications and transactions with the business sector.	This metric is difficult to measure. Some business sector participants believe increased consumer trust is a moral hazard in which risks are offset to be borne by the business sector.

Decreased levels of consumer complaints to external dispute resolution systems	Quantitative and qualitative	AFCA, *Annual Review*	AFCA has noted increased pressure of consumer scam-related complaints on the financial dispute resolution system, affecting the efficiency of complaints resolution. In 2022-23, AFCA received over 6,000 scam-related complaints, an increase of 46% from 2021-22.	Prevention of scams and improved business complaints handling processes will contribute to a decreased level of consumer complaints and greater level of internal resolution, leading to a decrease in external dispute resolution complaints over time.	Increased or decreased reporting may not indicate positive outcomes or broader trends in the scams ecosystem, as addressed in other sections in this column.
Increased consumer access to reporting outlets and support networks	Quantitative and qualitative	AIC, *Cybercrime in Australia* Treasury, *Scams Consumer Survey*	Despite there being several reporting avenues for support when a person is affected by a scam, there is low take-up of these services. The AIC estimates most Australians do not disclose their victimisation to scams or fraud with agencies, with low take-up of services such as ACSC and IDCARE and reporting outlets such as Scamwatch.	Improved complaints handling and reporting processes may improve the connection of victims to support services and increase the overall take-up of these services.	The evidence base for consumer take-up is survey-based and limited. There are personal and situational elements that influence consumers' beliefs relating to supports that may not be improved, particularly a reluctance to escalate supports if it is known that funds lost to a scam are unrecoverable from a financial institution. Also, not all victims of a scam report a loss, limiting their desire to escalate.