Australian Mobile Telecommunications Association Submission on the exposure draft legislation for the Scams Prevention Framework

4 October 2024

Scams Taskforce
Market Conduct Division
Treasury
Langton Cres
Parkes ACT 2600

Via email: scamspolicy@treasury.gov.au

4 October 2024

Dear Treasury Officials,

The Australian Mobile Telecommunications Association (AMTA) welcomes the opportunity to provide this submission in response to the exposure draft legislation for the Scams Prevention Framework.

AMTA is the peak industry body of Australia's mobile telecommunications industry. Our purpose is to be the trusted voice of industry, promoting the adoption, monetisation and sustainability of mobile telecommunications technology for the benefit of all Australians. AMTA members include the mobile network service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry.

The mobile telecommunications industry is strongly supportive of government attempts to combat scams. That is why our industry has had a registered and enforceable industry code aimed at reducing scam since 2020. In 2022 it was expanded to include obligations for short message services (SMS). As a result of this code, **the telecommunications industry had blocked more than 2.1 billion scam calls and 668 million scam SMS** by the middle of 2024[1].

While our work continues to combat scams, it is essential we acknowledge that no single solution will completely eliminate the threat. While the telecommunications sector and other industries have made significant strides in developing systems to detect and block scams and protect customers, scammers continuously evolve their tactics, and despite the best efforts of industries to stay ahead, some scams will inevitably slip through. This reality must be understood and accepted by policymakers and stakeholders, as it underscores the importance of ongoing collaboration and flexibility in our approach to combating scams.

The focus should be on creating a framework that recognises the efforts already made by industries, such as telecommunications, while encouraging further innovation and investment. However, it is crucial that any policy and legislative initiatives can adapt to the complexity of scams. We should prioritise measures that minimise risk, enhance consumer protection, and swiftly address incidents when they occur to ensure Australian consumers are an unattractive target for scammers.

A balanced approach - where industry initiatives are supported with flexibility to adapt over time to new scam approaches - will result in more sustainable, long-term success in the fight against scams.

If you have any queries or comments in relation to the content of our submission, please contact Louise Hyland on 0488 171 066 or by email louise.hyland@amta.org.au

[1] https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024

The facts about scams in Australia

- Australians lost $2.74 billion to scams in 2023[2] and scams have increased 320 per cent since 2020[3].
- ASIC found that the big four banks (ANZ, CBA, NAB and Westpac) only stopped 13 per cent of attempted scam payments before they took place. Once scammed, only 2 to 5 per cent of losses were reimbursed or compensated[4].
- In another report on 15 smaller banks, ASIC found that in 96% of cases where a scam occurred, the customer suffered the loss[5].
- The telecommunications industry had blocked more than 2.1 billion scam calls and 668 million scam SMS by the middle of 2024[6].

Overview

The mobile telecommunications industry is strongly supportive of government initiatives aimed at combating scams. We recognise that scams represent a significant and growing threat to both consumers and businesses across various sectors.

This industry has a long-standing commitment to working alongside the government and regulators to safeguard Australians from these criminal activities. In recent years, the mobile telecommunications sector has undertaken a range of proactive measures to disrupt scam operations, provide consumer education, and enhance technological defences. These efforts include the development of spam filters, real-time monitoring of fraudulent activity, and collaboration with law enforcement agencies to ensure that telecommunications networks are not exploited by scammers.

The mobile telecommunications sector has made significant efforts to prevent and disrupt scam activity and protect its customers' accounts from fraudulent takeover. We appreciate more can be done across the economy to prevent scams. The reluctance of other sectors to adopt proven anti-scam technologies and protocols has resulted in a less cohesive response to financial scams, placing additional pressure on telcos to compensate for deficiencies in other sectors.

The proposed Scams Prevention Framework is an important step in enhancing the protection of consumers across multiple sectors. However, we believe that in its current form, the framework's broad, principle-based obligations, while aimed at addressing deficiencies in the banking sector and digital platforms, risk creating unnecessary complexity and duplication for industries such as telecommunications, where a robust and enforceable Industry Code is already in place. While we acknowledge that ongoing innovation and adaptability are essential to staying ahead of scammers, it is crucial that the framework is appropriately flexible and tailored to recognise the differing roles and regulatory landscapes of various industries involved.

We encourage the government to take the time to get this legislation right. By refining the proposed Scams Prevention Framework, we believe that Treasury can create a more effective, streamlined approach to combatting scams that leverages the strengths of each sector and avoids unnecessary duplication of efforts. We look forward to further consultation and collaboration with all relevant stakeholders to achieve this outcome.

[2] https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

[3] https://www.abc.net.au/news/2024-05-01/australians-losing-5200-scammers-government-solutions/103785960

[4] https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-182mr-anti-scam-practices-of-banks-outside-the-four-major-banks/#:~:text=ASIC's%20analysis%20found%20that%20reviewed,the%202022%2D2023%20financial%20year

[5] https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-790-anti-scam-practices-of-banks-outside-the-four-major-banks/

[6] https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024

How our industry is fighting scams

The telecommunications sector has been working to combat scams, having developed and implemented several initiatives to disrupt scam activity.

Key actions include:

Reducing Scam Calls and Scam SMS industry code: In 2022, the telecommunications industry introduced a Reducing Scam Calls and Scam SMS Industry Code to reduce the number of scam calls and texts received by customers. This code was developed in collaboration with the communications regulator the Australian Communications and Media Authority (ACMA). The Code requires SMS service providers to identify, trace and block suspected SMS scams, and to conduct checks on organisations using text-based sender IDs. Carriage service providers (CSPs) are required to report to the ACMA blocked scam calls and SMS during each quarter. As a result of the code, the telecommunications industry had blocked more than 2.1 billion scam calls and 668 million scam SMS by the middle of 2024[7].

Engagement through the Scam Telecommunications Action Taskforce (STAT)[8]: The Scam Telecommunications Action Taskforce (STAT) was established by the ACMA in November 2019 to provide coordination and oversight of telco scam reduction activities across government and industry sectors. Carriers and carriage service providers have observer status to this Taskforce to provide expertise on specific matters. The STAT brings together representatives from key government agencies, telcos, law enforcement and other sectors to work collaboratively to combat phone scams (primarily calls and SMS) and to inform the ACMA's scam reduction activities and associated regulatory responses.

Action to prevent porting fraud: The mobile industry complies with the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*[9] which requires telcos to use multifactor ID authentication to stop porting fraud.

Advanced Spam Filtering and Call-Blocking Technologies: Telcos have invested significantly in developing and deploying advanced technologies to detect and block fraudulent messages and calls. For example, automated spam filters analyse message content, sender patterns, and suspicious links to intercept scams before they reach customers. Furthermore, call-blocking features have been enhanced to identify scam-related numbers and prevent them from making repeated attempts to defraud consumers.

Real-time Monitoring and Reporting: Telecommunications providers maintain sophisticated systems to monitor network traffic in real-time for signs of fraudulent activity, which enables blocking of suspicious activity and reporting it to law enforcement or regulators. The telcos also offer ways for customers to report scams to them. For example, in 2023 Telstra launched a new scam reporting service which allows customers to forward SMS and MMS scams to 7226 (SCAM) to help identify which scams are occurring. The service has received more than 250,000 messages[10].

Consumer Education Campaigns: The industry has led public education initiatives to raise awareness about common scams and how consumers can protect themselves. These campaigns have included SMS alerts, online resources, and educational partnerships with government agencies and consumer protection organisations.

[7] https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024

[8] https://www.acma.gov.au/scam-telecommunications-action-taskforce

[9] https://www.legislation.gov.au/F2020L00179/latest/text

[10] https://www.telstra.com.au/exchange/keep-snitching-on-scammers--how-our-new-7226-reporting-number-is#:~:text=How%20to%20report%20a%20scam,could%20be%20a%20little%20different

Cross-Sector Collaboration: Mobile telecommunications companies have worked closely with banks, government agencies, and cybersecurity experts to share information and coordinate efforts to stop scammers. This collaborative approach has resulted in the identification and shutdown of large-scale scam operations.

In March 2023, Telstra, in conjunction with QT (Quantium Telstra JV) and Commonwealth Bank announced a pilot trial of the 'Scam Indicator' aimed at protecting Commonwealth Bank and Telstra customers from phone scams where criminals try to trick people into transferring them large amounts of money. In October 2023, this pilot was expanded to a national effort, using a Telstra Application Programming Interface (API) that the Commonwealth Bank can integrate into their scam detection processes to identify high-risk scam situations in real time. Scam Indicator enables the bank to confirm if a customer is on a phone call, which is a prime indicator that a scam is occurring. This allows the partner the opportunity to contact the customer and conduct additional checks which protect individuals from transferring large amounts of money to criminals[11].

In July 2024, in a move to help stop bank impersonation scams and improve the customer experience, Westpac and Optus introduced a new in-app calling capability for Westpac customers[12]. Westpac SafeCall allows customers to receive calls via the app that are Westpac branded, verified by Optus and show a reason for the call. This will help give customers more certainty in the legitimacy of the call, at a time when bank impersonation scams are among the most common scam types impacting customers.

The Challenge of Combating Scams

While the telecommunications industry has made progress in combating scams, there is more to do, and it is an ongoing challenge. Unfortunately, there is no "silver bullet" solution to stop scammers. Just as techniques to stop scams evolve, so do the methods scammers use to scam, which makes it a never-ending game of 'whack a mole'. Tackling scams may need multiple solutions targeted at different aspects whether this be by blocking the delivery of scam communications or increasing protections for account security.

Even with the most advanced technology, robust industry codes, and increased collaboration between telcos, regulators, and other sectors, some scams will still occur. While regulatory and policy responses should focus on consistency in tackling scams across sectors this needs to balanced with sector-specific considerations. A flexible framework will support uplifting efforts in some sectors while allowing tailored approaches in highly technical and dynamic sectors, such as telecommunications, as all sectors will need to innovate and respond to evolving scam approaches.

[11] https://www.telstra.com.au/exchange/cyber-security-and-safety/cyber-safety/telstra-scam-indicator---how-it-works

[12] https://www.westpac.com.au/about-westpac/media/media-releases/2024/30-July/#:~:text=In%20a%20move%20to%20help,a%20reason%20for%20the%20call

Concerns with the Proposed Scams Prevention Framework

We are concerned that the proposed framework is attempting to address deficiencies in the banking sector and digital platforms by including principle-based obligations that may inadvertently create complexity and duplication in other sectors, such as telecommunications, where there is already an Industry Code in place. This approach may have unintended consequences, such as placing additional regulatory burdens on telcos that are unnecessary or impractical.

An overarching issue is the Scams Prevention Framework provides a lack of clarity about what constitute 'reasonable steps' for the telecommunications industry to deal with scams and therefore raises the risk of an interpretation being that telecommunications industry will block each and every scam from occurring. However, this approach would not recognise the constant and evolving nature of scams, and the flexibility telcos need to meet the inherently difficult challenge of blocking scams.

At a fundamental level, mobile operators should not, and do not, review the contents of every call or SMS. Rather, we have the capability to recognise patterns of calls and SMS which help us to identify and block scams. In addition, we have oversight over certain categories of high-risk transactions (eg SIM swapping or porting) that directly relate to our customer interactions. The specific obligations in the Scams Prevention Framework means there is little scope for a tailored code to be developed that reflects the role of mobile operators in preventing scams.

Duplicative Obligations

The framework introduces obligations that overlap with existing, well-functioning regulations in the telecommunications industry. For example, reporting and record-keeping requirements within the proposed framework duplicate obligations already imposed by the Reducing Scam Calls and Scam SMS Industry Code, creating unnecessary administrative complexity without improving scam prevention outcomes.

Complexity and Impracticality of Obligations

Some of the proposed obligations, such as extensive reporting, notification, and record-keeping requirements, appear onerous and impractical, especially when applied across multiple sectors with differing roles in scam prevention. In the case of telcos, these obligations could complicate operations without providing clear benefits to consumers.

For example, the balance between immediate disruption of scams and the opportunity for law enforcement to prosecute scammers needs to be carefully considered. Real-time reporting may compromise ongoing investigations if handled incorrectly.

Multi-Sector Regulators

The Framework proposes a tiered, multi-regulator model for oversight and enforcement of the proposed Framework. The ACCC would have responsibility for oversight and enforcement of obligations set out in legislation as well as systemic or cross-sectoral issues, with ASIC and ACMA respectively having responsibility for oversight and enforcement of sector specific obligations.

Our view is that introducing multi-sector regulators to oversee compliance with the framework could add unnecessary complexity. The creation of multi-regulatory models for duplicate obligations may confuse accountability and enforcement across industries, particularly for sectors like telecommunications that already have established, effective regulatory frameworks in place.

There is a need for clarity on how multiple regulators will interact under the proposed framework, particularly with respect to the establishment of an SPF External Dispute Resolution (EDR) scheme and the pathways for redress and compensation. Scams often involve multiple entities across different sectors, and we are uncertain how these schemes will handle jurisdiction and apportion liability across industries. The framework also provides multiple avenues for compensation, which raises additional complexity and uncertainty regarding liability. Any compensation scheme should be limited to the losses experienced due to scams associated with the customer's account with telecommunications providers, not the use of telecommunications services for a scam perpetrated for another regulated industry.

Additionally, a compensation scheme should include rules that mirror the UK compensation scheme's use of excess per claim and a cap on claims, to ensure the compensation scheme is protected from 'no risk' scam activity and fraudsters taking advantage of reimbursement schemes.

The Role of Subordinate Regulation

Typically, we would expect a framework of this nature to be drafted in such a way that obligations relate to what subordinate regulation or Industry Codes must address. For example, a framework might include provisions related to "Governance arrangements and policies" or similar obligations, which are then translated into specific industry standards and guidelines, such as the Consumer Data Right (CDR) framework.

However, in this instance, the proposed Scams Prevention Framework includes detailed obligations that relevant companies will need to comply with in addition to any Industry Codes or Rules. This risks duplicating existing obligations while also creating broader, less tailored requirements that may not fit the specific needs or circumstances of each sector.

Publication and Reporting Obligations

As noted earlier, the obligation to publicly disclose certain details about scam detection methods could have unintended consequences, including giving scammers insights into how to avoid detection. We also need to ensure that any privacy concerns are addressed.

Recommendations for Improvement

We encourage the government to take the time to get this right and we recommend that Treasury engage in further consultation with the telecommunications sector to develop a more workable framework that reflects the distinct roles, capabilities, and existing regulations of each industry involved in scam prevention.

This revised framework should allow for flexibility in drafting subordinate regulations that address sector-specific issues, such as Scam Prevention Framework (SPF) Rules or Industry Codes. We believe that an effective framework can be built around the following key principles:

Tailored Obligations for Each Sector

The framework should acknowledge the unique roles of different sectors in combating scams. For example, telcos have already established effective systems for blocking scam communications, while banks should focus on detecting and preventing fraudulent financial transactions. Obligations should reflect these differing responsibilities.

There should not be a 'one size fits all' approach to consumer reports, complaints handling and dispute resolution across all sectors. Participants in different sectors are likely to receive consumer reports about very different instances of 'scam'. For example, a telecommunications provider is likely to receive tens of thousands of 'scam' reports per day. Many are false positives: they are simply unwanted political and marketing messages or calls. It is not practical or desirable to keep individual records of these 'reports', even for the ones that are indeed scam. Keeping records on the volume of these reports would divert resources away from actions to disrupt scams.

Protection of Sensitive Information

The framework's reporting obligations should be designed to avoid disclosing too much information about how scams are detected and disrupted, as this could inadvertently assist scammers in developing workarounds. Similarly, care should be taken to ensure that reporting requirements do not compromise law enforcement efforts.

Clarity on High-Risk Customer Profiling

We need greater clarity on what is required to "identify customers at higher risk of being targeted by a scam" and how warnings should be provided. Given the volume of scam activity, telecommunications providers have no practical way of profiling customers who may be targeted, and we are unsure how this requirement would work in practice.

We need to address existing regulatory gaps[13]

The legislation and implementation of a mandatory SMS sender registry would assist the telecommunications sector in preventing scams. The telecommunications industry has previously urged the Australian Communications and Media Authority (ACMA) to tighten regulations around the use of mobile numbers, particularly to ensure that mobile numbers are only assigned to networks with intercell handover capability, as stipulated under the *Telecommunications Act 1997.* This requirement ensures that mobile numbers are used in genuine mobile networks, preventing misuse by fixed networks that lack mobile capabilities. Despite this clear regulatory framework, instances of non-compliance persist, undermining efforts to combat scams effectively.

Carriers without a proper mobile network or carrier licence have attempted to condition mobile numbers for use in fixed networks. In one instance, ACMA allocated mobile numbers to an entity lacking a legitimate mobile network, allowing them to route scam traffic from a fixed network. While an attempt to condition these numbers was refused, these entities have circumvented the rules by sourcing mobile numbers from legitimate providers to send scam traffic.

This not only violates the intended use of mobile numbers but also impedes efforts to prevent and track scam activity. Furthermore, the misuse of numbers across multiple networks severely limits the ability of carriers to apply more effective scam control measures, such as restricting numbers to the network to which they are conditioned or ported.

This issue has broader implications, including breaches of Integrated Public Number Database (IPND) obligations, presenting a national security risk. This makes it significantly harder for legitimate carriers to implement effective scam-prevention measures. As a result, carriers are left managing the fallout, often in a reactionary manner, as they attempt to address scam traffic in a fragmented regulatory environment.

If a regulator limits the tools available to carriers in fighting scams, it is unreasonable for telecommunications companies to bear the full cost of these regulatory shortcomings. Moreover, there are serious concerns around providing public information on how scams are being controlled, as such disclosures would provide scammers with the insights needed to bypass controls from mobile operators, further weakening the mobile industry's ability to protect consumers.

[13] AMTA member Pivotel, is an active supporter and proponent of the SMS SenderID Registry, and all forms of SCAM mitigation. Pivotel does not however support the remaining paragraphs of this section, acknowledging the complexities associated with the use of numbers and the Numbering Plan review and the subjective perspectives put forward.

AMTA

Australian Mobile
Telecommunications
Association