

**COMMUNICATIONS
ALLIANCE LTD**



Communications Alliance Submission

to Senate Economics Legislation Committee
in response to the

Scams Prevention Framework Bill 2024

8 January 2025

CONTENTS

ABOUT COMMUNICATIONS ALLIANCE	2
EXECUTIVE SUMMARY	3
1. INTRODUCTION	6
2. TELECOMMUNICATIONS SECTOR BACKGROUND	7
EXISTING WORK	7
TECHNICAL CAPABILITIES AND LEGAL CONSTRAINTS	7
3. INVESTMENT CERTAINTY AND ‘QUADRUPLE JEOPARDY’	8
‘QUADRUPLE JEOPARDY’	9
SECTOR CODE COMPLIANCE VS SPF COMPLIANCE	10
COMPENSATION & DIRECT RIGHT OF ACTION	11
4. SYSTEMS AND PROCESSES-BASED APPROACH	12
5. ‘ACTIONABLE SCAM INTELLIGENCE’	13
6. DELEGATION OF REPORTING DETAIL TO SUBORDINATE SECTOR CODES	14
7. IDR AND EDR	15
8. APPLICATION OF THE SPF	16
SUPPLY CHAIN AND SERVICE CONSIDERATIONS	16
EMAIL	16
INTERNET SERVICE PROVIDERS	17
CONSUMERS ROAMING OVERSEAS	17

About Communications Alliance

[Communications Alliance](#) is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

Executive summary

The telecommunications industry has long been at the forefront of the fight against scams, proactively developing an industry code in 2020. This code, which is registered and enforced by the Australian Communications and Media Authority (ACMA), has resulted in more than 2 billion scam calls and almost 700 million scam messages being blocked since its introduction. The code requires telcos to identify, trace, block, report, and disrupt scam calls and text messages.

There are positive signs that actions by Government and industry are starting to turn the tide against scammers. Financial losses to scams decreased by 13% between the calendar year 2022 and 2023¹, and decreased 41% from the financial year 2022/23 to 2023/24. The number of people reporting a financial loss decreased by 32% during the same period (2022/23 to 2023/24)².

However, more work remains to be done, and the telecommunications industry is committed to keeping up the fight against scammers.

Communications Alliance (CA) supports Government's ambition to develop a cohesive framework to limit scams across all sectors of the economy, including banking and digital platforms.

To make this framework as effective as possible, CA submits three key recommendations to make the draft legislation stronger and more enforceable:

1. Establish a safe harbour from 'quadruple jeopardy'

Under the draft SPF, telecommunications providers are subject to as many four concurrent enforcement mechanisms, and could face penalties even when they comply with sector-specific codes – creating a 'quadruple jeopardy' of liability.

CA submits that telecommunications providers that meet their requirements under a detailed sector code must have certainty that they have discharged of their obligations and:

- will not be subject to further enforcement action by the regulator;
- cannot be required to compensate SPF consumers for losses by an external dispute resolution scheme (EDR); and
- do not face civil liability brought by consumers, or by the regulator on behalf of consumers.

We recommend a 'waterfall approach' to compensation: banks, as custodians of consumers' monies, pay full compensation if found in breach of their sector-specific obligations. If banks are in compliance with their respective obligations but other sector(s) are not, those other sector(s) pay compensation, through a scheme of apportioning compensation yet to be determined through further consultation.

It should also be made clear that consumer complaints about scams should solely be handled by the designated EDR, AFCA, to prevent potential duplication of complaints to other EDRs, such as the Telecommunications Industry Ombudsman (TIO) or EDRs in other sectors.

Establishing a 'safe harbour' (alongside a focus on systems and processes) will create the necessary certainty for investment decisions (especially for entities that may be less inclined 'to do the right thing') and limit liability to areas that are within the realm of control of the entity. A sector-specific code that forms the minimum basis for compliance with the entire

¹ p. 1, Australian Government, National Anti-Scam Centre. (2024). *Targeting scams, Report of the National Anti-Scam Centre on scams activity 2023*. <https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

² p. 1, Australian Government, National Anti-Scam Centre, *National Anti-Scam Centre in action, Quarterly update April to June 2024*, Nov 2024. <https://www.nasc.gov.au/reports-and-publications/quarterly-update>

framework would send a clear signal for regulated entities as to how to focus company resources.

Under the Bill, a telecommunications provider would simultaneously be subject to liability across:

1. Sector regulator: the ACMA can be designated as the telecommunications sector regulator, responsible for registering and enforcing the sector's SPF code which must adhere to the principles in the framework;
2. General regulator: the ACCC would continue to regulate the telecommunications sector in relation to the SPF principles and any other provisions not contained in the code³;
3. External dispute resolution scheme (EDR): the Australian Financial Complaints Authority (AFCA) as the designated EDR⁴, with powers to determine compensation for consumers; and
4. Civil action: from SPF consumers and regulators (on behalf of consumers) through the courts, including class action.

If a telecommunications provider is found to be in breach of the sector code by the ACMA, then it would follow that it could also be subject to enforcement action or compensation through other mechanisms.

Given that sector regulators are responsible for mandating a code that reflects the SPF principles⁵, it is unclear how a telecommunications provider could be in compliance with the code but still be liable to enforcement by the general regulator that regulates those same SPF principles, as well as face liability under other enforcement/compensation mechanisms.

2. Target definitions and measures to the largest extent possible to individual sectors

While the current Bill contains substantially less detail than the Exposure Draft, further remaining detail ought to be delegated to sector-specific codes, including the definition of 'actionable scam intelligence' and attendant reporting requirements.

The resulting telecommunications sector code ought to reflect the state of technical capability, legal limitations and control, i.e. it comprehensively reflects telecommunications providers' roles and obligations.

Doing so will render the framework more effective and efficient as the (regulator-made) sector codes will be able to focus on the specific circumstances, technical capabilities and existing legal requirements of the regulated entities of each sector while also allowing for greater flexibility to adjust subordinate regulation as technology – and scam behaviour – evolves.

This approach would also provide an effective avenue to account for the diversity of the supply chains within respective sectors. As currently drafted, the SPF equally applies to all entities in the supply chain, irrespective of their control over the communications that traverse their networks.

For example, a single phone call or message between a sender and recipient will typically traverse the networks of several carriers and involve customer-facing carriage service providers as well as mere transit network providers – raising serious challenges about which link in the chain could or should be held liable when a scam occurs.

³ 1.24-1.27, 1.261, 1.272, The Parliament of the Commonwealth of Australia. (2024). *Treasury Laws Amendment Bill 2024: Scams Prevention Framework, Exposure Draft Explanatory Materials*

⁴ 1.30-1.31, *ibid*

⁵ 1.259, *ibid*

3. Focus on systems/processes (vs individual scams)

The SPF and subordinate regulation – and the definition of ‘actionable scam intelligence’ – ought to focus on the establishment of appropriate systems and compliance with required processes to prevent scams, as opposed to the prevention of individual scams.

Telecommunications providers do not have the technical capabilities, nor are they legally permitted (with limited exceptions) to scan individual communications. In addition, in the telecommunications sector, scams can only be detected through the aggregation of similar types of scam intelligence which, subsequent to validation, leads to the blocking of calls and/or messages. Consequently, a focus on individual scams creates significant implementation problems for our sector.

Note: CA's digital platform and other members did not participate in the development of this submission. Any reference to 'members', therefore, is limited to our carrier and carriage service provider (C/CSP) members.

1. Introduction

- 1.1. Communications Alliance (CA) welcomes the opportunity to provide this submission on the *Scams Prevention Framework Bill 2024* and associated Explanatory Memorandum (EM).
- 1.2. CA and its members have been proactively engaged in fighting scams for many years, having first registered a code with the Australia Communications and Media Authority (ACMA) in 2020, which has resulted in more than 2.1 billion scam calls and almost 700 million scam messages being blocked since its introduction.
- 1.3. We welcome the policy intent to develop a cohesive framework that seeks to limit scams across all sectors of the economy, including banking and digital platforms.
- 1.4. While some sectors are more advanced than others in efforts to combat scams, ongoing work is required in key sectors and across Government to enhance existing preventative measures and improve capabilities in a dynamic environment.
- 1.5. CA supports a framework that applies broadly, provided it:
 - is sufficiently clear and unambiguous in its application;
 - gives entities sufficient certainty as to their obligations, thereby allowing for and incentivising investment into scam prevention measures;
 - appropriately recognises the boundaries of responsibilities between entities within a sector, across sectors, and between entities and end-users; and
 - is flexible to account for sectoral differences and to adjust to the dynamic scam environment.
- 1.6. We commend Treasury for the amendments made in response to the consultation on the Exposure Draft of the Bill. In particular, we warmly welcome the removal of substantial detail from the SPF, with options for delegation to subordinate sector-specific codes.
- 1.7. We also appreciate the inclusion of a statutory review after three years, as well as the additional guidance provided in the EM of the Bill.
- 1.8. However, we remain concerned with the dual application of enforcement regimes alongside multiple avenues for consumers to seek compensation and to bring private action.
- 1.9. We equally believe that further work is required to ensure definitions and obligations are appropriately targeted on systems and processes, remaining detail (particularly with respect to reporting) is also delegated to subordinate codes, and IDR systems are empowered to function effectively, within entities and sectors but also across a complex, multi-sector environment.
- 1.10. These changes will ensure that the SPF can operate effectively.
- 1.11. We are keen to continue our constructive engagement with all relevant stakeholders, including Government, regulators and other regulated sectors to ensure the best possible outcome for consumers and the Australian economy can be achieved in the fight against scam activity.
- 1.12. We note that CA's digital platform and other members did not participate in the development of this submission. Any reference to 'members', therefore, is limited to our carrier and carriage service provider (C/CSP) members.

2. Telecommunications sector background

Existing work

- 2.1. The telecommunications sector, through Communications Alliance, took proactive action to combat scams in a coordinated manner at a time when many other sectors pursued scam prevention at a much more limited scale.
- 2.2. This work culminated in the registration of the ACMA-enforced C661:2020 *Reducing Scam Calls Industry Code* in 2020. This code was replaced by the C661:2022 *Reducing Scam Calls and Scam SMS Code (Scams Code)*, to also include scam short messages (SMS or 'texts') into the Scams Code.
- 2.3. Amongst other measures, the Scams Code sets out processes for identifying, tracing, blocking and otherwise disrupting scam calls and scam texts. The process is built on improved information sharing between C/CSPs as well as improved information sharing between industry and relevant Government agencies.
- 2.4. Since registration of the Scam Code(s), more than 2.1 billion scam calls and almost 700 million scam texts have been blocked, i.e. these scam attempts have never reached the intended recipient and likely harm has been averted or was, at least, minimised.
- 2.5. Recent reports by the National Anti-Scam Centre (NASC) show a reduction in scam losses by 41% in the FY 2023/24 and a reduction of people reporting a financial loss by 32% compared to the previous year.⁶
- 2.6. Our members also participate in other industry and Government-led activities that target the minimisation of fraud, for example in the work of the National Anti-Scam Centre (NASC), the Australian Financial Crimes Exchange (AFCX), including the Anti-Scam Intelligence Loop, and through the Security & Fraud Alliance Forum, an initiative of the telecommunications sector that brings together all major carriers, banks, crypto currency providers, large Australian brands and organisations, State, Territory and Federal police agencies, ID Care and law enforcement agencies, to exchange information in a highly operational context and cooperative environment.

Technical capabilities and legal constraints

- 2.7. C/CSPs cannot scan all content of all communications that traverse their networks for potentially malicious activity.
- 2.8. In addition to technical constraints and the sheer volume of such communications which act to prevent a comprehensive scanning, such action is largely prohibited under Part 13 of the *Telecommunications Act 1997* and Part 2-1 of the *Telecommunications (Access and Interception) Act 1979* (TIA Act). Such action is also subject to the interception warrant regime of the TIA Act.
- 2.9. Limited exemptions exist for the scanning of 'malicious SMS messages' under section 10A of the *Telecommunications (Interception and Access) Regulations 2017*. Importantly, the exemptions are limited to SMS where:
 - (a) the SMS message contains a link or a telephone number; and
 - (b) the purpose, or apparent purpose, of the SMS message is to mislead or deceive a recipient of the SMS message into using the link or telephone number; and
 - (c) the recipient would be likely to suffer detriment as a result of using the link or telephone number.

⁶ p. 1, Australian Government, National Anti-Scam Centre, *National Anti-Scam Centre in action, Quarterly update April to June 2024*, Nov 2024. <https://www.nasc.gov.au/reports-and-publications/quarterly-update>

- 2.10. There are no exemptions that would permit the scanning, i.e. interception, of voice calls without prior authorisation from a law enforcement agency through a warrant.
- 2.11. While C/CSPs have different technical tools and approaches, it is fair to say that, by and large, the identification of (potential) scams occurs on the basis of traffic patterns, including on the basis of the duration of calls, the calling line identification (CLI), the volume of texts, the presence of links and phone numbers combined with a 'call to action' for the intended recipients, and the alphanumeric sender ID (and its potential misuse). The detection of patterns is not ideal for solely identifying scam traffic, as it also captures legitimate traffic, but it is the primary technique carriers are using to detect and prevent potential scam communications. C/CSPs cannot target (nor do they have capabilities to target) individual scams using pattern recognition techniques.
- 2.12. It is key to understand that C/CSPs implement systems and processes that reflect the technical 'state of the art' at the time to detect suspicious traffic patterns. C/CSPs have limited capabilities to adjust their systems and processes to limit the likelihood of specific types of scams as those evolve, but make those adjustments to the extent this is possible.
- 2.13. The Scams Code reflects these technical capabilities in that it is based on the implementation of specific systems, processes and technologies to limit suspicious communications reaching their intended recipient. It also seeks to improve the 'quality' of CLI information through information sharing along the supply chain.
- 2.14. The SPF must recognise these limitations, alongside the responsibilities of our sector and those of other sectors that are often better placed to take meaningful preventative action. (Also refer to section 3.)
- 2.15. Consequently, the extent to which the SPF seeks to impose liability for compensation onto C/CSP, permits a direct right to action and includes severe penalties for non-compliance with the SPF – including potentially for individual scams – must be balanced with the substantial risk of incentivising C/CSPs to 'err on the side of caution' and block at scale, communications that are legitimate, and the risk of stifling investment into systems processes and competitive market outcomes.
- 2.16. Particularly in light of the commercial relationship between carriers (who own network units) and carriage service providers (who do not own network units and provide their service via the networks owned by carriers), the fact that there may be a number of providers between the scammer and customer, and the potential for penalties, this may encourage a heavy-handed approach by carriers adversely impacting the end-users receiving time sensitive information.

3. Investment certainty and 'quadruple jeopardy'

- 3.1. CA welcomes the inclusion of compliance with a sector code as one of the matters "*relevant to whether a regulated entity has taken **reasonable steps** for the purpose of a provision*" (s 58BB).
- 3.2. However, we do not believe that the mere inclusion of compliance with a sector code as only one matter 'relevant' to the consideration of the assessment whether reasonable steps have been taken will provide regulated entities with sufficient certainty in a framework that exposes entities to no less than four different avenues for enforcement and/or exposure to civil liability.
- 3.3. To be absolutely clear at the outset, we believe that C/CSPs have a role to play in the prevention of scams. In fact, the current sector code (Scams Code) already places substantial obligations on those entities. This code ought to form the basis of the future telecommunications sector code under the SPF (revised if and where necessary), as now envisaged by the Bill.

- 3.4. However, and contrary to the approach currently proposed in the SPF, C/CSPs that meet their requirements under a detailed sector code must have certainty that they have discharged of their obligations and
- will not be subject to further enforcement action by the regulator;
 - cannot be required to compensate SPF consumers for losses by an external dispute resolution scheme (EDR); and
 - do not face civil liability brought by consumers, or by the regulator on behalf of consumers.
- 3.5. This is a structurally inherent problem of the proposed approach and ought to be expressly addressed in the primary legislation through respective statements in relation to compliance with the SPF, and exemptions from compensation and liability in the appropriate sections.
- 3.6. Any underlying sector code ought to be regularly updated to ensure it evolves alongside a dynamic scams environment and technological capabilities. This dynamic approach is, realistically, impossible to be paralleled by the SPF contained in the primary legislation, thereby risking to further exacerbate the risk of 'compliance uncertainty' as it is unclear how the SPF would be interpreted to reflect the evolving sector codes.
- 3.7. We note that beaches of sector codes made by the general SPF regulator (ACCC) can attract civil pecuniary penalties.
- 3.8. We elaborate on the issue of multiple jeopardy below.

'Quadruple jeopardy'

- 3.9. The proposed SPF is applicable to designated entities irrespective of, and independent from, compliance with any sector-specific regulation, i.e. an entity can be compliant with its sector-specific subordinate regulation – yet still be found in breach of the primary legislation.
- 3.10. As a result, the proposed SPF creates a 'quadruple jeopardy':
- It subjects designated entities to a dual regime of obligations:
 - 1 the SPF itself; and
 - 2 subordinate regulation;with a dual set of penalties and a dual enforcement regime (ACCC and, for our sector, the ACMA); and
 - it subjects designated entities to a dual liability regime through:
 - 3 an external dispute resolution scheme (EDR), envisaged to be the Australian Financial Complaints Authority (AFCA) (s 58DC); and
 - 4 the right to private action which in turn hinges on compliance with the dual regime of obligations (s 58FZC).
- 3.11. In addition (and exacerbating the issue):
- regulators can make a claim against regulated entities on behalf of SPF consumers (s 58FZC); and
 - there may also be a dual EDR scheme. Also refer to our comments at section 7.
- 3.12. We strongly reject this approach.

Sector code compliance vs SPF compliance

- 3.13. It is unclear in what circumstances a C/CSP that has complied with the sector code could be deemed non-compliant with the SPF.
- 3.14. If the policy intent for this dual application of regimes (primary legislation and subordinate regulation) is to subject a designated sector to regulation immediately upon designation, we believe that alternative arrangements can achieve this aim. For example, sector-specific regulation could be made in parallel with the processes required for designation, with commencement of the regulation upon designation of the respective sector.
- 3.15. While some of the risk attached to this 'quadruple jeopardy' has been ameliorated through the removal of detail from the SPF itself, the issue remains of significant concern to our sector due to the remaining, partly ill-suited, detail contained in the primary legislation (also refer to section 5), and the continued existence of an approach that allows a regulator to find a regulated entity in breach of an SPF principle even if that entity had complied with its sector-specific subordinate regulation.
- 3.16. Under the proposed approach C/CSPs are subject to unacceptable uncertainty for investment decisions and risk of liability that they cannot reasonably limit. By contrast, a sector-specific code that forms the minimum basis for compliance with the entire framework would send a clear signal for regulated entities as to how to focus company resources.
- 3.17. For all commercial entities, investments are most likely to be made where they provide the best economic return and/or limit the risk of enforcement and liability. Investments for scam-related efforts compete with other investments. They may be viewed less favourably, especially by those less inclined to 'do the right thing', if they may not provide the 'immunity' that is required by the entity.
- 3.18. Additionally, the means to minimise exposure, to the extent possible at all, may involve substantial 'over-blocking' of legitimate communications as described under Section 2 above.
- 3.19. Consequently, C/CSPs that comply with the sector-specific regulation, i.e. the Scam Code (in its future revised version), ought to be deemed compliant with the respective principles of the SPF, i.e. compliance with the sector code must act as a 'safe harbour'.
- 3.20. Conversely, C/CSPs that do not comply with the sector code would be subject to enforcement action under the SPF.
- 3.21. The reforms to the *Security of Critical Infrastructure Act 2018* (SoCI Act) may serve as an example: that Act contains (as a cornerstone of the recent reforms) basic, sector-agnostic requirements for critical infrastructure entities to implement a Critical Infrastructure Risk Management Plan (CIRMP). Compliance with the telecommunications sector-specific rules to develop and implement a Telecommunications Sector Risk Management Plan (TSRMP) will be deemed as compliance with the CIRMP, but not the other way around. Tight sector rules were developed through a co-design approach with affected sectors. A similar approach ought to be pursued in the SPF.
- 3.22. Experience has also shown that the application of dual enforcement regimes – in our sector through the ACCC and the ACMA – can lead to confusion, duplication and, at worst, inconsistent outcomes. The complete delegation to subordinate regulation of all substantive obligations in relation to scam prevention would remove this additional complexity and risk.
- 3.23. If the Government felt it infeasible to remove all detail and dual application from the SPF, at a minimum, the primary legislation must put beyond doubt that compliance

with the applicable sector-specific code is sufficient for a regulated entity to be deemed as having taken all 'reasonable steps' and, consequently, also as having complied with the requirements of the SPF. The current addition of code compliance as only one factor in the list of matters for consideration is insufficient.

- 3.24. It is also important to bear in mind that an approach that subjects entities to multiple layers of liability equally bears the risk of creating multiple incentives to 'game the system' if compensation can be achieved through various avenues, with uncertainty for designated entities as to when they would be considered compliant with all layers of the SPF. Anecdotal (or at least not fully quantified) evidence from the UK suggests that the instances of consumers gaming the system, by fabricating a scam to claim compensation, are on the rise.
- 3.25. We note that s 58FM *Civil penalty double jeopardy* does not resolve the issue of dual application of two different sets of obligations and the resultant 'quadruple jeopardy' that we highlighted above. (S 58FM stipulates that if a person is ordered to pay a pecuniary penalty in respect of a particular conduct, then no pecuniary penalty can be ordered for the same conduct for the contravention of a civil penalty provision of an SPF principle or another Commonwealth law.)

Compensation & direct right of action

- 3.26. The volume, technical nature and legal constraints (that apply to protect the privacy of communications in Australia) in relation to communications travelling across telecommunications networks make the scanning for specific content in voice calls and SMS – and subsequent blocking of only illegitimate communications – often infeasible and/or exceedingly difficult (as well as, in many cases, illegal).
- 3.27. Limited exceptions apply, for example where scanning for specific URLs is being undertaken (see section 2).
- 3.28. C/CSPs can (and do) implement systems, processes and technical tools to detect scam activity. The requirements that underpin many of these actions are currently contained in the Scams Code and enforced by the ACMA. We would expect this code to form the basis for the telecommunications sector code under the SPF.
- 3.29. In addition to the requirements of that code, individual carriers have developed sophisticated tools to further increase the number of suspicious communications that can be detected on their services.
- 3.30. Carriers bilaterally engage with Australia's largest banks to further strengthen protections and make intelligence available, where permitted and feasible.
- 3.31. While all sectors have a role to play, it is incorrect to base the development of the primary legislation – or the subordinate legislation for the telecoms sector – on the premise that the designated sectors ought to be equally liable for damages or losses incurred as a result of scam activity.
- 3.32. While it may not be a popular opinion and unpalatable to other sectors, the telecommunications sector ought not to – and cannot – play the same role in the prevention of scams and, accordingly, in the liability for compensation where harm has occurred.
- 3.33. We submit that a 'Shared Responsibility Framework' similar to that proposed by the Monetary Authority of Singapore would be appropriate:

“Assessment of liability involves a 'waterfall' approach, which assesses the bank as the first line of responsibility as the custodian of consumer monies. If the responsible financial institution has breached any of its duties under the framework it is expected to fully compensate the consumer for the loss. If it is found to have met its

*obligations, telecommunications organisations will be assessed to ensure they have upheld their obligations and will be required to compensate the consumer for their loss if they have breached requirements. If both the responsible financial institution and telecommunications organisation are found to have upheld their obligations, the consumer will bear the loss and may seek recourse via dispute resolution bodies. The responsible bank and telecommunications organisation will be responsible for conducting the investigation in the first instance."*⁷

- 3.34. However, the above approach ought to be extended to also include other sectors with responsibilities in the scam ecosystem, including digital platforms, while maintaining the general principle of banks being the custodians of consumer funds (and the only entities in the ecosystem with control over financial transfers) with the first line of responsibility.
- 3.35. To be clear, C/CSPs ought to be held to account as part of the multi-sector approach to scam prevention, as they are already under the existing Code. However, liability – including liability to pay compensation or to private action – must be limited to instances of non-compliance with the underlying sector regulation, subject to the 'waterfall approach' outlined above. Alternatively speaking, the Scams Code (revised as necessary) ought to reflect the capabilities as currently available to C/CSPs for the prevention of scams through voice calls and/or SMS. Entities that comply with the Scams Code have discharged of their responsibilities in relation to scam prevention, noting that some carriers may be able to exceed the minimum requirements set out in such a code.
- 3.36. Importantly, the sector code ought to be seen as a key component – but not the only component – of the ecosystem approach to scam prevention. Other measures, including the SMS Sender ID Register and further work around enhanced CSP registration, 'Know Your Customer' and 'Know Your Traffic' requirements, and further strengthening the validation of the legitimate use of numbers/identification of customers using specific numbers, have the potential to further improve the ability to combat scams. The requirement to implement systems and processes in respect of such other measures could form part of the telecommunications sector code, thereby tying relevant obligations together in a single, clear and cohesive set of requirements.
- 3.37. Beyond these concerns, we highlight that the timeframe of six years (from the time of the action that relates to the alleged conduct) within which private action can be brought is extraordinarily long, given the vast amount of information (including personal information) that regulated entities would be required to hold in order to defend a claim.
- 3.38. Given that the vast majority (we were informally told about 75%) of scams are being identified within a month of the financial loss occurring (with many being identified within the first 24 hours after the loss occurring), the timeframe is, in our view, not justified.
- 3.39. The timeframe also appears inconsistent with Government's stated aim of data minimisation and reduced (and consistent) data retention obligations.
- 3.40. Consequently, we believe that this timeframe ought to be reduced to a maximum of 2 years.

4. Systems and processes-based approach

- 4.1. As highlighted above (see section 2), C/CSPs are unable and not permitted to scan the content of all communications that traverse their networks.

⁷ p. 29, Treasury, *Scams – Mandatory Industry Codes, Consultation Paper*, Nov 2023

- 4.2. In addition, scam activity is very sophisticated and highly dynamic, meaning that it is very hard to detect and disrupt in low numbers.
- 4.3. Usually, in the telecommunications sector, scams can only be detected through the aggregation of similar types of scam intelligence which, subsequent to validation, leads to the blocking of calls and/or messages. This necessarily means that until a 'critical mass' of scam intelligence has been available to a C/CSP, scams are likely to be delivered to customers prior to the application of preventative measures.
- 4.4. Customers may also report communications as scams which, while being undesired, in fact are marketing messages or similar (i.e. spam). Communications Alliance members report that the vast majority of scams reported directly to C/CSPs fall into this category. Note that these communications may or may not be in contravention of the *Spam Act 2003* or the *Do Not Call Register Act 2006*, i.e. they may be entirely legitimate. (Often, they are the result of unintended or 'unavoidable' subscriptions by consumers in order to avail themselves of an offer – an issue under investigation by the ACCC as part of its work around unfair trading practices.)
- 4.5. Beyond our concerns around the lack of legal certainty ('quadruple jeopardy'), we believe that the SPF is overly focused on individual scams and 'actionable scam intelligence'. Instead, the SPF – as well as the definition of 'scam' itself – ought to focus on the steps taken, through appropriate systems and processes, to detect and deter scams.
- 4.6. A changed focus, together with a clear and comprehensive compliance framework that provides a 'safe harbour', would provide regulated entities the certainty required to invest into capital and labour-intensive tools and measures that otherwise may be beyond the economic reach and incentive of an entity.
- 4.7. A focus on systems and processes (as opposed to individual pieces of content, or individual actions within millions of communications processed each day) is common practice in other regulatory regimes, e.g. the anti-money laundering and counter-terrorism financing (AML/CTF) regime which demands "*appropriate risk-based systems and controls*", the online safety regime enforced by the Office of the eSafety Commissioner, and the Security of Critical Infrastructure (SoCI) regime, just to mention a few.
- 4.8. Consequently, the SPF ought to be revised to ensure that relevant requirements – and criteria to establish whether 'reasonable steps' have been taken (if required at all under our proposed code-based compliance approach) – appropriately focus on regulated entities establishing adequate systems and following the required process.
- 4.9. Importantly, AFCA determinations are based on the (arguably subjective) standard as to whether a conduct is 'fair and reasonable in all the circumstances'. In line with the arguments above, an assessment by any EDR scheme in charge of scam-related complaints, including AFCA, ought to be directed at appropriate systems and processes being established and followed.

5. 'Actionable scam intelligence'

- 5.1. Against this background, we highlight the need to also amend the definition of 'actionable scam intelligence'. The definition, as currently drafted, focuses on "*a communication, transaction or activity relating to, connected with, or using a regulated service of the entity*" which, on reasonable grounds, is being suspected of being a scam.
- 5.2. The definition is overly broad, does not provide clarity as to the timing of the suspicion of a communication being a scam (i.e. does information become actionable scam

intelligence retrospectively, once 'critical mass' has been reached, or is it only forward looking?) and, as drafted, could include individual communications.

- 5.3. What constitutes actionable scam intelligence will be substantially different across sectors. It also appears likely that for all sectors it will be useful to limit 'actionable scam intelligence' to the information that is actually of use to the regulator and other parties in the system ('the signal vs the noise').
- 5.4. Consequently, we believe that the definition of 'actionable scam intelligence' itself would be best delegated to the respective sector codes, to ensure that each sector can provide the most meaningful information without overburdening the system or, worse, rendering information less valuable as useful information gets drowned out by less useful information.

6. Delegation of reporting detail to subordinate sector codes

- 6.1. We commend Government for removing substantial detail previously contained in the Exposure Draft of the legislation into sector codes that are to be developed (or revised) subsequent to the enactment of the SPF.
- 6.2. This will allow sector regulators to work with their respective sectors to develop targeted requirements that reflect the sectoral capabilities, legislative requirements and structural particularities, ultimately resulting in a more effective and efficient approach to combatting scams.
- 6.3. We note that this shift of detail has occurred with respect to most, but not all, principles: Each sector code is to include specific provisions for
 - principle 1—governance (division 2, subdivision B);
 - principle 2—prevent (division 2, subdivision C);
 - principle 3—detect (division 2, subdivision D);
 - principle 5—disrupt (division 2, subdivision F); and
 - principle 6—respond (division 2, subdivision G),with principle 4 – report (division 2, subdivision E) omitted from the principles that allow for sector-specific details to be set out in SPF codes.
- 6.4. We consider this omission impractical and strongly recommend detail in relation to reporting also be contained in sector-specific codes, i.e. we submit a provision similar to those contained ss 58BP, 58BY, and 58BZE find application for the reporting principle.
- 6.5. As currently drafted, the reporting requirements – also in conjunction with the definition of 'actionable scam intelligence' (refer to section 5) – are very onerous (or even impractical) while at the same time likely to offer limited value to other sectors and/or regulators.
- 6.6. As is apparent from the number of blocked calls and texts to date (more than 2.1 billion scam calls and almost 700 million scam texts), C/CSPs deal with an immense volume of potential and actual scam intelligence. However, the assumption that all of this intelligence would be of use to other parties is incorrect. In fact, we contend that the volume of information would overwhelm regulators while at the same time putting substantial strain on regulated entities.
- 6.7. Most scams that may be detectable for C/CSPs are conducted in campaigns (e.g. 'Hi Mum', 'You are the single heir') that exhibit similar or the same patterns and/or content, meaning that scam intelligence has the potential to be highly duplicative and/or outdated, and, therefore, to be of limited value.

- 6.8. It would be more useful, at least in our sector, to focus on new types of intelligence and patterns rather than individual pieces of 'actionable scam intelligence'.
- 6.9. Consequently, we recommend the inclusion of an option to delegate detail for reporting obligations to sector-specific codes, alongside a re-focused, sector-specific definition of 'actionable scam intelligence'.

7. IDR and EDR

- 7.1. Given the volume of communications, transactions and interactions with consumers across all sectors, it appears that any framework ought to be capable of dealing with a significant volume of complaints in relation to actual or alleged scams.
- 7.2. Any complaint system must place the customer experience of navigating the system front and centre.
- 7.3. Consequently, it will be imperative to ensure that the vast majority of complaints can be handled through IDR processes, including where scams may involve several sectors. Large numbers of complaints handled by an EDR scheme are likely to lead to a negative customer experience, unnecessarily impose costs on industry, and bear the potential of overwhelming the scheme itself. Only a small number of complex complaints ought to be referred/taken for resolution to an EDR scheme.
- 7.4. For regulated entities to be able to handle complaints in an increasingly interconnected scam environment, it will be necessary to enable a free exchange of relevant scam-related information, which may also involve (but not be limited to) a customer's personal information across regulated entities in regulated sectors.
- 7.5. Consideration ought to be given as to how this exchange of information can be facilitated, including where necessary through changes to relevant regulation/legislation and/or enabling legislation.
- 7.6. We would welcome further discussion with all relevant stakeholders on this issue.
- 7.7. Beyond the necessities to optimise IDR scheme responses and cooperation across sectors, we continue to be concerned with the apparent duplication of a scam-specific EDR scheme and the existing EDR scheme of the telecommunications sector.
- 7.8. The telecommunications sector is already subject to the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018*. The ACMA enforces the Standard.
- 7.9. Almost all C/CSPs must also be a member of the Telecommunications Industry Ombudsman (TIO) scheme, the independent EDR scheme for the sector.
- 7.10. In our view, scam-related complaints must only be dealt with by one EDR scheme. We cannot see a rationale for a duplicative approach and ask that the primary legislation establish a principle that a scam-related complaint will only be subject to the overarching EDR scheme established for the purpose of the SPF, envisaged to be the AFCA.
- 7.11. If indeed applicable at all, questions of liability for compensation ought only to be dealt with by the same EDR scheme (and, as applicable, the Courts).
- 7.12. In line with our earlier arguments, we advance that compliance with the respective sector regulation ought to establish an exemption from liability for compensation.
- 7.13. In instances where respective banks have complied with their sector code (i.e. the respective banks bear no liability for compensation), but more than one other sector has not complied with applicable sector codes, a mechanism for apportioning compensation is required. This could occur through subordinate legislation and/or

through arrangements/scenarios and worked examples, similar to the arrangements of the insurance sector.

7.14. We expect extensive and meaningful consultation on this issue will be required.

8. Application of the SPF

Supply chain and service considerations

8.1. The majority of communications involve two or more C/CSPs in their delivery. C/CSPs that form part of the supply chain are:

- the CSP owning the customer relationship with the end-user initiating the communication (e.g. sending a text);
- the originating carrier;
- transit carrier(s) (often several transit carriers are involved);
- the terminating carrier; and
- the CSP holding the customer relationship with the end-user receiving the communication.

Some of these C/CSPs may be international entities.

8.2. Importantly, not all C/CSPs in the supply chain have the same knowledge, control and influence in relation to a voice call or SMS that is being carried over a network. Depending on the circumstances, a C/CSP may have very limited or no knowledge or control over the communication and any intelligence in question.

8.3. As currently drafted, it appears that the SPF applies all obligations equally to all parties within the supply chain, irrespective of control and the efficacy of measures that regulated entities could apply. This approach is neither practical nor efficient.

8.4. The telecommunications sector code can (and does in its current version) deal with the respective roles within the supply chain and assigns requirements accordingly. However, the benefit of clear assignment of responsibilities afforded by the sector code is eroded by the dual application of the SPF and the sector code. In this context, the duality of compliance requirements not only causes unnecessary uncertainty, it also creates substantial inefficiencies and impracticalities for entities that are required to comply with the SPF obligations without appropriate control over the communication in question – all against the background of severe penalties, liability to compensation and private action. It appears that the C/CSPs would again heavily need to rely on whether (non-)compliance with a requirement of the SPF would be a 'reasonable step'.

8.5. At the very least, the SPF ought to contain the clear principle that (mandatory) sector codes (which are made by the general SPF regulator) can assign responsibility for compliance with specific aspects/principles of the SPF and, in doing so, exempt entities from the requirements of the SPF – without applying the test as to whether 'reasonable steps' have been taken.

8.6. We highlight that the assignment of responsibilities in our sector is complex. A designation of – or exemption for – specific sub-sector entities is unlikely to be able to adequately address these complexities.

Email

8.7. The SPF and/or the subordinate telecommunications-specific regulation ought not to apply to email services provided by C/CSPs, e.g. Bigpond or Optusmail (noting that

'Over-The-Top' (OTT) email services, such as gmail, Hotmail etc. would fall, if designated, in scope of the (sub-)sector for 'electronic services').

- 8.8. A screening of C/CSP email services is not feasible either because of technical limitations and/or because the implementation of measures would be vastly disproportionate to the likely harm caused and exceedingly costly to implement. Contrary to OTT email services, email systems provided by C/CSPs run on networks and systems that were not designed to provide these services. They are ancillary to the services of internet access and the provision of a mobile/fixed network. Many have been built to global standards, past or still applicable. Consequently, these networks and systems are far less adjustable (i.e. there are no simple 'bolt-ons' or network upgrades that could be used). Measures to 'scan' messages for specific scam intelligence would most likely require a 'rebuild' of systems associated with multi-year change programs and leading to unmanageable costs.
- 8.9. It should be noted that a large number of suspicious emails are being directed away from end-users through spam filtering. Spam filtering largely operates through a combination of volumetric indicators and sender identification but does not involve the screening of emails for specific URLs.
- 8.10. If it is envisaged that the SPF and/or subordinate legislation apply to C/CSP email services, any requirements or 'reasonable steps' ought to be limited to those that can be achieved through existing systems and tools, such as spam filtering.

Internet service providers

- 8.11. As currently drafted the primary legislation allows for designation of carriage services within the meaning of the *Telecommunications Act 1997*. Therefore, internet services, i.e. the provision of internet access and transmission of data ('the dumb pipe'), are included in the scope of sectors/sub-sectors that could be designated to fall in scope of the SPF.
- 8.12. We do not see a rationale for including internet services themselves (as distinct from services that use a carriage service, e.g. calls, SMS) into the scope of legislation as they have no knowledge (and cannot reasonably be expected to gain knowledge), control or influence over the communications that they facilitate. This ought to be rectified in the primary legislation by excluding internet carriage services within the meaning of the *Online Safety Act 2021* from the scope of the sectors that could be designated.
- 8.13. It is worth noting that s 313(3) of the *Telecommunications Act 1997* facilitates the blocking of domains through internet service providers when requested by appropriately empowered Government agencies. Such blocking is already taking place in relation to different illegal activity, for example, illegal offshore gambling, online academic cheating, the sale/advertisement of drugs without the required approvals, abhorrent violent materials, etc.

Consumers roaming overseas

- 8.14. We note that a C/CSP providing a mobile telecommunications service to a person in Australia that allows use of that service whilst overseas does not itself provide that service outside of Australia. Consequently, the person outside Australia may not be able to benefit from the same protections whilst overseas as the capability to control scam communications may be largely reliant upon the capabilities (and legal constraints) of the overseas mobile service provider.



Published by:
**COMMUNICATIONS
ALLIANCE LTD**

Level 25
100 Mount Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E
info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507