COMMUNICATIONS ALLIANCE LTD

Communications Alliance Submission

to Treasury
in response to the
Exposure Draft of the

Treasury Laws Amendment Bill 2024: Scams Prevention Framework

4 October 2024

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 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 2022 and 2023[1]. The median amount lost to scams decreased by half from $1,000 to $500. Reporting of scams increased by more than 18% in the same period. But there is more to do, 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. Move specific detail from primary legislation into codes

The Scams Prevention Framework (SPF) includes a significant amount of detail that would be more easily enforced and provide greater flexibility in sector-specific codes, rather than primary legislation. Regulated industries are likely to face implementation challenges as specific aspects which may be workable for one sector do not easily translate to others.

The telecoms sector is not homogeneous – the role of a carrier is different to that of a carriage service provider, which is different again to an internet service provider which merely provides access to the internet. 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 – raising serious challenges about which link in the chain could or should be held liable when a scam occurs.

These implementation issues could be avoided by moving detail into sector codes, which would still be required to be registered and enforced by sector-specific regulators (in the telecoms sector, ACMA).

2. Establish safe harbour from 'quadruple jeopardy'

Under the draft SPF, telcos 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 if a telco complies with the telco-sector code, it should benefit from a 'safe harbour' from enforcement by the general regulator (ACCC), the Australian Financial Complaints Authority (AFCA), and/or legal action.

Under the draft legislation, a telco would simultaneously be subject to liability across:

1. Sector regulator: The ACMA can be designated as the telecoms sector regulator, responsible for registering and enforcing the industry's SPF code which must adhere to the principles in the framework;
2. General regulator: The ACCC would continue to regulate the telecoms sector in relation to the SPF principles and any other provisions not in the code[2];

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

[2] 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*.

3. External dispute resolution scheme (EDR): The Australian Financial Complaints Authority (AFCA) as the designated EDR[3]; and
4. Civil action: From SPF consumers through the courts, including class action.

Given that sector regulators are responsible for registering a code that reflects the SPF principles[4], it is unclear how a telco 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 mechanisms.

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

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.

3. Accelerate practical measures to fight scams, including the SMS Sender ID registry and reforms to the Numbering Plan

The SPF must be supported by other strong measures to fight scams, and CA calls for the accelerated implementation of the SMS Sender ID Register and reforms to the Numbering Plan in concert with the SPF legislation.

The telecoms industry has already instituted a range of technical measures to identify, trace, block, report, and disrupt scams, and these measures will be bolstered by new SMS Sender ID requirements which will prevent scammers from pretending to be, for example, toll road operators or banks when sending bulk messages to consumers.

Similarly, the use of numbers across multiple service providers is an issue that the telecoms sector has sought clarification on from the ACMA. This clarification should be provided prior to any additional requirements being imposed on the sector.

The implementation of a mandatory CSP registry could also provide more accountability across industry by supporting targeted compliance and enforcement activity.

Note: As other industry groups represent the digital platforms sector, CA's digital platform members did not participate in the development of this submission.

[3] 1.30-1.31. The Parliament of the Commonwealth of Australia. (2024). *Treasury Laws Amendment Bill 2024: Scams Prevention Framework, Exposure Draft Explanatory Materials*.
[4] 1.259. ibid

1. Introduction

1.1. Communications Alliance (CA) welcomes the opportunity to provide this submission on the Exposure Draft (ED) of the *Treasury Laws Amendment Bill 2024: Scams Prevention Framework* (SPF) 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. 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.

1.3. 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.

1.4. 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;
- appropriately recognises the boundaries of responsibilities between entities within a sector, across sectors, and between entities and end-users; and
- can flexibly adjust to the dynamic scam environment.

1.5. The types of scams, the harm caused by them, the visibility of scams and the capabilities to prevent them vary substantially across sectors. Each sector has unique levers at its disposal to attempt to prevent scams and/or provide information and assistance to other sectors to do so.

1.6. Therefore, a truly overarching framework is likely to be most successful if it appropriately recognises sectoral differences and allows sectoral regulators with technical expertise to make subordinate legislation that reflects each sector's role and capabilities. The framework contained in primary legislation (i.e. the SPF) ought to limit itself to establish the structural components of the framework and the key requirements as they apply across all sectors. Any detailed requirements ought to be delegated to the subordinate, sector-specific regulation.

1.7. Unfortunately, we believe that the SPF does not take this approach as we will elaborate further below (section 3).

1.8. Beyond the SPF and subordinate regulation, other key measures must be progressed with urgency to enable the telecommunications sector to operate within a clear set of regulatory constraints and to maximise the sector's effectiveness in the battle against scams. Therefore, we urge Government and the relevant regulators to:

- to legislate and implement a mandatory SMS sender registry; and
- clarify the rules around the rights of use of numbers.

<u>Process</u>

1.9. We and our members are keen to continue our constructive engagement with all relevant stakeholders on this important issue.

1.10. Given the very limited time allocated for consultation on the ED of the SPF, the complexity of the proposed legislation and the concurrent large amount of unrelated regulatory proposals that affect our sector (e.g. 'Bean Review' recommendations), our feedback will be limited to some high-level observations. Unfortunately, we will be unable to provide detailed feedback on most of the drafting language and any issues that may arise from the specifics of the requirements. Our silence on these matters

does not reflect consent or dissent but is merely a reflection of the limited resources and time available to provide more detailed feedback.

1.11. We kindly ask the Treasury to also recognise the feedback that we and our members verbally provided during the two roundtable discussions on 1 October and at other occasions.

1.12. We would welcome an ongoing dialogue beyond the end of the formal consultation period. CA and our members are available for broader discussions as well as bilateral engagements.

1.13. We note that CA's digital platform 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) 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 SMs. 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 SMs 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. 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.

2.6. We note that, over the past decade, our sector has continuously warned of the use of SMs for the purpose of multi-factor authentication (MFA). The short messaging service (SMS or 'texting') was never intended for this purpose and, accordingly, was not developed on the basis of security protocols. In fact, SMS was not even intended for communication between end-users but rather with view to communicating network-related information.

2.7. Against this background and to ameliorate the situation (recognising that 'the clock could not be turned back'), our sector developed technical solutions that could contribute to minimise the risk that is associated with the ongoing use of SMS for MFA. We have consistently sought to engage with Australian banks to adopt those solutions. Unfortunately, these solutions were not taken up, despite what we believe limited costs. This needs to be recognised, including when considering sectoral responsibilities around compensation.

Technical capabilities and legal constraints

2.8. C/CSPs cannot scan all content of all communications that traverse their networks for potentially malicious activity.

2.9. 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.

2.10. 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.

2.11. 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.

2.12. 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 SMs, 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). While the detection of patterns is not the only avenue to detect and prevent scams, it is a key component in the arsenal of tools for our sector. C/CSPs do not target (nor do they have capabilities to target) individual scams.

2.13. It is key to understand that C/CSPs implement systems and processes, that reflect the technical state of the art at the given 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.

2.14. The Scams Code reflects the 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.

2.15. 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.

2.16. 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 must be balanced with the substantial risk of incentivising C/CSPs to 'err on the side of caution' and block, potentially at scale, communications that may be legitimate.

2.17. Particularly in light of the commercial relationship between carriers and carriage service providers, 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 relationship of carriage service providers and their customers.

Evolution of the existing Scams Code

2.18. We are keen to work with the ACMA, ACCC and the Treasury to ensure that the Scams Code reflects the policy intent of the six principles of the SPF.

2.19. To this end, it would be useful to get a better understanding of the policy intent of a number of specific requirements contained in the SPF, and to conduct a 'gap analysis' of the existing Scams Code vs such policy intent.

2.20. This process would allow our sector, in close collaboration with the ACMA, to address any deficiencies in a revised version of the Scams Code, without the need for ill-suited detail and prescriptiveness within the SPF.

2.21. In this context, we also reiterate our desire and previous request to make registered consumer codes, including the Scams Code, directly enforceable.

3. Approach of SPF and 'quadruple jeopardy'

SPF is overly detailed

3.1. As already articulated above, we support a cohesive overarching framework that seeks to address scams in key sectors of the economy.

3.2. However, we strongly believe that the SPF as proposed in the ED is overly detailed. As a result, and owed to the need to find application to all sectors in the economy, a number of the detailed requirements contained in the principles are ill-suited to the realities of our sector. We suspect that they may be equally inapt for other sectors.

3.3. Consequently, the primary legislation ought to limit itself to establish the structural components of the framework and mandate the development of and compliance with sectoral codes. All substantive requirements in relation to the prevention of scams (requirements currently contained under the six principles) ought to be delegated to the subordinate, sector-specific regulation.

3.4. To be absolutely clear, we believe that obligations to prevent scams can and ought to be placed onto C/CSPs, including through the SPF. However, it is, in our view, more effective and practical to impose such requirements through a revised version of the existing Scams Code. The ability to better target requirements to sectors will benefit consumers and designated entities alike.

3.5. This approach has been successfully employed in other economy-wide frameworks, including the reforms to the *Security of Critical Infrastructure Act 2018* (SoCI Act) and the *Consumer Data Right*.

3.6. We do not believe that this structurally inherent problem ought to (or can) be remediated through amended drafting language. We also do not believe that clarification or additional information in the EM are an appropriate means to address this issue. The EM is useful for clarification of policy intent and serves its purpose where legal action has been brought in relation to the primary legislation. It does, however, not provide the entities subject to the primary legislation with the legal certainty that they require in a technically complex and commercially challenging environment.

'Quadruple jeopardy'

3.7. 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 but yet be found in breach of the primary legislation.

3.8. As a result, the proposed SPF creates a 'quadruple jeopardy':

It subjects designated entities to a dual regime of prescriptive 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); and

4 the right to private action which in turn hinges on compliance with the dual regime of obligations.

3.9. In addition, there may also be a dual EDR scheme. Also refer to our comments at section 5.

3.10. We strongly reject this approach.

3.11. It is unclear in what circumstances and why a C/CSP that has complied with the sector regulator-approved/registered regulation could or ought to be deemed non-compliant with the SPF.

3.12. 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.

3.13. The issue of 'quadruple jeopardy' is exacerbated by the ill-suited detail contained in the primary legislation: where such detail is impractical in our sector or even potentially detrimental for consumers, and/or compliance is dependent on the interpretation whether all 'practical steps' have been taken, C/CSPs are subject to unacceptable uncertainty and risk of liability that they cannot reasonably limit.

3.14. We note that section 58FJ *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.

3.15. As a matter of principle, where entities are subject to liability and penalties, they must also be enabled to limit their exposure to such liability and penalties through compliance with clear and enforceable legislation/regulation. We believe that the ED of the SPF does fails short in that respect.

3.16. Additionally, the means to minimise exposure, to the extent possible at all, may involve substantial 'over-blocking' of legitimate communications.

3.17. 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 Scams Code must act as a 'safe harbour'.

3.18. Conversely, C/CSPs that do not comply with the Scams Code would be liable under the SPF.

3.19. Again, the reforms to the 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.

3.20. 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.

3.21. If the Treasury felt it infeasible to remove the 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, where it exists and is regulator-enforced, 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.

3.22. We consider this an unnecessarily complex approach and prefer the delegation of detailed requirements to the subordinate legislation and the complete removal of dual application of the two regimes.

3.23. 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.

4. Compensation & direct right of action

4.1. As previously highlighted, we believe all sectors, including the telecommunications sector, have an important role the play in the prevention of scams and the minimisation of the harms they cause.

4.2. Telecommunications facilitate almost every aspect of modern lives and societies. As a result, telecommunications networks and the services provided over those networks are also being used for an uncountable number of purposes. Some of these purposes are misaligned with the intended use of a service (as is the case of SMS) while others are simply malicious.

4.3. The volume, technical nature and legal constraints (that apply to protect the privacy of communications in Australia's democracy) 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.

4.4. Limited exceptions apply, for example where scanning for specific URLs is being undertaken.

4.5. C/CSPs can (and do) implement systems, processes and technical tools to detect scam activity. The requirements that underpin many of these actions are contained in the Scams Code and enforced by the ACMA.

4.6. In addition to the requirements of the Code, individual carriers have developed sophisticated, successful tools to further increase the number of suspicious communications that can be detected on their services.

4.7. Carriers bilaterally engage with Australia's largest banks to further strengthen protections and make intelligence available where permitted and feasible.

4.8. Unfortunately, not all of the initiatives that CA and its members have developed, that could further reduce the likelihood of scams causing harm to consumers, have been taken up by the banking sector.

4.9. Telecommunications services, in particular SMS, are being used for MFA, against the express warnings of our sector of the risks that are associated with such use.

4.10. To improve the security of SMS, such as where a bank will send a one-time-code for the purpose of authenticating a customer prior to resetting a password or conducting a financial transaction, the telecommunications sector has twice developed solutions that would signal to a bank that the phone number they were about to send the message to, was recently subject to a SIM swap, had been ported to another telecommunication provider, or was in an unexpected location such as roaming overseas. This would raise 'red flags' that the bank could use to gauge the risk of allowing such a high-risk transaction to occur.

4.11. While all sectors have a role to play, it is incorrect to base the development of the primary legislation – or the subordinate legislation for our sector for that matter – on the premise that the designated sectors ought to be, in principle, equally liable for damages or losses incurred as a result of scam activity. 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.

4.12. To be clear, C/CSPs ought to be held to account as part of the multi-sector approach to scam prevention. However, liability – including liability to pay compensation or to private action – must be limited to instances of non-compliance with the underlying sector regulation. 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 the Scams Code.

4.13. The Code ought to be regularly updated to ensure it evolves alongside a dynamic scams environment and technological capabilities.

4.14. Importantly, the Scams Code ought to be seen as a key component – but not the only component – of the ecosystem approach to scam prevention. Other measures – beyond measures specifically pertaining to other sectors – ought to be taken to complement our sector's Code:

- The implementation of a mandatory SMS sender registry could substantially assist all sectors of the economy, and especially the telecommunications sector, in the fight against scams. It is unclear why the SPF is being progressed in this manner and within the envisaged timeframes while the work on the register appears to make progress against a much less ambitious timeline.
- The use of numbers across multiple service providers is an issue that the telecommunications industry has sought clarification on from the ACMA for more than three years, and we believe that it is important for this issue to be resolved prior to any additional requirements being imposed on our sector.
- The implementation of a mandatory CSP registry could provide more accountability across industry by supporting targeted compliance and enforcement activity.

5. EDR

5.1. The telecommunications sector is already subject to the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018*. The ACMA enforces the Standard.

5.2. Almost all C/CSPs must also be a member of the Telecommunications Industry Ombudsman (TIO) scheme, the independent EDR scheme for the sector.

5.3. It is unclear whether the SPF envisages a dual regime also in relation to EDR. Section 58BZD appears to suggest this.

5.4. 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.

5.5. Consequently, questions of liability for compensation ought only to be dealt with by the same EDR scheme (and, as applicable, the Courts).

5.6. While we expect the detail for apportioning liability through an EDR scheme to be contained in subordinate legislation and be subject to extensive further consultation with the involved sectors, in line with our earlier arguments, we advance that compliance with the respective sector regulation ought to establish an exemption from liability for compensation.

6. Reporting

6.1. Accumulating and consolidating intelligence on suspicious scam activity across all designated sectors is an important component of a cohesive framework. Our sector supports measures aiming at improved sharing processes and intelligence quality.

6.2. Indeed, the Scams Code is built on information sharing along the C/CSP supply chain and with the ACMA. In addition, individual members (all mobile carriers) also engage in the Anti-Scam Intelligence Loop.

6.3. While we are not in a position to provide detailed feedback on the definition of 'actionable scam intelligence' (which is the subject of the reporting requirements of the SPF) and the details of the proposed reporting arrangements, we highlight the following points:

- It is imperative that the identification of actionable intelligence and the subsequent reporting be complemented by an improved verification of the intelligence, e.g. though impersonated entities. This will not only improve the quality of the scam intelligence but, importantly, minimise communications that are inadvertently blocked because they appear to be illegitimate when they are, in fact, not.
- The reported intelligence only ought to be reported into a single central point, i.e. to the general SPF regulator (ACCC NASC) instead of both, the sector regulators and the NASC.
- At a minimum, the sector-specific regulation ought to provide clear expectations as what constitutes such actionable scam intelligence, with view to such data being manageable in quantity and useful to the receiving regulator and other sectors. There is limited (or no) use in reporting actionable scam intelligence that is of unique use to the telecommunications sector but has no bearing on the potential actions of other entities.

7. Application of the SPF

Supply chain and service considerations

7.1. 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 sending end-user;
- the originating carrier;
- transit carrier(s) (often several transit carriers are involved);
- the terminating carrier; and
- the CSP holding the customer relationship with the recipient.

Some of these C/CSPs may be international entities.

7.2. 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.

7.3. Accordingly, we find it difficult to envisage how a designation of the sector (assuming all C/CSPs will be designated) will appropriately direct the detailed requirements contained in the principles of the SPF to the C/CSP that has, if at all, the capability to comply with those.

7.4. For example, requirements aimed at notification of end-users are only suitable for the CSP holding a relationship with the recipient whereas requirements to disrupt a scam may be impossible to comply with for that CSP (as it does not own any network components and merely resells a carriage service) or transit carriers (that may have very limited ability to positively identify a scam).

7.5. While we acknowledge that the Scams Code can (and does) deal with the respective roles within the supply chain and assigns requirements accordingly, the dual application of the SPF and the Scams Code again cause unnecessary and unwelcome uncertainty – 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 compliance with a requirement of the SPF would be a 'reasonable step'.

Email

7.6. 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').

7.7. A screening of 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 carriage service providers (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.

7.8. 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.

7.9. If it is envisaged that the SPF and/or subordinate legislation apply to 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

7.10. 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.

7.11. 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.

7.12. It is worth noting that section 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.

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