Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

AUSTRALIAN TELECOMMUNICATIONS ALLIANCE SUBMISSION

To: Department of the Treasury

Re: Scams Prevention Framework – Draft law package and position paper

19 December 2025

TABLE OF CONTENTS

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE

1.1 The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.

1.2 For questions on this submission, please contact Deputy CEO Christiane Gillespie-Jones, c.gillespiejones@austelco.org.au.

2. INTRODUCTION

2.1 The ATA welcomes the opportunity to provide a submission to the Department the Treasury (Treasury) in response to its consultation on the Scam Prevention Framework – Draft law package and position paper.

2.2 Our submission will focus on feedback on the exposure draft of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2025* (Designation), the associated Explanatory Statement, and the *Advancing Australia's Scams Prevention Framework through Codes and Rules: Position paper* (Position Paper).

2.3 We do not provide feedback in relation to the draft Designation or proposed code rules as they relate to the banking or digital platform sector.

2.4 We note the timeframe for consultation is spanning the Christmas and holiday period, thereby effectively limiting responses to be provided by 19 December. Therefore, at this stage, our feedback is limited to high-level considerations. We may provide further feedback at a later stage once members had an opportunity to consider the proposals in more detail.

2.5 Please note that only ATA's carrier/carriage service provider members participated in the development of this submission and Appendix A. Individual members may make additional submissions.

3. OVERARCHING FEEDBACK

3.1 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 2.3 billion scam calls and almost 1 billion scam messages being blocked since its introduction. The code requires telcos to identify, trace, block, report, and disrupt scam calls and messages.

3.2 Our sector is also in the process of implementing an SMS Sender ID Register, to commence operating by 1 July 2026. We believe that the SMS Sender ID Register will further significantly reduce scam messages reaching Australian consumers and, therefore, contribute to an additional layer of protections from scams in our sector.

3.3 In addition, individual members entered into bilateral partnerships with regulated entities from the other designated sectors, to develop powerful, customised solutions that target the specific threat vectors and capabilities of the involved entities. Members will continue to work collaboratively and extend partnerships where feasible.

3.4 The ATA supports Government's ambition to implement 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, additional sectors that pose a significant threat vector ought to be designated with urgency. Government ought to announce an upcoming designation and an indicative timeline as quickly as possible to put those sectors on notice and to allow those sectors to proactively uplift their respective scam protection measures. Those sectors include:

a) Online market places

b) Dating platforms

c) Non-bank money remitters

d) Remote access software suppliers

e) Crypto exchanges

f) Superannuation

3.5 Given the proposed timeline for commencement of the SPF sector codes on 1 July 2026, we urge Government to initiate a cooperative process of genuine co-design of specific sector obligations for the sector codes and rules, led by the respective sectors and sector regulators. This will provide for the most effective and efficient exchange of expertise and development of practical code obligations which often require significant technical and operational debate. It will also allow for the development of effective codes in the context of other requirements under already existing regulation, including (for our sector) the *C661:2022 Reducing Scam Calls and Scam SMs industry code* (Scams Code), the *SMS Sender ID Register (Application, Access and Administration) Determination 2025*, the *Telecommunications (Interception and Access) Regulations 2017*, the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*, the *Telecommunications Consumer Protection Code* (TCP Code, currently submitted to the ACMA with request for registration), and the *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* (before Parliament).

3.6 The Position Paper recognises compliance with the sector codes as the primary factor in the assessment whether a regulated entity has taken 'reasonable steps' under the SPF. The Paper lists a number of additional factors to be considered in that assessment, including the size and capacity of the entity, the kind of service, the tailoring of measures to the consumer of a service, and the risk profile of service.

In addition to those factors, and noting that some of those may not equally apply across sectors, additional factors ought to considered for an assessment of 'reasonable steps', including:

a) An entity's compliance with other regulatory obligations (outside of the SPF and subordinate instruments) that have a bearing on the SPS principles (for example the *SMS Sender ID Register (Application, Access and Administration) Determination 2025*); and

b) A consumer's behaviour, including negligence or where a consumer wilfully and knowingly accepts unreasonable risks.

3.7 The SPF seeks to apply high-level definitions and principles which do not convey sufficient specificity for entities to make investment decision for the purpose of developing processes and tools to further enhance protective measures. They also do not provide the desired level of regulatory certainty for entities seeking to demonstrate compliance with the SPF.

Consequently, it is imperative that the sector codes and rules contain a reasonable degree of prescriptiveness to ensure a regulated entity is clear about its obligations and the actions required to comply with those. It will be important to resist the temptation to draft principles-based obligations to account for all potential future scenarios at the expense of sufficient clarity for today's challenges. While we acknowledge that the scam environment is dynamic, we also highlight that codes can be adjusted as required and could be subject to a regular review cycle to ensure they remain fit for purpose and evolve with the threat landscape.

3.8 We note the proposal to defer commencement of the Report principle to late 2027, with the respective rules to be developed by March 2027. Presumably, this approach has been chosen to allow the National Anti-Scam Centre (NASC) to build an intelligence sharing platform and to allow regulated entities to develop systems and processes to share and receive actionable scam intelligence (ASI) through the NASC.

We believe that this approach is not viable given the SPF's reliance on ASI for all SPF principles, including the Respond principle, i.e., internal and external dispute resolution (IDR/EDR), and the liability that arises for regulated entities for non-compliance with all SPF principles.

The definition of ASI in the SPF is broad and, so we believe, does not provide sufficient specificity to stand on its own and does not provide adequate certainty to comply with the requirements of the SPF until the proposed commencement of the rules for the sharing of ASI (proposed for late 2027).

We elaborate on this matter at sections 5.71 to 5.78.

3.9 The Position Paper proposes a commencement of IDR-related obligations through the Respond principle as of 1 July 2026. The commencement of EDR processes through AFCA is proposed for 1 January 2027.

We believe that this approach and the proposed timeframes are not viable as they separate IDR and EDR commencement dates and risk creating substantial difficulties for regulated entities, AFCA, and consumers.

We elaborate on this matter at sections 5.44 to 5.56.

4. DESIGNATION

4.1 The draft Designation applies to all carriers and carriage service providers (C/CSPs), irrespective of size, supply chain considerations, technical capabilities, and end-user connection.

4.2 The telecommunications market is diverse comprising several hundred C/CSPs, many of which are very small and serve less than 1,000 customers. In addition, communications (SMS/MMS, voice calls) are delivered through a complex supply chain that often involves several entities to deliver a communication from the originating to the receiving end-user. Often entities in scope of the draft Designation neither have a connection to the originating nor the receiving end-user. Accordingly, technical and commercial capabilities vary substantially across the sector and along the supply chain for each of the SPF principles.

4.3 Consequently and noting the broad application of the draft Designation, we request that the differentiation required to account for those differences in capabilities and roles will be applied through the SPF sector code for each of the SPF principles and, as required, also in the overarching rules.

4.4 We also submit that the Explanatory Statement for the Designation ought to clearly convey that expectation.

4.5 Against this background and expectation, we make the following observations:

4.6 The draft Designation is, in-principle, workable provided the following changes are made:

a) The draft Designation defines 'message service' as *"a service that enables messages to be sent or received using a carriage service (other than where a message is carried wholly over the internet)"*. We assume that the definition is attempting to account for an inclusion of Rich Communication Services (RCS) into the scope of services provided by C/CSPs. The Explanatory Statement to the draft Designation also notes that the definition of 'message service' *"includes, but may not be limited to, a short message service, multimedia message service and rich communication service"*. [emphasis added]

This inclusion appears to rest on an incomplete understanding of technical detail. While C/CSPs enable the functionality of RCS and authenticate message entitlements, where messages are being transmitted over their networks, they have no visibility of or control over individual RCS messages and, therefore, would not be able to apply 'know your traffic' (KYT) measures under the SPF principles or subordinate

instruments to those messages. The ability to disrupt messages as part of the authentication process is also limited.

Consequently, the separate definition of 'message service' is unnecessary (or ought to be limited to SMS and MMS) and the definition of 'covered telecommunications service' ought to be amended to only include SMS, MMS and voice calls (not carried the internet).

b) Against the above, we also seek an amendment to the definition of 'covered telecommunications service' with respect to the proposal that *"voice call and message services that are initiated over the internet that terminate on a carriage service (or vice versa)"* be in scope for covered telecommunications services. This inclusion is infeasible for the same reasons as outlined in a) above and ought to be removed.

4.7 We have provided an explanatory paper on RCS and its regulatory context in Appendix A to the submission. While RCS and related services, such as Rich Business Messaging (RBM), are still evolving services, we believe that the explanations provided at Appendix A highlight that RCS (due to their over-the-top nature) would be more appropriately dealt alongside instant messages rather than carriage services.

5. PROPOSED CODE RULES

5.1 We welcome the proposal of specific rules for inclusion into the respective sector codes. We understand from our subsequent discussions with the Treasury that those are to be viewed as a 'starting point for discussion'.

5.2 It is imperative that the design of an effective and practical telecommunications sector code takes into account the different roles of C/CSPs in the ecosystem and, importantly, in the supply chain from origination to delivery of a communication. It must also rest on realistic approaches to the technical capabilities of the sector overall and as arising from supply chain considerations. We elaborate on both of these issues in the following sections.

5.3 Accordingly, our feedback on the proposed sector code rules for the respective SPF principles is predicated on an appropriate differentiation of such rules (including that they may not apply equally to all C/CSPs) to account for supply chain, technical, and commercial capabilities.

SUPPLY CHAIN AND SERVICE CONSIDERATIONS

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

a) the CSP owning the customer relationship with the sending end-user;

b) the originating carrier;

c) transit carrier(s) (often several transit carriers are involved);

d) the terminating carrier; and

e) the CSP holding the customer relationship with the recipient.

5.5 Some of these C/CSPs may be international entities.

5.6 Importantly, not all C/CSPs in the supply chain have the same knowledge, control, and influence in relation to a voice call or SMS/MMS 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.

5.7 Given the draft Designation applies broadly to all C/CSPs, the sector code and any rules must 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.

5.8 For example, requirements aimed at notification of end-users are, if at all, 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).

TECHNICAL CAPABILITIES AND LEGAL CONSTRAINTS

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

5.10 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.

5.11 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 (note that RCS are not in scope, for the reasons stated above) 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.

5.12 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.

5.13 While C/CSPs have different technical tools and approaches, it is fair to say that, to date, 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 or end-users.

5.14 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.

5.15 At this stage, 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 through information sharing along the supply chain.

5.16 Our members are also working with the ACMA on measures that focus on additional improvements to 'know your customer' (KYC) and 'know your traffic' (KYT) processes across the supply chain.

5.17 These efforts are complemented by the implementation of the SMS Sender ID Register. The Register will

commence on 1 July 2026, i.e., unregistered sender IDs will be over-stamped with 'unverified'. (Please refer to the ACMA's explanatory material for further detail on the Register.)

5.18 Given the SPF's provisions for liability for compensation, the severe penalties for non-compliance, and the direct right to action, any future sector code requirements 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.

5.19 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.

FLOW AND 'DECISION TREE' OF SUSPICIOUS COMMUNICATIONS

5.20 To assist with our subsequent feedback on some proposed sector code rules, it is useful to sketch out, at a very high-level, the flow and 'decision tree' around suspected scam activity for C/CSPs:

Communication blocked:

a) Communications at scale (i.e., all SMS, MMS, voice calls).

b) Appropriate C/CSP in the supply chain detects abnormal patterns for some communications.

c) Appropriate C/CSP in the supply chain concludes that identified communications are suspicious and ought to be blocked (i.e., 'potential scam threshold' reached).

d) Appropriate C/CSP in the supply chain blocks communications, i.e., no scams occur associated with those communications.

e) Potential remediation efforts where communications have been incorrectly blocked (false positive).

Communication delivered:

a) Communications at scale (i.e., all SMS, MMS, voice calls).

b) Appropriate C/CSP in the supply chain does not detect abnormal patterns or concludes that abnormalities are not suspicious (i.e., 'potential scam threshold' not reached).

c) Appropriate C/CSP in the supply chain delivers communications to the intended end-user. (Usually, this is not the same C/CSP that has made the threshold decision in b)).

d) No C/CSPs in the supply chain has any further knowledge whether the delivered communications are associated with (attempted) scams, unless this information is provided ex-post (i.e., after delivery of the communications) from an external source.

e) Potential efforts to detect further suspicious communications on the basis of the information provided by external sources, where possible (with limited options).

5.21 This highlights an important point: C/CSPs do not detect scams or fraud – they only detect suspicious activity at a systemic level rather than for individual communications. Our feedback on the SPF principles ought to be considered in this context.

GOVERNANCE

5.22 Given the limited time to respond, we do not provide feedback on the proposals for the Governance principle at this stage.

PREVENT

5.23 At a high level, most of the proposed policy outcomes and code rules for this principle appear sensible.

5.24 However, we note that the proposal to offer additional protections to consumers at higher risk of being scammed and to consider vulnerability over time is largely infeasible for C/CSPs. SMS, MMS, and voice calls are provided to and used by all end-user cohorts in Australia, i.e., any Australian is the recipient of these types of communications. It is not possible to discern communications on the basis of possible recipients and to apply targeted measures.

5.25 Even if it was legally permitted to do so (this would require user profiling), it is, in our view, also infeasible to directly address specific end-user cohorts to alert them to scam types. Such alerts and information would be best communicated through centralised information portals and/or through a C/CSP's website.

5.26 Importantly, suspicious activity is typically identified at or close to the originating network, whereas any preventative alerts or notifications would need to be directed at the end-user by the terminating network which holds the end-user relationship but is usually not the same as the originating network.

5.27 The Position Paper proposes that *"Carriage service providers must verify a customer has a legitimate use case before offering certain services. This includes confirming a customer has a legitimate use case to originate calls using a number not allocated to the originating carriage service provider."*

We note that the SMS Sender ID Register includes the verification of a legitimate use case for sender IDs.

Our members are also in ongoing, advanced discussions with the ACMA on further measures in relation to KYC/KYT to improve the legitimacy of voice calls overall, including those that make use of the multi service practice (MSP).

DETECT

5.28 As highlighted above, C/CSPs are not capable of detecting scams. They may detect suspicious communications/activity at a systemic level rather than individual communications.

5.29 It remains also important to consider supply chain differences: not all C/CSPs in the supply chain hold an end-user relationship and/or would have visibility of suspicious activity. The SPF sector code must, therefore, sufficiently differentiate obligations.

5.30 The Position Paper proposes policy outcomes and sector code rules that go to the investigation of a scam, understanding the nature of a scam, and having systems in place to detect consumers impacted or potentially impacted by a scam, and more specifically in the telecommunications sector, to identify consumers who received a scam communication and the consumer's subsequent engagement with that communication.

5.31 These proposals appear to misunderstand the capabilities of C/CSPs. As outlined in section 5.20 and 5.21, C/CSPs either block a suspicious communications (no knowledge of scams) in which case no further activity

with respect to those communications is required as no scam can derive from that communication; or, where the threshold for blocking has not been reached, the communication is delivered to the end-user without any further intelligence as to the nature of that communication.

5.32 Accordingly, C/CSPs are unable to undertake activities to understand the nature of a scam. Instead, they take measures to understand what types of patterns and abnormalities may be present in suspicious communications and refine their systems accordingly.

5.33 It also follows that C/CSPs cannot proactively and at scale identify customers that may be impacted by a scam associated with a communication that they have transmitted/delivered as it had not reached the threshold for blocking, for example where a scammer holds a 'normal' conversation with a victim as part of a romance scam.

5.34 C/CSPs may be able to take further action or investigate upon receipt of intelligence from an external source, e.g., once an end-user has made a report to a bank about a potential scam and discloses their phone number and/or the number (if available) which sent a communication, and/or information contained within the communication, such as a call-back number or a URL. Such further action already takes place where information is provided in a timely manner and is actionable by a C/CSP.

5.35 By and large, C/CSPs transmit communications 'real time'. After all, the nature and utility of voice calls and SMS/MMS lies in the almost instantaneous transmission of a message. Blocked communications are usually not stored, thereby not allowing for an investigation and subsequent 'release' if found legitimate. Even if this was possible, the delay incurred in doing so would render most communications futile. Consequently, any requirements to investigate and detect needs to be balanced against the alternatives available to C/CSPs, i.e., to 'err on the side of caution' and block messages with the risk of 'over-blocking, i.e., blocking messages that are legitimate, potentially at scale.

DISRUPT

5.36 Our feedback in response to the proposed policy outcomes and sector code obligations for the Disrupt principle flows on from the arguments outlined in section 5.20 and 5.21 and the Prevent and Detect principles.

5.37 To the extent a proposed outcome or code rule entails the identification of an affected or potentially affected consumer, e.g., for notification of disruptions to their service, these are either infeasible or implausible, for example where a communication has been blocked and, therefore, never reached a consumer. The consumer is clearly impacted by the disruption (although likely unaware) but it would be infeasible and implausible to notify the consumer of the blocking action.

5.38 We also reiterate our comments (also refer to sections 5.23 to 5.27) in relation to targeted alerts or notifications. Any such measures that would involve the profiling of end-users is either not permitted under law and/or infeasible and/or inappropriate. The provision of information through centralised platforms (e.g., ACCC Scamwatch) or a C/CSP's website appears more practical.

5.39 The proposal to withdraw CLI from calls and SMS/MMS to and from phone number that are the subject of an investigation of ASI requires careful consideration, and we caution against a blanket use of this measure. The removal of CLI can be effective where it neutralises the potential (fake) authentication through a number. However, CLI is also used to alert consumers of potential scams and, consequently, the removal of CLI would impede these protection measures.

RESPOND / INTERNAL AND EXTERNAL DISPUTE RESOLUTION

5.40 The proposals for the Respond principle, alongside the limited detail available about, and deferred implementation of, the sharing of ASI are of great concern to our sector.

5.41 We welcome the acknowledgement in the Position Paper that liability only arises from non-compliance with the SPF. The SPF in turn requires regulated entities to take 'reasonable steps' to comply with the six SPF principles, with the primary factor for assessment of such reasonable steps being compliance with the sector code. We highlighted the importance of other, secondary, factors for consideration in section 3.6.

5.42 We understand the proposals of the Position Paper on IDR and EDR, in broad terms, as follows:

a) IDR requirements (under the Respond principle) are to commence with the sector codes on 1 July 2026.

b) Regulated entities in the designated sectors are to cooperate for the resolution of complaints in IDR schemes in a manner that minimises the burden for consumers and through a 'no wrong door approach'.

c) Specific timeframes for the acceptance, acknowledgement and resolution of complaints apply, to align with the Australian Securities and Investment Commission (ASIC) Regulatory Guide 271 (RG271) on Internal Dispute Resolution for the banking sector where possible.

d) The exchange of ASI remains unregulated until late 2027. The (broad) definition of ASI in the SPF applies. Also refer to our comments at sections 5.71 to 5.78.

e) The Position Paper is silent on how non-designated sectors ought to be involved in IDR/EDR, implying that regulated entities handle all aspects of a complaint and, where redress is sought, compensate the consumer for losses arising from the actions of non-designated entities, provided at least one regulated entity is non-compliant with the SPF or subordinate instruments.

f) Regulated entities are to provide consumers with a statement of compliance with specific items of content, including outlining the steps taken for compliance, the remedy offered (if any), and escalation pathways.

g) Where more than one regulated entity has not complied with its obligations, those entities are to jointly provide compensation that reasonably represent the consumer's losses, with an equal share of compensation being paid by each entity as the default.

h) Where no resolution of a complaint occurs or the outcome is unsatisfactory in the eye of the consumer, the complaint can be escalated to AFCA as the EDR scheme.

i) AFCA will develop and consult on rules for the scheme, including eligibility, the complaint handling process, and its decision making process.

j) AFCA commences to accept complaints as of 1 January 2027. However, the issue that gave rise to the complaint may have occurred prior to that date (presumably as of 1 July 2026).

k) A 'scam complaint' or the scam-related portion of a complaint can only be adjudicated by AFCA, i.e., a complainant cannot seek resolution of the complaint through other EDR schemes, including the Telecommunications Industry Ombudsman (TIO).

5.43 We raise significant concerns with this approach overall and specific individual components of the approach.

Timing of IDR / EDR

5.44 Regulated entities of the three sectors are keen to cooperate with each other to further enhance scam prevention measures and address issues where those arise. In fact, regulated entities from different sectors (such as mobile network operators and banks) have already jointly developed very effective technical

solutions. Regulated entities also cooperate in the Security & Fraud Alliance Forum.

5.45 However, at this stage, it is unclear how regulated entities from designated sectors could cooperate to resolve complaints at scale.

5.46 This undertaking is made even more difficult because

a) non-designated entities are likely to form part of many or most potential scams; and

b) in the absence of a coordinated approach to the exchange of ASI across sectors, it is likely that any 'intelligence' (whether actionable or not, and potentially of low quality/certainty) will be provided by regulated entities to other regulated entities, in bilateral, manual processes. Given the 'intelligence' has been received, it must be assessed for 'actionability'. Also refer to our comments at sections 5.71 to 5.78.

5.47 Given the substantial complexities that the new development of any IDR scheme in one sector would involve, it appears that the simultaneous establishment of a new IDR scheme for three sectors, to operate alongside unregulated sectors without an IDR scheme, is bound to create a substantial number of complaints for escalation to an EDR scheme, in this case AFCA. We believe this will be the case, irrespective of any best intentions and efforts by all involved parties

5.48 Therefore, given the decoupling of the commencement dates for IDR requirements (1 July 2026) and the EDR scheme (1 January 2027), and the potentially large volume of complaints, AFCA is likely to inherit a significant backlog of escalated complaints, and this at a time where the organisation itself is still ramping up to full-scale operations. This is likely to create a bad experience for all involved, regulated entities, AFCA and, importantly, consumers alike.

5.49 We reiterate our desire to cooperate with other sectors to work together to implement IDR solutions that are practical, proportionate and, importantly, effective and useful for consumers. We are also keen to work with AFCA to minimise the number of complaints that are to be adjudicated through AFCA.

5.50 Therefore, we recommend delaying the Respond principle obligations until 1 January 2027 to align with the commencement of the EDR scheme. This will allow regulated entities to develop less manual and more cooperative processes that result a better consumer experience. It potentially also allows the three designated sectors to consider options for a third-party IDR administration scheme which has the potential to be the most effective and consumer-friendly approach to IDR.

<u>EDR scheme and rules</u>

5.51 The Position Paper proposes that the detail of the EDR scheme be prescribed in the AFCA rules to be consulted on and published by AFCA at a later stage. The Paper indicates that the Treasury believes that EDR-related obligations are not necessary in the sector codes.

5.52 However, in order to design an effective and efficient IDR scheme, across three sectors, it will be important for these sectors to have an understanding as to how the EDR scheme (i.e., AFCA) proposes to admit eligible complaints and make decisions on those complaints. How does it intend to deal with large volumes of low-value scam complaints? How does it propose to apply its 'fair and reasonable' jurisdiction? How would remediation work?

5.53 It will also be key to clearly delineate jurisdictions between existing sectoral EDR schemes, such as the TIO and AFCA to ensure that consumers, regulated entities and EDR schemes have a clear understanding of and pathway to dispute resolution that avoids duplication of efforts and, worst case, deliberate 'double litigation' by consumers.

5.54 It is worth noting that, to date, financial remediation in the telecommunications sector is fundamentally different to remediation in the banking sector. C/CSPs typically apply credit to existing accounts with account holders using the credit for future services provided by the C/CSP. By and large, they do not 'pay out' customers. In addition, the C/CSP that holds the customer relationship is unlikely to be the C/CSP which may

have contributed to a scam messages reaching the end-user. This means that the C/CSP that may be liable for redress (fully or in part, where non-compliant) may have no relationship with the complainant and, therefore, no established way to compensate the complainant.

5.55 Therefore, we request that AFCA provide an initial draft for consultation on the rules prior to the sector codes being made so that, where required, sector codes can be guided by the proposed approach.

5.56 To reduce initial complexity, we believe it could be worth exploring staging the implementation of the EDR scheme by the loss that resulted from the scam, potentially with higher-value losses (that may have life-altering consequences) forming the first phase of complaints adjudicated by AFCA.

Non-designated entities

5.57 We acknowledge that an ecosystem approach to scam prevention would be difficult to implement with all sectors of the economy onboarding at the same time. Therefore, by definition, regulated entities will need to interface with non-regulated (i.e. not designated) entities in the interim. This includes the resolution of complaints where non-designated entities are involved.

5.58 This being the case and given some non-designated sectors must be considered key scam vectors, we again urge Government to prioritise the designation of additional sectors and to make respective announcements (including timelines) to put those sectors on notice.

Doing so is not only important to relieve already designated sectors of unnecessary commercial and operational burden, but also to minimise the number of 'sectors for retreat' for scammers who will dynamically adapt and move to sectors with lesser preventative measures and friction.

Statements of compliance

5.59 The Position Paper states that upon receipt of a complaint, a regulated entity is required to provide a statement of compliance (as prescribed by the SPF) and to "*resolve the complaint (including issuing any proposed remedy) within specified timeframes*". We disagree with this statement. Why (and how) would a regulated entity be required to resolve a complaint when it has complied with its obligations under the SPF and subordinate instruments?

5.60 It also appears that the term 'statement of compliance' may be confusing or a misnomer. We understand from the Position Paper that it is contemplated that this statement could also indicate non-compliance with requirements under the SPF or subordinate instruments. However, we believe it is highly unlikely that a regulated entity would proactively attest to non-compliance to a consumer and, as a result, potentially invite regulatory action in addition to being held liable (potentially at large scale) under the SPF.

5.61 The proposed statement of compliance more resembles an IDR response as prescribed in the ASIC Regulatory Guide 271 Internal dispute resolution.

5.62 We believe that, in principle, an IDR response from regulated entities alleged to be involved in a scam can be a useful tool for consumers, either for escalation to AFCA, or for the purposes of further pursuing their complaint with a non-designated entity. However, we note that the content of this response must allow the regulated entity to apply automated processes to establish whether, in its opinion, it has complied with requirements, and any other information it is required to provide.

5.63 This is important as C/CSPs will have very limited abilities to further investigate a complaint where a complainant or another regulated entity shares an originating (or terminating) phone number (or other intelligence) with a C/CSP. We anticipate that the introduction of the SMS Sender ID Register and additional KYC/KYT measures are likely to further reduce instances where a C/CSP's actions (or lack thereof) contribute to scam activity.

Apportionment of compensation

5.64 The Position Paper suggests an equal apportionment of compensation where more than one regulated entity has not complied with their respective requirements.

5.65 We disagree with this default approach and request that the quality and quantity of information available to a regulated entity, and the capacity to control and influence individual scam activity must be taken into account in the apportionment of compensation.

5.66 We maintain that, as a default, liability should be allocated to the entity that is best placed to mitigate the harm. Banks hold this position as the custodian of a consumer's funds. Banks also hold high-quality and reliable consumer information, such as data on financial wealth, and transaction habits and history. C/CSPs, in contrast, can only assess communications at scale travelling across their networks by technical indicators and patters, without any further knowledge of the consumer receiving a communication. In other words, a knowledge imbalance must not be remediated by means of a 'compensation balance' on the basis of a misunderstood concept of 'fairness'.

5.67 Therefore, in our view, regulated entities in the banking sector involved in the scam loss occurring ought to bear the responsibility for full redress if those entities have not complied with relevant requirements. After all, it is hard to see why a C/CSP would be asked to pay an equal share of compensation in a scenario where control over the funds rested with the bank and only the transfer of those funds created a compensable loss while the C/CSP had very limited ability to detect the scam and, as a result, to prevent it, irrespective of its compliance obligations.

5.68 This approach would also more closely align with the approach taken in other jurisdictions, notably Singapore and the UK.

5.69 This approach also appears to the most economical, efficient and consumer-friendly approach, presumably the reason why it has been chosen in those jurisdictions.

5.70 We also highlight that an 'equal by default' approach risks tilting a C/CSP's blocking attitude towards an otherwise unacceptable level of blocking with a significantly increased likelihood of blocking, at scale, legitimate communications.

ACTIONABLE SCAM INTELLIGENCE

5.71 The Position Paper proposes to defer commencement of the Report principle to late 2027, with the respective rules to be developed by March 2027. Presumably, this approach has been chosen to allow the NASC to build an intelligence sharing platform and to allow regulated entities to develop systems and processes to share and receive ASI through the NASC.

5.72 At this stage, we have very little visibility or understanding of the solution or platform that the NASC is developing. From what we understand so far, we believe that the NASC is largely relying on application programming interfaces (APIs) to exchange ASI between relevant parties (including potentially other exchange platforms such as the AFCX Intel Loop or the Global Signals Exchange (GSE)) but does not develop a centralised case management system.

5.73 However, in the medium term (if not in the short term) a centralised case management system is required. It is imperative to capture ASI alongside with the outcome of an affected entity's investigation whether the reported ASI was indeed actionable and, if so, what actions have been taken, to what effect, and by which entity. The sharing of this information is at least as important as the sharing of ASI itself in order to maintain a viable sharing environment. Without a centralised case management system it is likely that regulated entities unnecessarily invest resources into scam investigations (for scams that have already been 'resolved'), fail to receive the ASI in a timely manner (thereby greatly reducing the value of the ASI), or operate in an environment that requires numerous (potentially unmanageable) peer-to-peer engagements.

5.74 Without further rules and detail on ASI prior to 1 July 2026, regulated entities are only guided by the definition of ASI in the SPF. This definition is broad and, so we believe, does not provide sufficient specificity to stand on its own and does not give entities the required certainty that they have complied with the requirements of the SPF in relation to ASI.

5.75 Given the SPF's reliance on ASI for all SPF principles, including the Respond principle, i.e., internal and external dispute resolution (IDR/EDR), and the liability that arises for regulated entities for non-compliance with all SPS principles, we believe clarity of what constitutes ASI for each designated sector, and an efficient mechanism to exchange and manage the ASI is required.

5.76 However, we are also conscious of the complexity of this task. Therefore, we propose to:

a) For commencement by 1 July 2026, clearly define a limited set of data points per sector that may, subject to the threshold test at b) being met, constitute ASI;

b) For commencement by 1 July 2026, clearly articulate, building on the definition in the SPF, when ASI is actionable. We believe ASI is actionable when a regulated entity has the information necessary to identify a specific transaction, communication, or other activity that is suspected to be a scam (activity), and determines for its own internal purposes that the activity has violated its terms of service, guidelines, or product policies and is likely a scam, so long as its policies are reasonable. This last question, of whether an entity's policies are reasonable, is well suited to investigation and enforcement by a regulator under the SPF codes.

c) Subsequently, phase in the exchange of ASI, potentially by source (intra-sector, cross sector, other external sources etc.) The phasing of the exchange of ASI ought to be done in alignment with the commencement of IDR/EDR.

5.77 In addition to the concerns and proposed alternative approach put forward above, we are mindful that the ASI exchange platform built by the NASC may in itself be a target for perpetrators of scams and other malicious activity as, in order for it to achieve its intended purpose, the platform is likely to contain vast troves of information, including personal information. While it could be argued that only information that has met the threshold of ASI, and therefore of likely criminal activity, is being shared through the platform, we are concerned that it may be impossible to neatly separate ASI from associated information (including personal information) that may not pertain to a criminal actor.

5.78 Designated sectors, including the telecommunications sector, will continue their cooperative efforts to develop timely, efficient and proportionate sharing arrangements. In doing so, we will continue our constructive engagement with the other designated sectors, the Treasury, the ACMA and the NASC.

6. OTHER ISSUES

6.1 As already outlined in the Position Paper, the definition of a scam is broad and insufficiently, if at all, delineates scams (as originally intended to be captured under the SPF) from misleading and deceptive conduct in trade or commerce where disputes relate to the buying and selling of goods and services.

6.2 In our members' experience, many consumers 'mistake' misleading and deceptive conduct and unsolicited sales as scams (in its intended meaning). While we acknowledge that both are distressing for consumers and can have far-reaching negative consequences, they are substantively different from a legal and technical perspective.

6.3 Consequently, we strongly recommend additional clarity and delineation be provided through the sector codes and/or rules.

APPENDIX A: RICH COMMUNICATION SERVICES

A.1 This document has been developed by the mobile network operator members of the ATA as an informative and explanatory piece on Rich Communication Services (RCS) more broadly. While its original intention does not relate to scam prevention, we believe it to be helpful to understand the limitations of C/CSPs in this context and for the purposes of the draft Designation.

A.2 We highlight that the RCS environment and supply chain is complex and evolving. We welcome further discussion on technical and regulatory aspects of RCS with of all involved stakeholders.

WHAT IS RCS & WHY IMPLEMENT IT?

A.3 RCS offers consumers several advantages over legacy SMS and MMS, providing a more interactive and versatile messaging experience. Unlike SMS, which is limited to plain text messages, and MMS, which can handle multimedia but lacks advanced features, RCS enables the sending of longer messages, supports new media types, and uses end-to-end encryption. RCS also includes advanced delivery notifications such as read receipts and typing indicators, enhancing the user experience. Ultimately, this makes RCS a more feature-rich alternative to traditional SMS and MMS, offering consumers a modern and seamless messaging experience.

A.4 The retail RCS market is dominated by Apple (via its iMessage platform) and Google (via its Google Messages platform). All Apple iOS devices support iMessage and all Android devices support Google Messages. A longstanding issue has been the lack of interoperability between the two RCS platforms. That results in messages exchanged between an iOS device and Android device being sent as SMS messages rather than via RCS. However, this is changing following the announcement by Apple that they will support interoperability with Google RCS, enabling the ubiquity of RCS across smartphones.

A.5 The reliance on access to an underlying data carriage service for RCS communications to be exchanged between two RCS-compatible devices remains unchanged.

CURRENT STATUS OF RCS

A.6 Apple and Google have launched iMessage and Google Messages respectively as over-the-top (OTT) services, integrating with the native message clients on iPhones and Android phones, with all Apple iOS devices supporting iMessage and all Android devices supporting Google Messages. This enables messages to be exchanged between iPhones or between Android phones without traversing MNOs' messaging infrastructure.

A.7 In some markets, message exchange between iPhones and Android devices has been enabled (usually in cooperation with local Carriers), increasing the number of potential messages exchanged outside MNO visibility. In Australia at present there is no integration of MNO capability with Apple iMessage or Google Messages. The only function supported is the data connection used by the OTT service.

FUTURE STATUS OF RCS

A.8 The anticipated enabling in Australia of a subset of the 'Service Entitlement Configuration' (TS.43) standard

from the GSM Association (GSMA), will facilitate interconnectivity between Apple and Android devices (including eSIM swaps) and enable MNOs to facilitate OTT delivery of more RCS functionality to customers.

A.9 Enabling TS.43 will enable Apple's and Android's messaging apps to use rich messaging features between devices in these two different ecosystems, including Rich Business Messaging (RBM). RBM will enable businesses to use logos, send invoices, and offer other rich messaging services to customers.

A.10 Enabling TS.43 will also allow the creation of an RCS token for customer authentication. This will enable RCS customers to send RCS messages to Apple and Android devices. Customers will need to have an active service with the MNO, having accepted the MNO's Terms of Service, to utilise RCS. The authentication token is the only part the Carrier plays in the call flow, with the actual customer messaging not traversing carrier-provided network units for RCS messaging, in contrast to the way SMS is handled today. Apple and Google remain in full control of the servers and network units used for the iMessage and RCS services.

A.11 The timeline to enable TS.43 to allow for RCS as an MNO-facilitated OTT service in Australia is to be confirmed. MNOs will have individual plans that may have different release dates, the details of which remain commercial-in-confidence.

A.12 The rollout of interoperable RCS environment means that in future, it is highly likely that RCS will use end-to-end encryption, like OTT and other application-based services. (Refer to additional comments below on regulatory implications.)

RCS DOES NOT QUALIFY AS A CARRIAGE SERVICE

A.13 RCS is a messaging protocol layered on top of IP networks. While it may resemble SMS/MMS in user experience, its architecture and operational model diverge from traditional carriage services. Reasons for this include:

a) Application Layer Delivery: RCS messages are transmitted via servers controlled by Apple or Google using internet connectivity, not directly over carrier-controlled infrastructure.

b) RCS providers have no Direct Control of Network Units: Neither Apple nor Google own or operate the underlying transmission facilities (i.e., network units) used to deliver RCS messages. These are typically provided by Carriers operating mobile networks or by Internet Service Providers (ISPs).

c) End-to-End Encryption and OTT Characteristics: RCS functions as an over-the-top (OTT) service, like WhatsApp or Signal, where the service logic and data routing are managed independently of the Carrier network. The use of end-to-end encryption for RCS would limit the ability for regulatory oversight under legacy telecommunications arrangements.

A.14 As such, RCS is not a listed carriage service to the public using a Carrier's network unit.

TREATMENT OF RCS UNDER REGULATORY OBLIGATIONS

A.15 Different implementations of RCS are likely to appear the same to end users but will have different underlying behaviours for the purposes of multiple regulatory obligations.

A.16 The implications of RCS not being a carriage service include:

a) *Telecommunications Act 1997*: RCS is not subject to CSP obligations e.g. emergency call routing, service standards, telecommunications consumer protection (TCP) industry code.

b) *Telecommunications (Interception and Access) Act 1979*: As RCS is an OTT service, not a carriage

service, it is not subject to lawful interception or metadata retention requirements. Even if OTT services like RCS were to be included under this legislation, the anticipated use of end-to-end encryption at the device level would have implications for lawful interception and law enforcement. The location/jurisdiction for message storage (i.e. inside/outside Australia, USA vs Singapore vs Taiwan) is also relevant for lawful interception, data sovereignty and data retention obligations.

c) *Telecommunications (Consumer Protection and Service Standards) Act 1999*: RCS is outside the scope of consumer protections specific to the telecommunications industry.

d) *Competition and Consumer Act 2010* (Parts XIB and XIC): RCS is not subject to access or anti-competitive conduct provisions tied to carriage services.

e) *Scams Prevention Framework Act 2025* (SPF) and subordinate instruments: RCS might be subject to obligations for digital platforms under the SPF but it must not be subject to the proposed obligations for the telecommunications industry sector due to the lack of visibility and control of RCS by carriers. Even if OTT services like RCS are included under the SPF, the anticipated use of end-to-end encryption at the device level would have implications for scam detection and scam prevention.

f) *Telecommunications (Interception and Access) Regulations 2017*: the protections afforded to carriers and carriage service providers to allow them to identify and block malicious messages (to the extent possible) only apply to SMS/MMS but not RCS.

g) Limited Regulatory Oversight: ACMA has limited jurisdiction unless broader digital platform regulation is introduced.

Ends

Australian
Telecommunications
Alliance

Level 25 / 100 Mount Street
North Sydney NSW 2060

T 02 9959 9111
E info@austelco.org.au
W austelco.org.au

ABN 56 078 026 507