Submission on the Scams – Mandatory Industry Codes – Consultation Paper

2 February 2024

Submission on the Scams – Mandatory Industry Codes Consultation Paper.

2 February 2024

1. EXECUTIVE SUMMARY

1.1 Pivotel Group Pty Limited ("**Pivotel**"), Australia's fourth Mobile Network Operator ("**MNO**") welcomes the Treasury and the Department of Infrastructure, Transport, Regional Development Communications and the Arts (**DITRDCA**) consultation into Mandatory Industry Codes intended to combat scam. For simplicity, in this submission we will simply refer to Treasury.

1.2 Pivotel does not intend to address all of the questions raised in the Consultation Paper published in November 2023 (the "**Consultation Paper**"). Rather, it has sought to address the broader issues and topics raised by the Consultation Paper.

1.3 In many respects, the telecommunications sector has been ahead of the game in combatting scams. Since the Reducing Scam Calls and SMs Code 2022 (the "**Telco Anti-Scam Code**") was amended, CSPs have blocked over 336.7 million SMS, while 1.4 billion scam calls have been blocked since the code was first introduced (from December 2020)[1]. As a result, Pivotel considers that a key part of the Government's response should involve other sectors benefitting from the lessons learned in telecommunications and potentially adopting similar frameworks.

1.4 Pivotel supports Treasury's initial view that the existing sector-specific arrangements for telecommunications should, subject to any necessary updates or amendments, continue to operate alongside the overarching economy-wide principles enshrined in law. It will be important though to ensure that regulatory duplication is avoided or minimised as it can give rise to uncertainty and harm incentives for investment. The role of the ACCC and the primary legislation should, in Pivotel's view, focus on what constitutes "scam", specify how and when code-making powers should be used (and to enable the ACCC to introduce sector – specific codes as a backstop), and to set out the broad principles that any sector-specific code should seek to address.

1.5 Pivotel also considers that a flexible and responsive regulatory framework which allows industry bodies and, if necessary, the ACCC to implement codes of conduct is appropriate to combat an issue such as scams where malicious actors look to exploit loopholes and vulnerabilities and frequently change their approach as new opportunities arise. Part IVB of the Competition and Consumer Act 2010 (CCA) has already proven to be a suitable place for industry codes of this nature and would likely be appropriate in this case too.

1.6 Pivotel agrees that Treasury would be best placed in commencing any initiatives to combat scam with those sectors where either the scams originate or the resulting harms eventuate. In that sense, the telecommunications sector, the digital platforms and the banking industry are a logical starting place. However, as set out above, the key differentiator there is an existing regulatory framework for combatting scams in the telecommunications sector and a regulator that has been diligently enforcing it of late.

[1] https://www.acma.gov.au/publications/2023-08/report/action-scams-spam-and-telemarketing-april-june-2023

1.7 In relation to the telecommunications industry more specifically, Pivotel considers that the broad principles of the Telco Anti-Scam Code are fit for purpose and broadly align with the proposals contained in the Consultation Paper. However, Pivotel considers that the Telco Anti-Scam Code may require amendment if contraventions are going to be subject to more severe penalties rather than the current framework which only provides for directions to comply at first instance.

1.8 One of the key concerns that Pivotel has regarding the Telco Anti-Scam Code is the effectiveness of the traceback notifications shared among C/CSPs, in accordance with 4.4 and 4.5, and 5.4 and 5.5 of the Telco Anti-Scam Code, and whether improvements to the traceback process may help to reduce the level of SCAM at the source. Of particular concern is whether the existing capabilities to detect, notify and traceback SCAM SMs arriving via grey routes or originating from SIM boxes, is effective.

1.9 It will be necessary to ensure that any reforms do not conflict with other obligations that carriers and carriage services providers have under the Telecommunications Act 1997 (the "**TA**"), or the Telecommunications Interception and Access Act 1979 (the "**TIA**"). For example, any information sharing or gathering obligations should not conflict with the obligations contained in Part 13 of the TA or the TIA.

1.10 Finally, Pivotel is conscious that there are a number of consultations underway which may affect or intersect with the outcomes that the Consultation Paper seeks to achieve. For example, draft legislation to reform interception and surveillance laws was expected to be published in late-2022, while in the wake of network outages that occurred last year, the Government has indicated that telecommunications providers will be directly regulated by the Security of Critical Infrastructure Act (rather than the existing sector-specific rules). Similarly, a sender-ID register is also being developed to prevent scammers from using alphanumeric sender IDs that emulate existing industry or government brand names. Pivotel considers that a holistic approach needs to be taken and that any robust industry code for the telco-sector will need to be consistent with these reforms.

2. ABOUT PIVOTEL

2.1 Pivotel operates a mobile and satellite telecommunications network as a Mobile Network Operator ("MNO") pursuant to a carrier licence issued by the Australian Communications and Media Authority in accordance with the *Telecommunications Act 1997* (Cth) ("**Telco Act**"). It has points of interconnect in the Australian major capital cities and points of interconnect internationally in Auckland, Los Angeles, and New York.

2.2 The Pivotel group comprises Pivotel Group Pty Limited and its wholly owned subsidiaries including but not limited to Pivotel Satellite Pty Limited, Pivotel Mobile Pty Limited and Pivotel Communications Pty Limited. For the purposes of this submission, they are referred to severally and collectively as "Pivotel".

2.3 Pivotel has demonstrated a willingness to invest in networks in regional and rural Australia and is active in most States. It also provides wholesale messaging services to its customers (including facilitating application-to-person SMS services).

2.4 Pivotel welcomes initiatives across the economy to combat scam. Pivotel is a participant in the working committee within Communications Alliance that prepared the Telco Anti-Scam Code and actively involved in various forums and committees to combat SCAM including in establishing and advising the ACMA on the SenderID registry.

2.5 Pivotel has also led the industry in developing filtering services to prevent scam calling and SMS. In addition, Pivotel has conducted proof-of-concept trial for a product called SecureSMS, which enables messages from organisations to be authenticated by

understanding the Call to Actions (CTAs) included in messages sent using pre-registered Sender IDs. Further details can be found in Pivotel's response to the ACMA Sender ID Registry consultation.

3. PROPOSED FRAMEWORK

3.1 Pivotel agrees in principle with the creation of a broad framework overseen by the ACCC with sector specific codes overseen by industry-specific regulators in consultation with industry bodies.

3.2 However, Pivotel considers that the new framework should not impose undue burdens on business and should leave the more prescriptive obligations to the sector-specific codes, which are developed in consultation with industry participants. Part IVB of the CCA contemplates industry codes that regulate the conduct of participants in an industry towards other participants in the industry or towards consumers in the industry. As such, the broad framework could build upon Part IVB of the CCA and set out:

- the circumstances in which the ACCC could request that a suitable authority introduce a new code for a specified sector, it could retain a backstop for itself if they are unable to do so (or as with the digital platforms, where the ACCC is best placed to do so). This would be similar to the powers the ACMA has under the Telco Act;

- specific sector code-making powers should be left to appropriate regulators with industry knowledge. For example, the Telco Anti-Scam Code should be brought under the remit of the ACMA, a banking code left to either ASIC or APRA and the digital platforms code to be prepared by the Digital Platforms Branch of the ACCC; and

- the criteria which an industry code would need to meet. This should largely reflect the ecosystem-wide obligations detailed in the Consultation Paper.

3.3 Pivotel does not consider that the statutory framework should contain mandatory obligations *for businesses* in designated sectors. This should be left to sector specific codes. Each sector has its own unique challenges and pre-existing compliance obligations (particularly, the telco and banking sectors which are already highly regulated). As an example, Pivotel would not be in favour of the ecosystem-wide obligations being as prescriptive as the News Media Bargaining Code (which is in any event specific to the news media sector).

3.4 In terms of whether the regulators proposed under the framework are appropriate, Pivotel accepts that, given the nature of APRA's mandate, ASIC is the appropriate regulator for a sector-specific code for the Banks. However, in relation to the digital communications platform sector (as currently proposed), Pivotel queries whether this would better sit with the ACCC – Digital Platform Branch rather than the ACMA. This is because of the considerable industry knowledge that the ACCC has built up over the course of the Digital Platforms Inquiry, the "Ad Tech" Inquiry, and the Digital Platforms Services Inquiry.

3.5 Pivotel also considers that consideration should be given to including transaction-based digital platforms (online marketplaces). According to Scamwatch in 2023, classified scams and online shopping scams totalled $14,612,070 in losses to consumers[2]. Similarly, investment scams in 2023 led to reported consumer losses of $275,923,066 (approximately 60% of all consumer losses reported by Scamwatch).

4. DEFINITIONS

[2] https://www.scamwatch.gov.au/research-and-resources/scam-statistics?scamid=21&date=2023

4.1 Pivotel agrees with the Consultation Paper that hacking, data breaches and identity theft should be treated as outside the scope of any Codes and dealt with by other means. By way of example, there are a number of legislative instruments that apply to carriers and carriage service providers which require identity verification before the C/CSP undertakes certain high-risk transactions (such as SIM swaps and number changes). However, there are certain types of fraudulent activity, which would commonly be thought of as a "scam" and which may blur the lines between fraud and a scam. For example, recent highly publicised 'invoice scams' where a hack leads to the falsifying of an invoice which is then received by email[3]. It will be important to ensure that these do not fall between the cracks.

4.2 Pivotel agrees with the definition of both "Telecommunications Provider" and a "Bank" as proposed in the Consultation Paper. It considers that it is important that any Industry Code applying to the Banks covers all authorised deposit taking institutions. Pivotel considers that the definition of digital communications platform appears targeted at the right types of businesses, however it queries whether the reference to a "*primary function*" may present challenges in the future depending on how these businesses are structured.

4.3 Pivotel's concern with defining the sectors captured by the Framework in the primary legislation is that these may evolve over time (for example, new types of digital platforms may emerge, particularly with advances in AI technology). Pivotel would recommend that these be left to the sector specific codes.

5. PRINCIPLES-BASED OBLIGATIONS

5.1 Pivotel broadly agrees with the proposed eco-system wide obligations, although as noted above it considers that rather than imposing such obligations on service providers, these should be used to define what the requirements are for a mandatory industry code. The obligations should then flow down into a sector-specific code.

5.2 Pivotel notes that the Telco Anti-Scam Code already contains many of the provisions recommended in the Consultation Paper. To that extent, Pivotel considers that the overarching obligations are already reflected in existing business objectives or requirements aimed at providing safe services for customers. For example, the Telco Anti-Scam Code already requires that C/CSPs:

- provide educational campaigns on their website;
- identify scam calls and SMs;
- not send calls which exhibit characteristics of scam traffic (such as where the caller doesn't have rights of use in the number, or the Caller Line Identification appears incorrect;
- monitor for scam calls;
- share information with other C/CSPs and the ACMA about alleged scam traffic;
- trace and block scam traffic; and
- report scam traffic to the ACMA on a quarterly basis.

[3] https://www.smh.com.au/national/the-mercedes-documents-were-identical-except-for-14-numbers-that-cost-georgina-38-500-20231207-p5epw3.html

5.3 Pivotel takes its obligations under the Telco Anti-Scam Code extremely seriously. It has a strong record of detecting, blocking and reporting scam traffic. Pivotel takes action to block numbers that are the source of scam and blocks entire routes from A2P SMS providers where it detects high levels of scam from a single source (while also working with its customers to help them identify and block scam traffic). It also provides information about scam prevention for its customers on its website.[4]

5.4 Pivotel considers that these existing obligations if, observed by carriers and CSPs, are sufficient to mitigate many of the harms of scam traffic and would duplicate many of the proposed ecosystem wide obligations listed in the Consultation Paper. This is why Pivotel considers that the burden of these obligations for C/CSPs (or digital platforms or banks) should primarily sit in the sector-specific codes to avoid regulatory duplication.

5.5 Technology and innovation should be at the heart of any initiatives to combat scam traffic (including any industry codes). Pivotel has led the way in developing filtering services to prevent scam calling. Pivotel first implemented its solution in March 2019. Investment in these solutions comes at a significant cost and remains an ongoing exercise as scams become more sophisticated.

5.6 However, Pivotel accepts that not all C/CSPs are of the same size and scale, and that for Pivotel its commitment to combatting scam is also a real differentiator in the market. As such, what may be a realistic anti-scam strategy or anti-scam system for one will not be for another. The costs of compliance should not be so great that it inhibits innovation (including in scam detection and prevention technology). Similarly, if businesses invest in a new anti-scam product or technology (which may come with considerable cost), they should not be required to migrate to an alternative product as soon as the latest technology is rolled out.

5.7 Pivotel agrees that C/CSPs should have a documented anti-scam strategy. Indeed, Pivotel sees an analogy with the approach in Europe with the GDPR where 'privacy by design' was introduced. As a consequence, when new means of processing personal data are introduced, privacy was put at their core. Pivotel queries whether a similar approach may be adopted in Australia in relation to scam – scam prevention by design. This would ensure that businesses in sector specific industries would at least consider scam prevention and detection when introducing new products. Pivotel is already developing a new product introduction process which will incorporate identifying scam risks and compliance into the product development and release process.

5.8 It will also be important that businesses domiciled overseas that provide services to Australian consumers are not able to avoid responsibility under any sector-specific industry codes. The Telco Anti-Scam Code currently captures all carriers and carriage service providers including those located overseas.

5.9 DITRCA held a consultation last year which considered whether a registration or licensing scheme for CSPs should be introduced. Pivotel considers that the introduction of a CSP register would bolster the effectiveness of the Telco Anti-Scam Code and minimise avoidance. At present, some providers of telecommunications services (including offshore providers) may be unaware that they are carriage service providers.

5.10 With regard to reporting obligations, Pivotel considers that C/CSPs should not be required to report to multiple regulatory bodies e.g. both the NASC and the ACMA. If C/CSPs are reporting instances of scam traffic on a quarterly basis to the ACMA as required by the Telco Anti-Scam Code, then the ACMA should have a better view of industry wide trends or

[4] https://www.pivotel.com.au/knowledge-base/security-account-safety/scam-call-guidance-faqs.html

organised large scale scam activity. As such it considers that the regulator which receives reports of scam activity should be responsible for broader industry reporting to the NASC.

6. ANTI-SCAM STRATEGY

6.1 Pivotel considers it reasonable that telecommunications providers, banks and digital communications platforms should be required to develop an anti-scam strategy and would agree that these should be approved at the highest level of the business.

6.2 If enhanced enforcement powers or pecuniary penalties for non-compliance are to be introduced as part of the code process, then it is important that industry participants are fully aware of the obligations and that this receives attention from the most senior levels within the organisation. Furthermore, given directors have obligations under the *Corporations Act 2001* to discharge their obligations with a reasonable degree of care and diligence, it seems appropriate that anti-scam measures should be discussed and understood at that level.

6.3 Pivotel would not support anti-scam strategies being made public in whole or in part. This is because, as foreshadowed by the Consultation Paper, scammers may use this to look for vulnerabilities and publication of high-level information would be of limited benefit to consumers. Instead, information about the code and the obligations on participants could be published by the relevant regulator.

6.4 Pivotel would suggest that industry participant's anti-scam strategies should be made available to the regulator upon request. Alternatively, if the regulator is to require that it be provided with a copy of the anti-scam strategy then Pivotel would not be opposed to a register being maintained by the service specific regulator identifying all industry participants that have submitted an anti-scam strategy. For the reasons discussed above, the register should not include details of the anti-scam strategy.

6.5 Pivotel does not consider that anti-scam strategies should be subject to a specified review period. Ultimately, it should be for industry participants to update their strategy as they deem appropriate or as their anti-scam measures evolve. Provided that the sector – specific codes address the economy-wide obligations outlined in the Consultation Paper and that the regulator has a power to request a copy of the anti-scam strategy upon request, then there would appear to be sufficient incentive for industry participants to maintain robust and current anti-scam measures without a legislated review date.

7. INFORMATION SHARING REQUIREMENTS

7.1 The existing Telco Anti-Scam Code already provides for information sharing. Currently, all carriers and carriage service providers have an obligation to alert the C/CSP that originated or transited the call or SMS where it identifies a "material issue" of alleged scam. A copy must also be provided to the ACMA.

7.2 The Consultation Paper states that: "*the NASC or other relevant regulators would be able to request that data on individual scam instances or reports, and actions taken in response, be shared*". Obviously, a degree of information sharing will be necessary in order for the mandatory industry codes to be effective. However, Pivotel considers that any information sharing obligations relating to potential scams will need to be carefully considered given the existing obligations under telco-specific legislation.

7.3 At present, Pivotel considers that carriage service providers would be constrained in the level of information that they could provide about individual messages. This is because of existing legislation such as Part 13 of the Telecommunications Act ("**TA**") and the Telecommunications (Interception and Access Act) 1979 ("**TIA**").

7.4 At a high level, both the TA and the TIA prevent interception, access and disclosure of the contents of communications unless an exception applies. Exceptions include where a warrant has been issued or where interception is required to protect the network. The TIA regulations allow a court to have regard to the impacts and the extent to which the act or thing is aimed at addressing malicious scam messages when deciding whether interception is reasonably necessary. However, this does not provide authorisation for a C/CSP to disclose the contents of a communication to a third party. Nor does this exception in the regulations enable scam detection for carriage services other than SMS. C/CSPs will be wary of information sharing, particularly in relation to individual messages, unless the legality of doing so is unequivocal.

7.5 While C/CSPs are permitted under the TIA to share the metadata of suspected scam messages voluntarily, this disclosure is limited to enforcement agencies where the C/CSP believes disclosure is reasonably necessary for enforcement of the criminal law and such disclosures cannot be instigated at the request of the enforcement agency. This may not cover the types of disclosures contemplated here.

7.6 The Consultation Paper proposes potential actions that C/CSPs could take following information sharing. Proposals include removing identified scam accounts from a service or blocking identified scam users from signing up to use the service. The current Telco Anti-Scam Code already provides for certain measures that C/CSPs can take in response to scam traffic. These include:

- taking action (as soon as possible) to block the Scam Calls (or SMs) being originated and/or carried over their network (unless the C/CSP forms a reasonable view the number has been spoofed).
- Originating CSPs should disconnect their own customer's service where scam calls are detected,
- all CSPs can block a number if they have a reasonable view that is sending scam calls or SMs

7.7 Pivotel considers that care would need to be taken if more onerous obligations to pre-emptively block users were to be introduced. This is because of the potential for CLI spoofing or overstamping, and the risk that innocent users could be blocked in circumstances where their number has been spoofed. These concerns are recognised in the existing Telco Anti-Scam Code (as noted above) and were also flagged by the ACMA when it revisited the Numbering Plan in 2022.[5]

7.8 As referred to at para 7.1 above, Pivotel considers that information sharing regarding scam traffic should be reported to C/CSPs that have originated or transited the service and to the regulator responsible for the sector specific code i.e. ACMA, and potentially to an enforcement agency, if these powers are made clear. Any additional reporting on trends or volumes should fall to the responsible regulator as the ACMA will be better placed to recognise these.

8. CONSUMER REPORTS, COMPLAINTS HANDLING AND DISPUTE RESOLUTION

8.1 Both telecommunications providers and digital communications platforms are used by scammers to get access to consumers. However, these sectors ultimately have limited visibility of a consumer's finances. Nor are they able to prevent consumers from dispersing funds to bad actors. Accordingly, Pivotel considers that it would be inefficient and

[5] Proposal to vary the Telecommunications Numbering Plan 2015 - Consultation paper pg.8

inappropriate for them to be held liable for compensating customers for any losses incurred as a result of interactions with scammers.

8.2 Any sanctions imposed on telecommunications or digital communications platform providers should be limited to enforcement action by the sector-specific regulator (and potentially by the ACCC) for a failure to comply with the obligations under the code.

8.3 While compensation (subject to a sensible cap) may be appropriate for certain types of regulated business, Pivotel considers that this should be limited to those businesses that have the ability to put in place controls over customer's access to and use of their funds.

8.4 It is also important to note that the responsibility for scam losses does not sit exclusively with the sectors proposed to be subject to the initial codes. All businesses within the economy bear some responsibility. For example, businesses with weak cyber security controls may enable hackers to subsequently initiate compelling scams.

8.5 Notwithstanding the above, Pivotel agrees that C/CSPs should provide a reporting mechanism for their customers to report potential scam traffic. This will support C/CSPs in addressing particular instances of scam or identifying emerging scam trends. This in turn would assist C/CSPs in undertaking their own reporting requirements detailed above.

9. SECTOR SPECIFIC CODES

9.1 For the reasons set out above, Pivotel supports- sector-specific obligations contained in mandatory industry codes as an appropriate measure to combat scam. Indeed, Pivotel considers that these sector-specific codes should contain the primary obligations to be imposed on the relevant sectors.

9.2 The current obligations contained in the Telco Anti-Scam Code are broadly fit for purpose but, as Pivotel has identified above, require certain improvements.

9.3 The proposed approach also raises broader questions about the status of the co-regulatory framework which has been a feature of telecommunications legislation in Australia for some time.

9.4 The Consultation Paper states:

"*...the telecommunications industry body, Communications Alliance, would be asked to review this code in 2024 and consider what changes are required to improve the operation of the Code and ensure consistency with the Framework. If changes are required, Communications Alliance would need to update the code and the ACMA would consider it for re-registration*".

Pivotel considers that industry bodies such as Communications Alliance will play a crucial role in the development of any industry code. However, Pivotel is also conscious that there have recently been questions raised by both the Telecommunications Industry Ombudsman and the ACMA regarding co-regulation vs direct regulation[6]. These questions have focussed on the TCP Code, which like any codes relating to scam prevention have customer protection at their core.

9.5 Pivotel considers that it is important that the future of co-regulation is secured if Comms Alliance is to have the core responsibility of drafting the Telco Anti-Scam Code. If Treasury has concerns about the benefits of co-regulation (notwithstanding that this forms part of the

[6] https://www.acma.gov.au/articles/2023-07/acma-puts-telco-industry-notice-improve-consumer-protections

regulatory policy contained in the TA[7]) then this should be resolved before industry bodies are asked to update or review the existing Telco Anti-Scam Code.

9.6 The sector-specific code (and any primary legislation) will also need to adopt a holistic and consistent approach. There is already considerable reform being implemented across the telecommunications industry, which will impact on anti-scam measures. These include:

- draft legislation to reform interception and surveillance laws which has been pending since late-2022;
- proposals to bring telecommunications providers within the ambit of the Security of Critical Infrastructure Act; and
- introduction of a sender-ID register to prevent scammers from using alphanumeric sender IDs that emulate existing industry or government brand names.

Any mandatory industry code for carriers and CSPs will need to consider these reforms in addition to the existing obligations on telco's in order to avoid regulatory duplication, excessive costs and inefficiency. For example, an anti-scam strategy could be incorporated into any future risk management programme that may be required under SOCI, while information sharing obligations are likely impacted by interception law reform (which could address the concerns we have raised in section 7 above).

10. OVERSIGHT, ENFORCEMENT AND NON-COMPLIANCE

10.1 Pivotel considers that principal oversight of sector specific code participants should probably sit with the regulator which has the best understanding of how that sector operates at a technical level. For C/CSPs this would be the ACMA. However, the ACCC should have powers that enable it to impose codes in circumstances where other regulators will not.

10.2 Pivotel considers that enforcement powers and civil penalties for sector-specific code contraventions should be consistent across all sectors. However, Pivotel does not consider that CSP's or digital communications platform providers should have liability to consumers to pay compensation for any losses incurred given they are unable to mitigate this risk and the harm ultimately occurs further down chain.

10.3 The Consultation Paper refers to penalties in the CCA being the greater of:

- $50 million;
- three times the value of the benefit obtained, or
- 30 per cent of the corporations adjusted turnover during the breach.

While this is true, these levels of penalties do not apply to all contraventions under the CCA. For example, s.76 of the CCA also provides that the penalty amount for a contravention of a civil penalty provision in an industry code should be the amount set out in the code itself. Pivotel considers that, for telecommunications providers, those penalties should not exceed the existing penalties under the TA, which already deal with serious contraventions such as a breach of carrier licence conditions or the service provider rules. To impose higher penalties in this instance would risk undermining existing business cases and harm investment in a crucial and fast-moving industry.

[7] Telecommunications Act 1997, s4.

10.4 Giving the sector-specific regulator the powers to enforce the relevant code, rather than the ACCC, would ensure that the concerns flagged in the Consultation Paper around multiple regulators taking simultaneous action for a breach would be avoided. The ACCC could have a power to recommend that the sector-specific regulator commence proceedings if it detects problems with a particular industry participant.