Department of Home Affairs submission to the Communications Alliance Reducing Scam Calls and Scam SMs Industry Code (C661:2022)

March 2022

1. Introduction

1.1 The Department of Home Affairs (the Department) welcomes the opportunity to make a submission to the Communications Alliance on the draft Reducing Scam Calls and Scam SMs Industry Code (the Code) which was released for comment on 9 February 2022.

1.2 The Department supports the development of the Code as a revision to build on the 2020 Reducing Scam Calls Code (C661:2020) (the 2020 Code) and extend efforts in the telecommunications industry to identify, trace and block scam calls and messages.

2. Impact of malicious scams

2.1 The Department notes the 2020 Code saw over 357 million scam calls blocked by industry in the first year of the 2020 Code's operation.

2.2 Notwithstanding this, scam calls and messages continue to have a significant impact on the Australian community. Reports to Scamwatch of scam calls and messages increased by 56 per cent in 2021 from 2020, and related financial losses were more than double those reported in 2020. In 211,000 of the 286,000 Scamwatch reports received in 2021, contact was made by phone or SMS and over $100 million was lost.

2.3 Malicious actors continue to use a range of methods to send harmful text messages at scale, with innovative and ever-changing approaches to trick victims into compromising their devices and data.

2.4 For example, the 'Flubot scam', which can cause malware to be downloaded onto the recipient's device, has shown how difficult it can be for individuals to identify whether a message is a scam or not, especially when scammers can spoof telephone numbers or make them appear to be sent from legitimate and trusted organisations.

2.5 The prevalence of scam messages also has the potential to strain the effective operation and maintenance of telecommunications systems. Scam messages can impact the effective operation of telecommunications systems by:

- placing an additional burden on industry
- impacting the delivery of telecommunications services
- causing harm to users of the system who click on the malicious links
- undermining public confidence in the telecommunications system, and
- causing a range of secondary harms, such as to legitimate communications.

3. Initiatives to combat malicious scams

3.1 As part of the Cyber Security Strategy 2020, the Government is committed to continuing to support the telecommunications industry to implement threat blocking technology to prevent the proliferation of scams over the telecommunications network and protect the public from malicious scams.

3.2 The Department values close collaboration between the telecommunications industry and law enforcement and national security agencies to prevent malicious scams and other criminal activity.

3.3 The Department welcomes the expansion of the Code to introduce obligations on the telecommunications industry to identify, trace, and block scam messages.

3.4 The inclusion of scam SMs in the Code complements the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021* (the Amendment Regulations), which were made on 25 November 2021.[1] The Amendment Regulations provide the telecommunications industry with confidence to deploy capabilities to detect and block malicious messages and protect their systems.

3.5 The Amendment Regulations specify matters that courts must have regard to in determining whether an act or thing done by a person for the purposes of identifying and blocking malicious scam messages was reasonably necessary for the operation and maintenance of the telecommunications systems.

3.6 The Department recommends that the Code highlight that carriers and carriage service providers (C/CSPs) should have regard to the operation and maintenance of telecommunication systems when undertaking threat blocking activities. It may be useful for the Code to include references to the *Telecommunications (Interception and Access) Act 1979* in addition to the *Telecommunications (Interception and Access) Regulations 2017*.

4. Caller Line Identification

4.1 Section 4.2 of the draft Code relates to improving Caller Line Identification (CLI) accuracy. The Department strongly supports CLI obligations being addressed in the Code. CLI accuracy is an important element of preventing scam calls and messages and is also critical for national security and law enforcement investigations.

4.2 In the absence of accurate CLI, national security and law enforcement agencies cannot easily identify the C/CSP responsible for the service number belonging to a target. This is especially pertinent to time-critical investigations, such as a threat to a person's life, where the inability or length of time taken to identify a C/CSP of a service number could have potentially disastrous consequences.

4.3 In addition, loss of the target's traffic and telecommunications data can also occur. This means that evidence which could otherwise be of importance to serious crime and national security investigations is not available.

4.4 It is imperative that the obligation on CSPs to maintain CLI accuracy is retained and extended to SMs, whether through the Code, or through other regulatory mechanisms. Failure to do so would impact the availability of lawfully accessed telecommunications interception data in an increasingly high-risk operational environment.

5. Conclusion

5.1 The Department will continue to work with the telecommunications industry to deploy threat blocking solutions at scale and thanks the Communications Alliance for its cooperation and constructive engagement.

---

[1] https://www.legislation.gov.au/Details/F2021L01622.