Australia and New Zealand's national identity and cyber support service

IDCARE's Submission

Industry Code DR C661:2022

Reducing Scam Calls and Scam SMS

IDCARE's Submission to the Industry Code DR C661:2022 Reducing Scam Calls and Scam SMS

Executive Summary

IDCARE congratulates the Communications Alliance on the release of the Reducing Scam Calls and Scam SMS Code (DR C661:2022). The revised code is a necessary development on the C661:2020 to better address concerns around the number of scam SMS being received by Australian consumers. As Australia's national identity and cyber support service, IDCARE is uniquely positioned to provide comment on the revised code as our charity assists thousands of Australians each year impacted by scam calls and texts. In IDCARE's formative years we strove to bring this issue to the industry's attention without much success. We are pleased now that efforts are being made at an industry level and with Government on an issue which only continues to escalate in causing harm to our community. What we as a country have done previously has been inadequate. What we must do requires different thinking and different approaches individually and collectively. We welcome the opportunity to provide comment and our submission will focus on the following areas:

- Prevention, awareness and response support for individuals impacted by scam calls and SMS;
- Reporting, notification and exchanging information of scam calls and SMS activity;
- Responding to incorrectly blocked numbers;
- Role of ACMA and the Australian Government in supporting assistance from International Operators; and
- Additional considerations for enhancing the Code's objective to disrupt scam activity.

About IDCARE

IDCARE was launched in 2014 by the Commonwealth Minister for Justice as a unique joint-public-private not-for-profit national support body for victims of identity crimes, scams and cybercrimes. As a registered Australian charity, our role is unique and not one that duplicates others, nationally or globally. We have responded to over 520,000 client engagements from members of the Australian community who have experienced cyber-enabled crimes either resulting in the compromise of personal and account information or their online misuse. The demand for our service continues to rise exponentially, with an increase of over 100,000 engagements in the last year alone. Despite this growth, our client satisfaction rating remains the strongest of any organisation in Australia (average 8.7 out of ten).

We believe the reason for this enduring community sentiment is because we have found the right mix of personalised, empathetic care with the provision of the most up-to-date pragmatic response advice aimed at reducing harm for each person tailored to their needs and concerns. Our frontline staff include qualified counsellors, social workers and computer scientists and we invest heavily in training them to become Identity & Cyber Security Case Managers to provide a human response to complex and diverse problems. Such a cohort exists nowhere else. These staff work as Case Managers to provide expert care when a person has responded to a scam call or text. They tailor personalised responses on how best to address immediate issues and concerns and build resilience to the inevitable risks of identity and account misuse that many of these crimes pose to our community. This is a free community service aimed at providing essential relief to those that now face very tangible risks within their online and offline environments.

Around a quarter of IDCARE's funding comes from the Commonwealth government for the delivery of additional services to the Commonwealth and the support of Commonwealth referred victims of these crimes. The remaining funding for our charity comes from delivering services to the private sector and State and Territory governments. This is then reinvested to provide the critical support to community members without charge as a charitable service through our Case Management and community education programs. Interestingly, only 1.7% of IDCARE's funding in the last financial year came from the telecommunications industry. This is despite around one in four community members presenting to IDCARE over the last three years because they had experienced a telephone or SMS scam.

The Practical Operation of the Draft Code

Addressing Section 3: Education Information about Scam Calls and Scam SMs

The volume of scam calls reported to IDCARE's National Case Management Centre since 2019 has increased by 188%. This situation isn't unique to IDCARE, with Scamwatch, Telstra and others also highlighting this growth. In 2019, telephone scams represented 15% of all IDCARE clients. In 2021, they accounted for to 27% of all client engagements to our charity across the Australian community. In the three-year period from 2019-2021, IDCARE provided help and support to over 10,000 Australians who had not only engaged with telephone and SMS scammers, but had also experienced other crimes being committed in their name as a result of the scam engagement, such as unauthorised account access and new account establishment across industry and government. This underpins the nature of this crime and the permeations felt by victims well after the initial call or text message across industries and sectors and not just within the confines of the telecommunications industry.

The draft Code highlights the necessity for Carriers and CSPs to make up-to-date guidance material on scam calls and Scam SMS. The draft Code at *3.1.1 d* states *the actions that customers should take if they find they have received Scam Calls or Scam SMs such as reporting the scam to www.scamwatch.gov.au*

The draft Code omits a recommendation to include the role of support organisations, like IDCARE.org, following scam events. While most Carriers and CSPs are aware of IDCARE, provisioning of information about Government reporting channels and omitting joint industry-government supporting capabilities, such as IDCARE, is a deficiency of the current draft. When some community members lose their entire life savings to these scammers, completing online forms for Government is not likely to address the very real pragmatic and emotional needs they have.

Recommendation 1: Emphasise in the awareness campaign that people impacted by scam calls and texts can contact IDCARE and other support services.

Addressing Section 4.2: The Problem with Spoofing

The draft code makes various recommendations to address the problem of CLI Spoofing. This is timely as complaints about CLI spoofing of A-Party CLI reported to IDCARE increased by 63% in the year 2021 when compared to 2020. The introduction of methods to block or limit the spoofing of 13, 1300 and 1800 numbers by ACMA in March 2020 resulted in scammers quickly changing their methodology to spoof Australian mobile phone numbers and landlines numbers. This created multiple victims – the person who engaged with the scammer and the person whose number was spoofed as they were being contacted by people assuming they were a scammer.

IDCARE applauds the measures to improve CLI accuracy as detailed in 4.2 as necessary - albeit perhaps onerous for Carriers and CSPs - to limit the impact of spoofing in the Australian context. Currently, measures addressing A-party spoofing vary between carriers and CSPs. A standard protocol would be welcomed as well recognising the need to support impacted victims of spoofed numbers (i.e. the account holders). Support in this context could include Carriers and CSPs offering to arrange temporary messaging services for spoofed number account holders to limit the calls received from individuals that believe they are calling a scammer and filtering those who are attempting to call the actual account owner. Many victims of CLI Spoofing to engage IDCARE seek immediate and practical support to limit the reputational damage they suffer. Enhancing

online content and awareness raising materials about recognising that a number is spoofed and what to do if you suspect your number is spoofed would be an invaluable addition for consumers with the Code.

Recommendation 2: That the draft Code include a requirement for Carriers and CSPs to standardise their response methods for clients experiencing A-party spoofing that can be shared as part of the education and awareness campaign.

Recommendation 3: That the draft Code include a specific requirement for Carriers and CSPs to offer additional support, such as call filtering, for victims of CLI Spoofing that is timely.

Section 4.4: Exchanging information about alleged Scam Calls

IDCARE welcomes the measures to exchange information about alleged scam calls between Carriers and CSPs along with ACMA. However, the absence of a need for broader information sharing to industries, such as the banking sector, highlights a need for greater appreciation of the problem. Those who scam via calls and SMS are mostly after identity credentials, account login details, and money. The Carriers and CSPs are one means to an end with this criminal activity. The Code must recognise the need to share information with a broader audience of financial crime prevention and response professionals. Without doing this, the proposed sharing will have limited effect in reducing the overall impacts of these crimes on the Australian community. As an extension, the scam call or SMS pre-text as it relates to an existing entity, such as an impersonated government or private sector entity, should be a mandatory inclusion in relation to this sharing provision.

Recommendation 4: Expand the sharing provisions within the draft Code to include directly impacted stakeholders, such as those likely to confront risks of harm through reputational and financial impacts.

Section 4.6: Blocking Scam Calls

The usefulness of blocking scam calls can be considered in the context of Telstra's Cleaner Pipes Initiative which has reportedly resulted in up to 13 million calls blocked a month, yet the number of people being impacted by scams continues to increase. An important consideration around blocking scam calls is the impact this can have when a number is incorrectly identified as a scam number. IDCARE experienced this issue in 2021 where our 1800 number was incorrectly marked as a "possible scam number". Crucial to the success of valued campaigns to block scam calls is the ability to quickly recognise and correct mistakes. This will also be essential for clients whose numbers have been incorrectly identified as scam numbers due to CLI spoofing. Without proper timeframes for redress, these clients will be further victimised. A timeframe for redress needs to be included to give context to the wording in 4.7.2 "as soon as practicable'.

Recommendation 5: Introduce clear measures on how to unblock a number which has been incorrectly identified as a scam call within a recognised short (48-hour) timeframe.

Section 4.8 Seeking assistance from International Operators

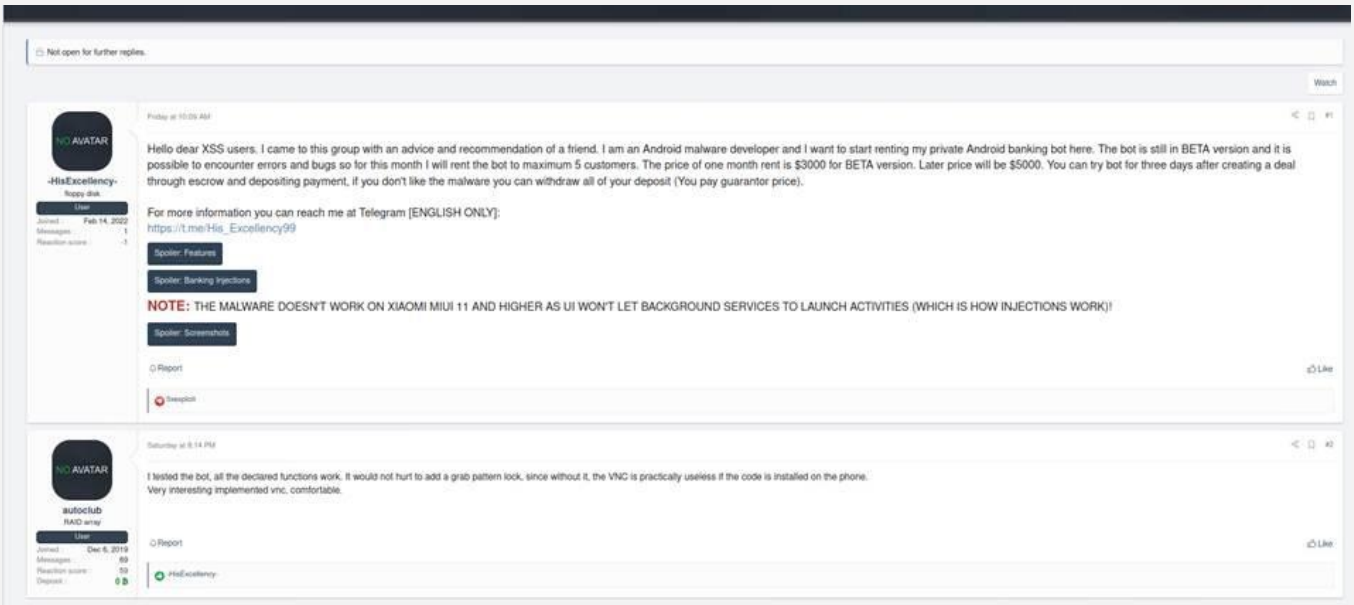
The internationalisation of the scam problem does mean that offshore telephony and voice providers are likely to place an increasing role in supporting campaigns that target the Australian community. The Code does reference the need for Carriers and CSPs to use all available contractual arrangements to secure the assistance of the relevant international operator. IDCARE would prefer to see that ACMA or a related

Government entity also have this as a shared responsibility under the Code. Whilst the nature of the Code is to guide the practice of Carriers and CSPs, the increasing number of regulatory reporting requirements placed on industry to inform Government must also extend to better understanding the value of such disclosures. For example, the disclosure of breach data to the Privacy Commissioner does not create any real value to impacted persons of a breach. In this context, IDCARE does believe there is a shared role and responsibility for Government to also use its levers with counterparts in foreign jurisdictions to assist the industry in the efforts in gaining assistance from International Operators. Simply stating that a report is to be made to ACMA or another Government entity is not a sufficient proposition.

Recommendation 6: An inclusion is made under Section 4.8 that explicitly references assistance that can be provided by ACMA (or other relevant Government agencies) to escalate via Government-to-Government relations where cooperation is not forthcoming between operators.

Section 5: Scam SMS

The Code is limited in addressing the most prolific forms of SMS exploitation over the last 12 months. From August 2021, FluBot has impacted millions of Android users. Whilst the initial deployment of the virus and its variants may present in a manner that is addressed via the scam SMS provisions, the actual promulgation of the virus has included variants where the contact list of account holders is targeted in the name of the account holder. Not as a Caller ID spoof in terms of scam calls, but virus laden SMS text messages from innocent (and victimised) account holders. Given the effectiveness of the FluBot campaign, it is anticipated that similar targeted malware attacks will continue to be developed. Indeed, this is already evident, with IDCARE analysts noting in March 2022 a thread on 'XSS.IS" by forum member 'HisExcellency" who claimed to be a malware developer who had designed a trojan named "Escobar" capable of overlaying banking applications on infected android devices akin to variants of the FluBot. Escobar would be spread via an SMS phishing campaign which would then have the ability to access a device's contact list and spread the malware even further.



While the recommendations in the draft Code are needed, IDCARE is concerned about the ability to counteract the threat of these types of malware attacks where it combines Caller ID spoofing with SMS-based

malware deployment. As these attacks are spread quickly by accessing contact lists, it is not obvious how the measures in the draft Code will address this type of threat, least of which would be to remedy and support impacted numbers that innocently promulgate such viruses.

Recommendation 7: Measures to block SMS need to be considered in the rapidly evolving space of cybercrime where criminals are likely to quickly develop schemes to circumnavigate and create new threats.

Section 6: Reporting

Reporting is a regulatory tool that is increasingly popular amongst policy makers. However, the actual effectiveness and market visibility of reporting has had mixed results. IDCARE believes that to be effective, ACMA should publish publicly the Carriers and CSPs that host scam numbers each month. From IDCARE's ongoing analysis of scam number hosting, we typically do not see market share by Carriers and CSP being representative of scam number hosting. Consistently we see entities that offer exclusive VoIP service providers featuring much more prominently. Public disclosure each month of the entities that host scam numbers would create within the market necessary incentives to more effectively detect and address these occurrences. This should include average times to detect and respond. Simply reporting to a regulator without public visibility will provide little incentive to motivate positive change. In some cases, IDCARE has reported to Carriers and CSPs scam numbers that took some eighteen months to remedy. In the interim many Australians lost thousands of dollars. If such reporting on timeframes were publicly disclosed, in addition to the responsible Carrier and CSP, it is likely that the time taken to respond would have been a lot less and many hundreds of Australians would likely have not been exposed to that number exploited by the scammers.

Recommendation 8: Under the Reporting provision an inclusion of public disclosure by ACMA of the named Carriers and CSPs that have hosted a scam number each month and the average time taken to detect and respond.

Concluding remarks

The introduction of a revised Industry Code for Reducing Scam Calls and Scam SMs is necessary in the current environment where the public is expecting action from Government and Industry to curtail this pervasive threat. However, the difficulty in drafting a Code is that the fluid and adaptable nature of the scam environment constantly sees corrective measures fall short of new advancements by the time they are officially introduced. This is a problem that cannot be easily overcome. The inclusion of Education Information in all Carrier and CSPs websites and the provision of up-to-date guidance is one measure to mitigate this risk. However, there are also a number of measures that the telecommunications industry could put in place to reduce the impact of Scam Calls and Scam SMS. The IDCARE submission makes a number of recommendations that are focused on prevention and reduction of harm to the individual consumer and reduce the success rate of scammers. These would be a welcome inclusion in the draft Industry Code.