Comments on Communications Alliance's Proposal for Reducing Scam Calls (Industry Code DR C661:2020 issued 24th March 2020)

Submitted by:

mobileum

Action driven by intelligence

Document Version: 20200508_AUS_CA_RFC_01

Date: May 8th, 2020

1. Summary

Mobileum is a well-recognized and respected name in the telecommunications industry for the last two decades, and its products and services are used in over 150 countries by 700+ mobile, fixed, and cable networks. Mobileum specializes in Roaming, Security, Fraud, Revenue Assurance, Risk management, and its solutions are built around actionable analytics that leverage artificial intelligence and machine learning at the core.

Mobileum is pleased to be a member of Communications Alliance in Australia. With reference to the recent Industry Code *DR C661:2020 REDUCING SCAM CALLS*, issued 24th March 2020, Mobileum would like to contribute the following comments.

Preamble

Detecting scam calls, especially those where the CLI has been spoofed, is not easy. In fact, there cannot be any solution that is able to provide hundred percent coverage or accuracy, and hence bring enough confidence in blocking **all** calls. However, it is possible to develop solutions that reduce the number and area of *attack surfaces*, thereby making it difficult for the stray, or should we say, well-spoofed, call to get through. In our global experience, while it is possible to block specific numbers (the premium rate numbers used for IRSF and Wangiri fraud) from making or receiving a call, this often creates a problem where the CLI actually belongs to a genuine business or consumer, and has been spoofed for Robocalling (typically one-way campaigns) or malicious purposes (ransom, access to services, impersonation, etc.). Hence, apart from blocking premium rate numbers, the industry should *leverage modern available techniques that correlate and cross-examine evidence, using analytics at the core*, in order to evaluate if the CLI presented in the context of a specific call, is genuine or potentially spoofed.

Comments on the document

Cross-Reference #	Comments
4.1.1.c (ii)	There can be cases where the CND is genuinely blocked due to privacy reasons.
4.1.1.c (iv)	It is possible for an inbound international call to contain an Australian CLI. Two cases are: 1. An Australian out-roamer, in a foreign country makes a call to another Australian number. 2. An Australian out-roamer received an incoming call from another Australian number, but a Late Call Forwarding condition resulted in the call coming back into Australia.
4.3.1 (b)	This should also consider in-roamers. In-roaming traffic is due to a commercial relationship and the serving operator has no idea if the CLI, when a call is made, is genuine. Australian operators should further try and inspect the MAP/Diameter/CAMEL signaling messages coming from abroad, especially those that are trying to manipulate CLI. Mobileum can provide additional technical details based on its experience.
4.3.3	This does not consider the case of roaming. For example, if an Australian out-roamer in Singapore makes a call to an Indonesia number, and it is transited via an Australian carrier, they will be in violation of 4.3.3

	as currently stated. Further, the C/CSP may be satisfied if it is only required too know that the A# is roaming, but still may not be able to verify if the CLI presented in the call is genuine, or if the A# belongs to other local operator, the transiting carrier may not even know if A# is roaming. Mobileum proposes that there be a mechanism between Australian CSPs that enables lookups. Mobileum would be happy to discuss the technical details separately.
4.3.5	In an international scenario, it may not be possible to accurately identify the originating C/CSP.
4.3.6	Some countries send the call to the B-Party. However, they change the CLI to something like +111 (to indicate to the user that the call came in on the international interconnect), and/or add SIP DISPLAY INFO or CNAM to indicate something like "SCAM LIKELY". Mobileum would highly recommend that Comms Alliance considers something like this instead of dropping the call.
4.3.7	This section can be further strengthened by adding that Australian CSPs that provide SIP Trunking services should closely monitor the CLI used by their customer, and block originating calls with a non-Australian CLI, unless there exists a prior written agreement for use of an international CLI.
4.4.2	Mobileum recommends that apart from the CLI, the Australian operators also monitor the Redirecting number or Diversion number.
4.6.1	If a Robo-caller has spoofed the CLI of a genuine business or subscriber, then this clause, along with 4.6.4 will result in a lot of changes (additions/deletions) and will make the process unwieldy. Modern techniques of analyzing SIP Calls may be used to identify spoofed CLI and use that in the decision-making process to block a *CLI in the context of a call*, instead of all calls.
4.6.3	Similar comments as in 4.6.1
4.7.1	Robo-callers can spoof genuine international number. Indiscriminate blocking of all such false positive numbers will lead to denial of service issues and B-party's loss of confidence in their service CSP.
4.7.4	While the CSP can retain the option of temporarily blocking an international operator, in our experience this usually causes the scam calls to move to another international operator. We recommend that this be used as a last resort, with the focus being working with the carrier to identify the source of and blocking the scam CLI in the context of the call.
4.7.6	Refer to comments in 4.7.4. A Robo-caller who is intent on disrupting communication in Australia, may spoof genuine numbering ranges.

For further information,

Shankar Maniraj (shankar.maniraj@mobileum.com) / 0458 256 627

---- End of Document ---

Mobileum, Inc.

mobileum
Action driven by intelligence

20813 Stevens Creek Boulevard
Suite 200, Cupertino, CA 95014
United States of America

Phone: +1 (408) 8446600
Fax: +1 (408) 252 1566

www.mobileum.com