Industry Code Scam calls

Submission by
Vodafone Hutchison Australia

May 2020

~~This document is classified as | C1 - Public~~
This document is classified as | C1 - Public

Formatted: Font color: Black
Formatted: Font color: Green

Introduction

Vodafone Hutchison Australia (VHA) welcomes the opportunity to provide comment on the Industry Code: Scam Calls.

VHA has put considerable effort into identifying fraud and scam activity and has put in place various arrangements to protect consumers, because it is the right thing to do. VHA is one of the strongest driver of this capability across mobile carriage service providers and as a global communications service provider the Vodafone group has an international approach to acting to protect consumers and minimise the impact of scams.

VHA has taken a firm stand in implementing a range of actions to minimise the impacts of scams We already monitor for scam calls and SMS .

Vodafone provides online support and information for our customers regarding the latest scams (https://www.vodafone.com.au/support/notify/scams), which is updated on a regular basis and includes steps customers can take to mitigate risk.

On our main website www.vodafone.com.au – in the support tab both 'Fraud' and 'Scams' is included ono the support dropdown options (for both Personal & Business Tabs)

VHA welcome the introduction of the Industry Code to ensure that consumers of all carriage service providers are protected from scams, to the extent possible.

Preliminary comment on content of the Industry Code

The Code is a good first draft to limit the impacts of scams. Much of the content is fit for purpose in providing protection to consumers and it provides a level of detail that ensures that there is limited opportunity for solutions that could otherwise continue to allow scams.

There are some business factors that need consideration why alternate CLI is used in some call cases.

For example, VHA has been made aware as part of our investigations into potential scam traffic that some VOIP service providers use a single geographic number for calls from their VOIP outbound only call. These outbound call services, may be either from their care staff to another department, which may traverse another network, or for outbound calls, such as calls to customers. Essentially, they are over-stamping geographic numbers for calls. Where the over-stamped geographic numbers for the call is handed off to another networks and the CLI is marked as non-display to prevent return calls. As such, this number is a floating number, used on various calls and not dedicated to one end-user.

Formatted: Font color: Black

Formatted: Font color: Green

These calls are valid call cases and the Code should recognise this use of numbers. For example, in 3.1.1 an additional item could be added as (xi) to the effect that: allow unknown calls to go to Voicemail and then listen to any message left to ascertain if this might be a genuine call.

Final call out is around 3rd party applications – Viber, WhatsApp, WeChat etc... where we are notified by our customers of scams.

VHA understands that the Code does not answer the question of how we deal with these, as they are derived from apps, however, from a consumer point of view VHA believe that our customers would expect there would be an agreed approach to scams from these sources.

Following are a few matters that require some minor change:

Comment on the content of the Industry Code

3 Consumer Information.

VHA supports the obligation as we already provide online support and information regarding latest scams (https://www.vodafone.com.au/support/notify/scams) which is updated on a regular basis (includes steps customers can take to mitigate risk).

On our main website www.vodafone.com.au – in the support tab both 'Fraud' and 'Scams' has added to the support dropdown options (for both Personal & Business Tabs),

To improve this section VHA suggests the following:

3.1.1 (c) add (xi) as noted above (i.e. to the effect that: allow unknown calls to go to Voicemail and then listen to any message left to ascertain if this might be a genuine call).

3.1.1 (d) As SMS typically includes a sender name, in lieu of a number, VHA suggests changing this clause to: not responding to SMS from an unknown source..

4 Scam Calls

Vodafone has sound criteria for identifying scam calls which align with section 4.1, which we support, however note previous comment re high volume use of some numbers. A note to the effect that high volume calls is not primary evidence that the calls originating from an individual number are scam calls would be helpful under 4.1.1 (a) and 4.2.1 (a).

4.3 Improving CLI accuracy

Formatted: Font color: Black

Formatted: Font color: Green

Improving CLI accuracy needs further technical review.

4.3.1 Needs to allow for the inclusion of originating calls from CLI that are from inbound international (e.g. Vodafone UK customer using Vodafone Australia network) or domestic roaming on that network (e.g. Vodafone customer roaming on Optus). VHA suggest adding:

> (d) allocated to an entity the Originating C/CSP has a domestic or international roaming agreement with.

4.3.3 While VHA understands the intent, the obligation is impractical. VHA does not understand how we can satisfy ourselves that an Australian CLI coming from overseas is a genuine call case vs. a scam call. There is presently no mechanism to distinguish genuine call cases from scams.

Even supposing we have some system to check these calls as genuine, we are not sure how we would know if say a Telstra roamer overseas is calling our customer (or we transit the call to another networks customer), or if the call is from a fraudster spoofing that number and calling our customer (or transit to another networks customer)? If a call was from a PSTN number to a roamer overseas who later call forwarded the call to an Australian mobile number and if ISUP routing was used, the redirection number would be lost (not supported in ISUP v1) making the call appear to come from overseas with an Australian PTSN.

CLIR is not mentioned in the code. Is CLIR going to be allowed or not? If we receive a call with presentation restricted but with CLI present the customer wouldn't see the CLI. People might spoof a legitimate number in E.164 format with presentation restricted leaving the customer with no CLI. We cannot tell from the Code if we should allow these calls, or not .

4.4 Monitoring for Scam Calls

VHA supports the obligations in 4.4

VHA currently works in parallel with our Partners in relation to the monitoring of outbound international calls and has proactive blocking arrangements in place for suspect numbers and ranges that have been identified as spam/scam calls.

VHA also utilises internal reporting to monitor for suspect scam calls domestically both incoming and outgoing.

4.5 Tracing Scam Calls

VHA supports this obligation, however we note that we often face difficulties with smaller VOIP providers use of numbers (refer to overstamping noted above) and customers have ongoing concerns about calls

Formatted: Font color: Black
Formatted: Font color: Green

made via Third Party Apps such as Viber & Whats App. We understand why these have not been included, but suggest comment be made somewhere in the Code about why the Code does not address apps.

4.6 Blocking Scam Calls

VHA supports these obligations and currently has monitoring in place where alerts are generated and sent for action. If the alerts are out of hours, they are actioned on the next business day. We review the number ranges and take a hard-line approach to blocking them in our network for both inbound & outbound calls. We are typically placing the block at the level of the last 4 or 5 digits of the number range. We also take action against any services used on our network found to be generating scam calls.

4.6.3 It should be noted that many SCAM calls use spoofed numbers. If we are compelled to block calls to a number that was spoofed we may be blocking the real owner of that number from being able to receive calls even though they didn't originate the scam call. We are also blocking the real owner of the number from sending calls into our network. Processes need to be in place to quickly remove a block that would impact a genuine customer. While 4.6.4 has inclusion of a requirement to unblock a number 'incorrectly blocked' there is no helpful information to say what 'incorrectly blocked' means.

VHA suggest the addition of a note box to mention that 'incorrectly blocked means blocking of a number as a result of transposition, and/or blocking the number of a customer, affecting their ability to use the service. Alternately, VHA suggest addition of a new 4.6.5 to the effect that: Where a Public Number is found to be blocked affecting the use of a service by the Customer, a C/CSP must take action to unblock the Public Number as soon as practicable.

4.6.4 The obligation in this clause results in a game of whack-a-mole. If we identify a scam number and block it the perpetrators will immediately move to another number. This blocking is already happening today on VHA and most days there is a new list of numbers that our fraud team block incoming and outgoing calls, attached is the past week of requests. VHA suggests inclusion of guidance on how long a number is to be left blocked and not used for scam calls before unblocking and especially noting the potential impact on Public Numbers that are presently in use by a Customer, or may be in the process of being Issued to a Customer.

4.7 Blocking calls from International Operators

VHA currently works in parallel with partners in monitoring inbound international calls and proactively block suspect numbers and ranges that have been identified as spam/scam calls

VHA also proactively monitor through internal reporting for suspect scam calls domestically both incoming and outgoing.

Formatted: Font color: Black

Formatted: Font color: Green

However, VHA, like most C/CSP's, has partner companies that we interconnect with that aren't subject to Australian law. Whilst most C/CSPs both here and overseas are already taking action to mitigate scam communications, given most scam calls come in from overseas and we cannot compel all partners to follow this Code, its obligations may be of little value other than as window dressing.

4.7.2 Requires that the C/CSP must block CLI identified as scam calls. If any C/CSP is blocking the CLI used in the scam calls, as required, the perpetrators will likely move to use another CLI , so there wouldn't be any traffic from that CLI as its already been left unusable to the perpetrators. If there was further traffic its already been blocked by the C/CSP who first receives it from overseas carrier. Either way the CLI isn't able to terminate a call. 4.7.1, 4.7.3 thru 4.7.8 requires us to threaten our interconnect partners with being blocked and then block them if they don't prevent the calls arriving which the C/CSP' are already required to block. If the already issue is solved by 4.7.2, why is there a need to try to fix it again ? Blocking interconnect partners could be detrimental to our business as it would cause our partners increased costs to terminate via another way, or create a loss in revenue if they can't carry traffic. This would likely lead to a souring of a relationship that we depend on for low cost IDD. Our partners in most cases aren't directly connected to the originating source and are just transiting traffic.

5 C/CSP Contact List

VHA will separately supply details of the Vodafone Technical Fraud Team

Formatted: Font color: Black

Formatted: Font color: Green