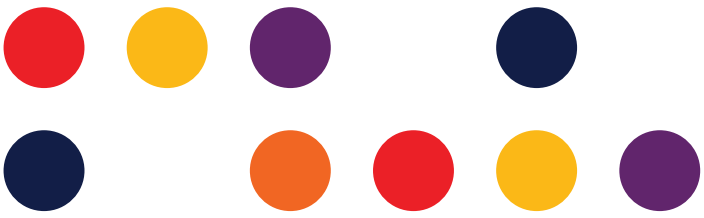
DR C661:2022 Reducing Scam Calls and Scam SMS

Response to request for public comment

March 11, 2022

Confidential



vodafone TPG iinet Internode LEBARA AAPT felix

TPG Telecom Limited ABN 76 096 304 620 Level 1, 177 Pacific Highway, North Sydney, NSW 2060

Introduction and key issues

Thank you for the opportunity to provide the views of TPG in relation to the draft Industry Code DR C661:2022 Reducing Scam Calls and Scam SMS (the draft Code). We have contributed to the development of the draft Code and its associated guideline.

We recognise the significant impact of scams utilising telecommunication services on our customers and the Australian community. We dedicate significant time, resources, and staff to engage with partners, industry, and regulatory and policy agencies to address scam and fraudulent activity associated with telecommunication services.

This includes information sharing activities with other industry sector groups, such as the finance sector and with government agencies to keep abreast of the latest scam activity and to mitigate its impact through enhancements to our processes and systems. The controls we have in place are under constant review to ensure we are on top of the latest variants of scam communications.

We appreciate the opportunity to continue to contribute to productive discussions on improvements that can be made to protect consumers.

We wish to take this opportunity to reaffirm our strongly held views on two issues in the current draft, notably:

- Our support for Option 1: issued to the A-Party caller by the Originating C/CSP under sub clauses 4.2.1 and 5.2.1 (e).
- Our support for the adoption of the Verified Origin Registry solution for alpha-numeric scam SMS

We also have additional ad-hoc drafting comments.

Use of Issued numbers

Cl 4.2.1 Improving CLI accuracy and cl 5.2.1 Improving Public Number and Alphanumeric Sender ID accuracy

We wish to raise concerns about any approach taken that allows calls and SMS to originate from a CSP other than the CSP that issued a number to the customer. On the drafting note for clauses 4.2.1(e) and 5.2.1(e), TPG Telecom supports *Option 1: issued to the A-Party caller by the Originating C/CSP*.

The are several impacts if the alternative approach proposed by *Option 2: issued to the A-Party caller by any C/CSP* was included in the Code.

Unless the industry maintains current expected regulatory arrangements, it will not be possible to ensure that scam traffic is blocked, as in this alternate model any number could use any network.

Current practice

As we have discussed in industry meetings, the industry should not see originating traffic from a CSP that does not have those numbers held by them via ACMA allocation, transfer, or number portability. This is a generally accepted practice and the foundation upon which telecommunications have operated for many years that:

- a number is allocated to a CSP by the ACMA;
- the CSP will arrange that number block to be conditioned on a particular carrier's network (it may or may not be a network they operate);
- the CSP may issue a number from that number block to a customer;
- the CSP may transfer a number block to another CSP via the ACMA numbering portal or may transfer individual numbers or blocks of numbers to another CSP via a commercial arrangement*, or may Surrender the number block if unused;
- the CSP may also transfer numbers via a commercial arrangement that may include the whole number block or a portion thereof to another CSP;
- usage data is retained by the CSP and associated carrier of communications made. Interception is arranged based on information available to investigation and enforcement agencies via the Integrated Public Number Database and the ACMA numbering portal and porting records.

* a number transferred to another CSP under a commercial arrangement will still be conditioned for use on a particular network.

For the customer this means:

- a number is issued to them by a CSP, who is the holder of that number;
- upon being Issued a number by the CSP, the customer then has ongoing rights of use of that number on the network used by the CSP that issued the number (Note: this has never meant the customer has free unfettered use of this number on any other network);

- if the customer chooses to port the number, calls to that number will be via the network associated with that CSP and identified accordingly in porting data.

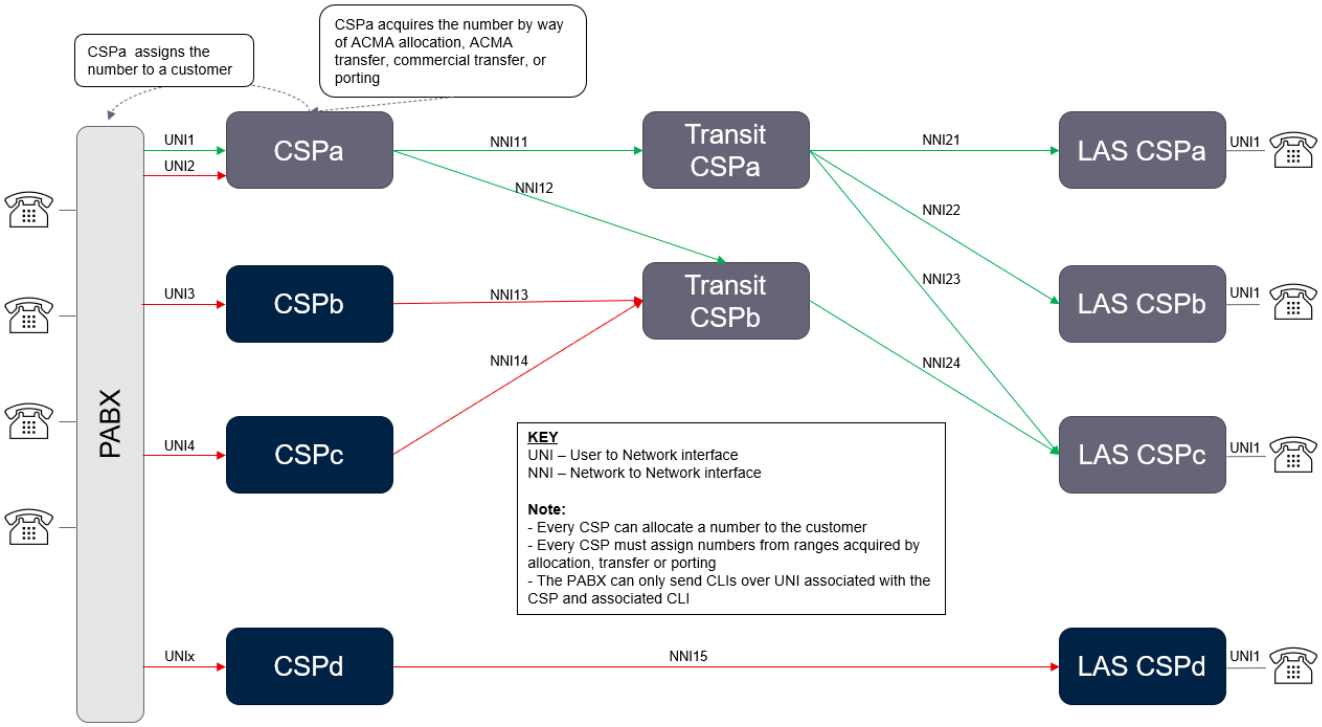
For the CSP:

- a number that is conditioned to be used on a particular network is issued to the customer;
- the number and the associated customer and service information is loaded into the Integrated Public Number Database (IPND);
- for certain categories of numbers, they may be subject to an Annual Number Charge payable by the CSP holding that number.

For enforcement and other agencies

- agencies can look up a number in the IPND and access data for that number and ask the CSP for additional data associated with the service and may ask for interception of communications to and from this number on the network associated with the number.

TPG Telecom submits that to stop scam traffic, traffic from a number held by a CSP - either by way of ACMA allocation, ACMA transfer, commercial transfer, or by porting - must only originate from the relevant network associated with the CSP that holds the number. Below is a diagram for clarity that there is no impact on transit providers nor is there a competition issue, as every CSP can supply services to the same customer.



If the current regulated approach is to be broken to allow customer free choice of network for a particular communication, investigation and enforcement agencies will never know who to approach for call and other communications data and to apply interception. CLI accuracy will

be seriously impacted as a CLI cannot be trusted to be the actual CLI of that communication and its authenticity cannot be verified.

If a CSP wants to supply service to customers, they should do so through their own numbers conditioned on a single network.

Impact of Option 2

The current expected approach has served both customers and the industry well for many years. The approach in Option 2 will facilitate will result in suppliers taking commercial advantage of the CSP that holds the number without meeting any associated regulatory burdens - for example, the costs associated with Annual Numbering Charges and the provision of assistance to enforcement agencies.

There is an argument from some service providers that unwinding these longstanding arrangements is necessary for competition. The issue is misrepresented as an issue of choice for the customer and competition, particularly affecting transit service providers. The approach of making the originating network responsible for identifying whether the customer has a right of use of that number when other CSPs have nothing with which to validate that the customer will ensure the continuation of number spoofing and allow calls to originate on any network.

There are very clear engineering and network management arrangements that must be in place to block number spoofing and scams.

This ‘trust’ approach is already causing a very significant issue with a CSP using another CSP’s numbers, creating an inability to identify CLI spoofing unless traffic originates from the expected source. We see this today where significant traffic is being originated on other networks using numbers held by TPG Telecom brands.

As evidenced by regulation in Europe[1] (see the table below), in order to stop CLI spoofing and scams TPG Telecom believes the only way to achieve an outcome to significantly reduce scam calls and SMS is to have an approach that requires calls to be blocked unless they originate from the expected network. If a number is allocated or ported to Vodafone it should only originate from Vodafone, not on a different mobile network, or from a fixed network.

Country	Solution
Belgium	BIPT published new CLI guidelines in 2020: > each call has to be associated with a network number; > network number identifies the calling connection (of an individual or an organisation) in a unique manner > the presentation number has to be dialable; and > the network and presentation numbers have to be valid. A blacklist has been developed of certain geographical numbers (e.g. from banks) that are sensitive to CLI spoofing.

[1] Draft EEC Report 338 (2021)

France	ARCEP has taken a multipronged approach: > banning the use of premium-rate numbers (starting in France by 089) as a CLI. > routing can be blocked for calls or messages with a French geographic or non-geographic number received through an international interconnection (outside the EU); > mobile, geographic, and fixed non-geographic numbers cannot be used as a CLI for calls or messages sent from automated systems (national and international). A dedicated numbering range is available for calls and messages from automated systems; > phone number used as a CLI must be a part of a range assigned by ARCEP; > banning the sub-assignment of new numbers for non-geographic and mobile numbers from 1 August 2018. This will extend to geographic numbers on 1 January 2023.
Germany	Changes to the German Telecommunications Act in December 2021: > if the CLI is a German number using a foreign network, the number (except for mobile numbers) must not be displayed and the path of ingress of the call into the German network must be identified; > obligations for disconnecting calls from "forbidden" numbers (including emergency numbers); > allows prosecution for breaches of the provisions on number manipulation.
Latvia	Operators must block calls where A-number has been manipulated, including cases when the end-user does not have the right to use the A-number or where the A-number is not routable. CLI-spoofing, including partial or full replacement of an A-number replacement, is considered numbering misuse and fraud. CSPs should include in their interconnection agreements actions to be taken in case of fraud and measures to prevent fraud and incorrect use of numbering. The NRA has the right not to grant or to cancel the right to use numbering for a CSP where fraud has been detected using numbering or incorrect use of numbering.
Norway	CSP must block, if technically possible and economically feasible, calls where the end user does not have the right to use the A-number or where the A-number is not routable. Nkom have developed an industry guideline for CLI Limited operator-based initiatives to reduce SMS spoofing on a case-by-case basis
UK	Ofcom requires: > operators to provide CLI facilities; > ensure that the CLI data provided with a call includes a valid, dialable telephone number that uniquely identifies the caller. o valid number: complies with the International public telecommunication numbering plan. If it is a UK number, it must be assigned by Ofcom under the UK numbering plan. o dialable number: in service and can be used to make a return or subsequent call o uniquely identifies the caller: number has been assigned to the caller Originating operators are responsible for ensuring that accurate CLI data is provided with a call and transit/terminating operators are expected to check that the number provided is from a valid number range. All calls must be associated with a Network Number that identifies the origin of the call. The

	Presentation Number may be changed to another valid, dialable number. Where the CLI contains invalid or non-dialable data, operators are required to prevent the calls from being connected to the called party, where technically feasible. Ofcom provision of a list of 'protected' numbers and a compilation of a 'Do Not Originate' list of numbers.

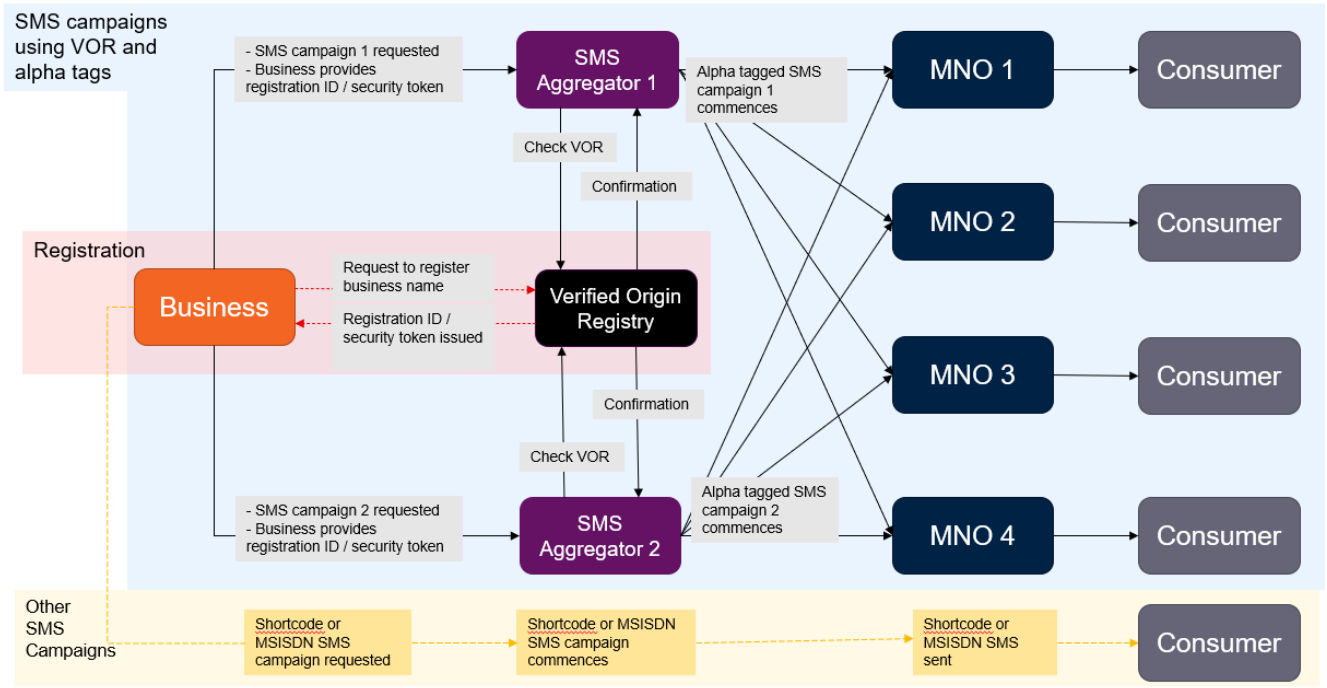
Alpha-numeric scams

TPG Telecom has previously submitted a proposal to the WC92 industry working group which contains a proven solution to stop scam activity associated with alpha-numeric sender IDs.

The proposal is to establish an Australian-based SMS sender ID protection registry. The Verified Origin Registry would enable CSP and aggregator scheme members to authenticate the use of alpha tags.

Members would register an authenticated alpha-numeric tag. Only messages with a CLI using the authenticated tag from trusted sources who are part of the scheme would be allowed to transit to the destination number – that is, the development of a whitelist for alpha tags.

All other alpha-tagged traffic from untrusted sources who are not part of the scheme would be blocked. For consumers, all alpha tagged traffic could be trusted, adding value and trust to the alpha tag via enhanced security, with a simple education message to consumers.



We do not view this as a competition issue, as businesses and individuals that do not want to afford themselves the added protection offered by the Verified Origin Registry using a registered alpha tag would be able to use mobile numbers as sender ID.

Other network protections being put in place to minimise scam call traffic would continue to

apply to SMS with a mobile number as its origination point (subject to that communication originating from an expected source i.e., the network that holds that number).

The scheme would not require significant funding for its operation, nor would it require a change of legislation.

Some parties have put forward a model of message inspection as a solution to limiting scam traffic. This approach seeks to identify malicious content and block those messages. This content inspection and message blocking approach would have a high administrative overhead to continually monitor messages for content URLs that can change instantly.

We strongly urge industry to adopt our proven solution for blocking alpha-numeric scam SMS.

Ad-hoc comments

Include a reference to C566 Number Management – Use of Numbers in Section 1 (possibly in 1.1.3), as not all number obligations are included in the Numbering Plan.

There are several clauses that should move to Note boxes for guidance.

For example clauses 4.1.1 and 4.1.2 should be Notes. They are somewhat repetitive such as comments re high volume calls and should be merged into a more cohesive guide.

NOTE: Scam Calls are often characterised by:

(a) High volume of calls from a particular CLI or range of CLIs where there is no valid use case (e.g., an outbound call centre), noting that high volume calls are not the primary evidence that the calls originating from an individual number are Scam Calls;

(b) Short duration;

(c) CLI issues:

(i). the A-Party CLI does not present to the Terminating C/CSP as a Public Number that can be called back, i.e. there is no way of verifying the originating A-party (for example the call cases where a dummy A-party CLI has been inserted by the Originating C/CSP for compliance with CA G549:2020 Interconnection Implementation Plan & CA G500:2020 Interconnect Signalling Specification;

(ii). the CND is Blocked with CLI Restriction;

(iii). the A-Party CLI is from an 'incorrect' number range, i.e. the Originating C/CSP has not been allocated the number range, or the number has not been ported to the Originating C/CSP (see Clause 4.2.1);

(iv). the A-Party CLI of an Inbound International Call is an Australian number (see CA G664:2022 for examples) or is not conforming to the ITU-T Recommendation E.164;

(v). the A-Party CLI is a number which is longer than normal and/or is being generated from unallocated number ranges (see Clause 4.2.1);

(vi). the A-Party CLI is not used in accordance with the Numbering Plan; and (vii) no A-Party CLI has been provided by the International Operator for an Inbound

International Call.

Further evidence is required to identify Scam Calls this may include:

(a) abnormally high volumes of traffic from a Carriage Service that does not usually generate that volume of traffic in the ordinary usage of that service;
(b) receiving customer complaints regarding phone calls that appear to be seeking information, for the purposes of committing fraud or where the customer has been scammed;
(c) customer complaints that their A-Party number has been subject to CLI Spoofing;
(d) complaints to relevant government agencies about particular A-Party CLI being used for Scam Calls; and
(e) the CND details are invalid, or the number presented as the A-Party CLI is valid but has been subject to CLI Spoofing.

5.1.1 and 5.1.2 should be merged into a single NOTE.

NOTE: Scam SMs are often characterised by:

(a) a high volume of messages to a large number of B-Parties where there is no valid use case;
(b) attempting to engage the consumer to click on a malicious URL;
(c) attempting to engage the consumer by eliciting a call or return SM to the scammer;
(d) attempting to obtain personal information in order to impersonate the consumer; and
(e) the misuse (impersonation) of the Alphanumeric Sender ID used by trusted brands (such as banks, telecommunications providers or government departments).

4.2.1 and 5.2.1 should both include reference to C566 as not all arrangements are included in the Numbering Plan.

Originating C/CSPs must only originate calls on their Telecommunications Network with CLIs, in accordance with the Numbering Plan and Industry Code C566 Number Management Use of Numbers, using the numbers or number ranges that are:

The below clauses should be Notes:

- 4.2.2
- 4.2.6
- 4.6.3
- 4.6.4
- 4.6.6
- 5.2.3
- 5.6.1
- 5.6.2

6 References – should include reference to C566 Number Management Use of Numbers Industry Code