For the attention of:

The Electronic Communications Committee

European Conference of Postal and Telecommunications Administrations

Nyropsgade 37, 4th floor

1602 Copenhagen

Denmark

Sent by email only to: Vassil Krastev

22 September 2023

Business Carrier Coalition views on the *"Draft ECC Recommendations (23)03 - Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers"*[1]

The Business Carrier Coalition ("BCC") is an industry coalition representing the interests of a number of international business telecommunications providers, namely Colt, Lumen, Orange Business and Verizon (collectively "we" or "us" or "our" in this letter).

The BCC provides a forum for issues of common interest to its members to be raised and presented to relevant regulatory stakeholders across Europe, the Middle East and Africa. The BCC members provide predominantly large business users with advanced electronic communications services across Europe.

The views expressed are specific to the markets under review by the European Conference of Postal and Telecommunications Administrations (CEPT) and their regulatory regimes and should not be considered as an expression of the views of the BCC or any or its members in other jurisdictions where the market and regulatory environments may differ from those considered in this consultation.

We are fully committed to implementing efficient measures to tackle spoofed calls so that our customers maintain their trust in telephony services and the Calling Line identification.

We would like to recall that the CEPT, in its report 338 of June 2022, is concerned of having a fragmented approach for a problem which is international in nature. We support the recommendation that the ban of CLI spoofing (for misuse/ and or fraudulent use) should be included in the EU legislation and/or having a set of common and feasible principles for banning it.

[1] https://cept.org/files/9522/Draft%20ECC%20Recommendation%20(23)03_v1.docx

We believe that a flexible approach is key to ensure that legitimate calls are not impacted by any measures adopted by National Regulatory Authorities. It is therefore essential to ensure that exceptions are defined.

We urge the CEPT to recognise that there is no one size fits all approach and global enterprise providers / International operators may not be able to fully comply but can offer other alternatives based on their capabilities.

We support the objective of these recommendations but their implementation is not always technically feasible.

"CEPT administrations should ensure that operators when directly handling incoming international voice calls over their international network interfaces adopt measures:

a. to block calls which do not respect ITU-T Recommendation E.157 [3];

Our understanding of this statement is that the CEPT expects an International Gateway Operator (IGO) in the terminating country to be able to validate that the calling number meets the E164 numbering format regardless of which country that call originated from.

In principle operators are able to partially validate the format - in as far as these formats are shared internationally (ITU). We understand the E.157 recommendation is not validating the veracity of the subscriber number.

b. for national geographic/fixed E.164 numbers: to block calls, or to suppress the CLI of calls with a national geographic/fixed E.164 number, except in justified cases. Any exception should be carefully considered and justified, since exceptions may be particularly attractive for spoofers. If exceptions are allowed, a mechanism to securely manage the exceptions should be adopted (e.g. secure whitelist between providers);

Whilst we are very supportive of this recommendation, we are concerned that the proposed intervention is not sufficient enough to ensure that all legitimate traffic is not blocked.

We also consider that clarification needs to be provided to fully understand the consequences of removing the CLI notably in regards to the Delegated Regulation 2023/654 not setting a maximum fixed voice termination rate in case of an invalid CLI[2].

<u>Potential issues identified</u>

- 2 CLI functionality

The 2 CLI functionality is attracting a lot of interest, notably from global enterprises that have chosen a country to establish their call centres that is different from the country they are providing the service in. This in turn means that the number of legitimate use cases where an international call is using a national presentation CLI is also increasing.

[2] Clarification of what "CLI" actually refers to in case of its invalidity from a technical point of view (PAI and/or FROM) is needed. For instance, in France, the authentication rules are generally leveraging the FROM field, not the PAI, whereas in other countries what is regulated seems to be the PAI. Are these proposed regulations intended only to screen the CLI presented to the called party, or are they intended to screen all CLI's being carried across the international gateways. For example, if a single call contains two calling numbers (such as the "Calling Party Number" and the "Generic Number" in an Q,767 ISUP IAM) do the operators only need to screen the actual CLI presented to the called party. Similarly, if the caller has set their calling number to CLI-RESTRICTED or WITHHELD, do the operators need to screen any CLI if the CLI will NOT be presented to the called party?

- Single node supporting multiple countries

Furthermore, with a large number of operators looking at options to improve the efficiency of their network, some functionality such as screening and blocking is being centralised into a single node supporting multiple countries. This situation creates a bleary line between the distinction of national and international calls. We therefore consider that the focus of the recommendations should be on ensuring that operators have enough flexibility to identify their legitimate traffic and to block illegitimate traffic.

- Diverted calls

In addition, we see a risk that legitimate diverted calls would be blocked because the IGO in the terminating country can't verify whether an inbound national calling number is the real originator of the call[3].

Proposed solution/alternative

We believe that there are considerable and serious risks when establishing a whitelist: for example; if fraudsters find out one of these numbers, it would be impossible to screen valid whitelist calls versus the number in the whitelist that have been spoofed. It also means that fraudsters will not only use exceptions, but they will also spoof valid numbers.

For example: a call from the number +32 2 xxx xx xx where the fraudster extended a valid number in FROM and PAI. For this reason, it will also not be possible to validate an international number (see E.157)

An alternative solution would be for international providers to establish dedicated trusted connections through an overlay network to route legitimate calls with national CLIs, for instance for international call centres.

It is recommended to change text to for national E.164 numbers which are allowed as CLI, excluding national mobile numbers (see 1.c.) to block calls.

c. for national mobile E.164 numbers: to block calls, or to suppress the CLI of calls with a national mobile E.164 number as CLI after checking and verifying that the user is not roaming abroad, except in justified cases. Checks on roaming status should be carried out while respecting relevant privacy provisions.

Potential issues identified

Fixed carriers do not have the functionality to connect with mobile operators to check if a customer is roaming or not. The requirement would be to do this per call, instead of per mobile user (so as to avoid high risk for spoofing on users with long-term stay abroad) in a secure manner (encrypted).

The implementation of a network-based solution is very challenging. There is still a considerable amount of legacy network equipment that does not (and will not) have the technical capability to interface with a mobile carrier's roaming database.

---

[3] Operational functionality issues
Any operational functionality issues on networks may lead to large call-blocking events. For example, there could be situations where operators mistakenly nationalise calling numbers which they are sending over an international link.

Choosing a network-based solution would create counterproductive results as terminating providers might be in a position where they have no other choice than to block all legitimate internationally originated calls in order to be compliant with their obligations, ie: to ensure that no spoofed mobile CLI's are allowed to pass.

There is also a risk of large call blockages if any such "roamer check" functionality was to have an outage or service issue. There is also no compulsion on the mobile providers to share roaming data with fixed line operators, and any such solution would need unrestricted near real-time access to all the mobile operators roaming database.

A technical and industry-based solution will also take significant effort to design and implement in a cost-efficient manner.

Proposed solution/alternative

To come to a workable solution will require further investigation. Such a solution should be harmonised, efficient, and practical with regards to implementation.

2. ensure that any measures adopted do not jeopardise the handling of legitimate calls or block nationally permitted exceptions (as further discussed in the informative Annex 1);

It is crucial to ensure that handling of legitimate calls remains possible. We believe the below scenarios provided in the annex to the recommendations are a valuable source of information, identifying important use cases where calls are legitimated.

In the scenarios mentioned to avoid impact on legitimate calls, it is important to allow for enough flexibility and time to implement, as technical and contractual rearrangements might be necessary to adjust. Therefore, a gradual EU-wide implementation of such a requirement will allow for international operators to enable this and to do so in a level-playing field.

For more information, please contact:

- Colt – Pablo Diez (Pablo.Diez@colt.net)
- Lumen – Dougald Robinson (dougald.robinson@lumen.com)
- Orange Business Services – Frédérique Imbrechts (frederique.imbrechts@orange.com)
- Verizon – Rob Rosendaal (rob.rosendaal@nl.verizon.com)