

**RÉSULTATS DE LA CONSULTATION PUBLIQUE NATIONALE  
DU 07 AOÛT 2023 AU 18 SEPTEMBRE 2023**

**CONCERNANT LE PROJET DE REGLEMENT RELATIF AU BLOCAGE DES APPELS PROVENANT DE NUMÉROS  
GÉOGRAPHIQUES AU DÉPART D'UN PAYS AUTRE QUE LE GRAND-DUCHÉ DE LUXEMBOURG**

**VERSION NON-CONFIDENTIELLE**

**LUXEMBOURG, LE 08 janvier 2024**

---

**SECTEUR COMMUNICATIONS ÉLECTRONIQUES**

---

Le présent document clôture le processus de la consultation publique nationale du 07 août 2023 au 18 septembre 2023 concernant le projet de règlement relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg (référence : CP/T23/5).

En application de l'article 4(4) du règlement ILR/T23/7 du 23 mai 2023 relatif à la procédure de consultation instituée par l'article 27 de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, l'Institut tient à rappeler qu'il tient exclusivement compte des commentaires qu'il a reçus durant la période de la consultation et qui se rapportent directement et uniquement au projet en question.

Ainsi, tout commentaire reçu après ce délai, ou qui ne se rapporte pas strictement au projet soumis à une consultation publique ne saurait être pris en compte et ne fera donc l'objet d'aucune publication de la part de l'Institut.

L'Institut a reçu une contribution de la part de :

- Fédération des opérateurs télécom du Luxembourg (« OPAL ») ;
- Microsoft Ireland Operations Limited ;
- Mixvoip S.A. ;
- POST Technologies ;
- NV Verizon Belgium Luxembourg S.A. ;
- Twilio Ireland Limited.

Le fait d'inclure ces commentaires dans ce document ne signifie nullement que l'Institut approuve ou désapprouve les opinions exprimées.

Institut Luxembourgeois de Régulation  
17, rue du Fossé  
L-1516 Luxembourg

Courrier envoyé par e-mail à [telecom@ilr.lu](mailto:telecom@ilr.lu)

Luxembourg, le 18 septembre 2023

**Concerne** : CP/T23/5 – Consultation publique nationale

Madame, Monsieur,

Les membres de l'OPAL ont revu avec soin le projet de règlement soumis en consultation et portant sur le blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg.

Depuis plusieurs mois, les opérateurs ont constaté une recrudescence des appels frauduleux auprès des leurs clients. C'est dans ce cadre qu'ils ont rencontré l'ILR à la fin du 1<sup>er</sup> semestre 2023 afin de demander du support sur ce genre de fraude et notamment l'autorisation de bloquer ce type d'appels.

En d'autres termes, les opérateurs ont initialement sollicité l'ILR pour obtenir l'autorisation de bloquer des appels frauduleux, sans nécessairement demander que cela devienne une obligation. Cependant, avec ce nouveau Règlement, il est évident que la demande initiale de soutien des opérateurs, qui visait à obtenir une **autorisation** pour bloquer les appels, s'est transformée en une **exigence contraignante**.

Les membres de l'OPAL comprennent et soutiennent l'objectif de l'ILR et la légitimité de la mise en place de ce nouveau Règlement afin d'éviter au maximum toute campagne d'appels frauduleux sur le réseau luxembourgeois.

Cependant, ils souhaitent souligner que la mise en place de ce Règlement va engendrer des coûts conséquents aussi bien en termes d'investissement financiers que humains. Il risque également de bloquer du trafic légitime (par exemple, le transfert/renvoi d'appel, les appels provenant et destinés au même pays ne pourront plus transiter par des routes internationales, les appels provenant des centres d'appel établis dans un pays différent de celui dans lequel ils fournissent le service).

De plus, ils notent que le Règlement ne présente qu'**un seul article** et qu'aucun document de motivation ne l'accompagne. Ainsi ils jugent ceci insuffisant et disproportionné et demandent à l'ILR une entrevue pour prendre en compte les remarques des opérateurs ; ceci afin que l'objectif de limiter les tentatives de fraude soit atteint sans mettre de surcharge inutile sur les opérateurs et éviter de bloquer des appels légitimes.

En effet, le sujet étant très technique et ayant des répercussions importantes sur les opérateurs qu'ils soient nationaux ou internationaux, afin d'**éviter toute incompréhension** dans la formulation des cas d'exception que les membres de l'OPAL souhaiteraient voir appliquer au Luxembourg, ceux-ci demandent à l'ILR **une rencontre afin de discuter plus en détail les différents cas de figure** afin d'avoir une mise en application efficace et en lien avec les réalités du marché luxembourgeois.

De plus, les membres de l'OPAL sont d'avis qu'une **harmonisation au niveau européen** serait recommandée pour éviter une mise en œuvre différente et coûteuse dans les états membres de l'Union. A cet effet, l'OPAL a consulté le document (en version 'draft') de l'Electronic Communications Committee (ECC) présentant ses recommandations pour traiter les appels vocaux internationaux entrants avec des numéros E.164 nationaux suspectés d'être falsifiés. Et ils recommandent à l'ILR d'attendre la version finale de ce document afin de prendre en compte les compléments d'information qui pourraient également être applicables au Luxembourg.

En restant à votre entière disposition pour toute demande d'information additionnelle, nous vous prions de croire, Madame, Monsieur, en l'assurance de nos sentiments distingués.



Pour l'OPAL,

Géraldine Bélier

Secrétaire générale



## MICROSOFT IRELAND OPERATIONS LIMITED

### Comments on the Luxembourg Regulatory Institute Consultation on Proposed Regulations on the Blocking of Calls from Geographic Numbers from a Country Other Than Luxembourg

18 September 2023

Microsoft Ireland Operations Limited (“Microsoft”) appreciates the opportunity to provide its views on the proposal of the Luxembourg Regulatory Institute (“ILR”) to block all calls with Luxembourg phone numbers that are routed into Luxembourg from another country. While Microsoft understands the concerns of the ILR and agrees that action must be taken to combat nuisance and fraudulent calls, there are more effective approaches to the problem, that will not inadvertently block legitimate calls, as described below.

#### **Distinguishing Legitimate Calls from Fraudulent Calls**

At the outset, it is important to highlight that not all number “spoofing” or Calling Line Identification (CLI) number manipulation is fraudulent or performed with malicious intent. There are several reasons an alternative number that is not directly tied to the calling line may be displayed as caller ID to the receiving party, as well as numerous situations in which legitimate calls are routed over international trunks displaying domestic CLI. Below are several examples:

- Cloud-based conferencing services, such as Microsoft Teams Meetings, are global in nature and may, for legitimate reasons, display a Luxembourg CLI on calls routed into Luxembourg over international trunks. This can happen because Teams enables online meeting participants to dial a phone number – in this example, a Luxembourg phone number – from the bridge to add a user, on her mobile or landline, to the online meeting through a conference call. The outbound call to a Luxembourg landline or mobile, which originates from the online Teams conference bridge caller inside Luxembourg, will display a Luxembourg phone number (either a Luxembourg phone number that has been issued to Microsoft and then associated with the Teams conference bridge, or the Luxembourg Teams customer’s telephone number). The call from the conference bridge to the called party in Luxembourg is a Luxembourg-to-Luxembourg call. Due to the characteristics of our cloud architecture, we would process this call via EU data centers outside Luxembourg. Thus, when the media returns to Luxembourg from the data center where it was processed, network operators in Luxembourg are likely to perceive such calls as international traffic, even though the call was initiated by a user in Luxembourg and terminated with a user in Luxembourg. As a result, such a call would be blocked if the ILR enacts its proposed policy. Unfortunately, in countries where CLI blocking on inbound international calls has been implemented, we have encountered this scenario and it has caused significant disruption to government agencies and large enterprises because they suffer degradation to their cloud conferencing services.
- In the enterprise context, a user may dial out from their individual direct line, but the enterprise’s general number will be displayed as caller ID so that the employee’s direct line is

not shared with the receiving party. For example, a medical practitioner that is calling from their clinic or an employee of a non-for-profit organization providing services to a client.

- There are growing numbers of scenarios in which phone numbers are temporarily assigned to an outbound call for privacy, security, or other reasons, such as in a food delivery service app scenario.
- Global call centers often legitimately modify the CLI that appears on outbound calls to ensure their customers answer inbound calls from a familiar number (i.e., the company's local number).
- In the consumer context, Skype to Phone is a one-way outbound VoIP-to-PSTN calling service that does not have inbound calling capabilities and therefore does not assign dialable phone numbers to the user that could be used as CLI by default. However, Skype allows users to assign their authenticated Luxembourg mobile number as displayed CLI on outbound calls. This enables Skype users to display CLI using their mobile number that their friends and family can recognize, thus vastly increasing the chances that the call will be answered as well as providing a number to call back if the call is missed. Skype to Phone partners with several global telephone network operators to convert these IP calls to the PSTN for delivery to the recipient's terminating carrier. Many of Skype's partners use international trunks to deliver Skype to Phone calls to terminating carriers in Luxembourg. In these cases, a call made from a Luxembourg Skype to Phone user to another person in Luxembourg may nevertheless be delivered to the local telephone network over international trunks and would be blocked as international traffic carrying local CLI.

All the examples above ensure that: (1) the displayed number is a legitimate, assigned number that the calling party has the authority to use; and (2) the displayed number uniquely identifies the caller and originating carrier in a manner that enables the source of the call to be traced. These examples further demonstrate that the increasingly cloud-based telecommunications marketplace, with infrastructure in a single country supporting calling services across the globe that necessitates the legitimate manipulation of CLI, requires precise solutions to combat fraudulent and nuisance calls/texts. Such precise solutions that do not overreach and inadvertently block legitimate calls are also necessary to ensure Luxembourg's compliance with the EU's single market goals.

### **Solutions that Properly Balance Protecting Against Fraudulent Calls While Enabling Legitimate Calls**

Below, Microsoft offers solutions that properly balance the need to protect consumers while simultaneously enabling emerging and legitimate pan-European business models. Microsoft respectfully requests that ILR consider implementing some or all of the following as alternatives to its proposed blocking requirement.

#### **Streamlined Call Blocking Options.**

Rather than simply blocking all calls transmitted from foreign locations with domestic CLI, the ILR could adopt more streamlined blocking approaches.

The ILR could adopt regulations that block calls from numbers that are either "Do Not Originate" (DNO) or have not been allocated by ILR to any provider ("Prohibited Number" or PN) and the formalization of the related DNO and PN lists. In both scenarios, there is no legitimate basis for making outbound calls

using these numbers. Therefore, blocking all such calls will protect consumers from harmful, fraudulent calls while not putting legitimate business models at risk.

Additionally, the ILR could leverage the advanced capabilities of Session Initiated Protocol (SIP) fields that are communicated between operators in the delivery of VoIP calls. There are two SIP fields for CLI that don't necessarily need to provide the same number. First, the P-Asserted Identity (PAID) field conveys the "Network Number," a unique network identifier associated with the call that is communicated from operator to operator, but not displayed to the called party. The second SIP field is the FROM field, often thought of as traditional Caller ID, which communicates the "Presentation Number" that should be displayed to the called party. For example, as described above, when a user makes a call from Teams, the number associated with their individual direct line might be the Network Number in the PAID field, but their enterprise's general number might be used as the Presentation Number in the FROM field.

This approach has been used in the UK wherein the UK's Ofcom has implemented blocking of international inbound calls with a local Network Number in the PAID field but permits local CLI to be used as the Presentation Number in the FROM field.<sup>1</sup> Although Ofcom issued this approach as a guideline rather than a requirement, we understand that it was requested by incumbent network operators in the UK to afford regulatory authority to block certain forms of inbound international traffic. Thus, in practice, it has become the *de facto* approach in the UK. It could just as easily be implemented as a mandatory requirement in Luxembourg. The advantage of this approach is that legitimate traffic, such as Microsoft's Teams Meeting traffic, can continue to display UK CLI to the called party and avoid blocking insofar as Microsoft modifies the PAID field to include a non-UK telephone number *issued to Microsoft*. An inferior approach, but one that is still better than the blocking proposal being considered here, would be the approach taken by Germany which requires carriers that receive inbound international calls with domestic CLI to change the display number to ANONYMOUS before delivering the call.<sup>2</sup> This approach at least permits the option for the called party to answer the call, albeit with caution.

Finally, there are emerging technologies that enable carriers to implement a voice firewall, using Machine Learning and Artificial Intelligence (AI) techniques to identify fraudulent calls so the called party can decide whether to block it. This is a potentially useful tool that – if implemented successfully – could be used to combat fraud while preserving and protecting legitimate business operations. Microsoft itself is currently developing products that will deploy AI as a powerful tool to combat illegitimate scam calls. The risk with firewalls, however, is rushing them to market, before they are fully tested and proven. This likely would result in overreach and blocking of legitimate calls. Based on Microsoft's experience studying these types of tools, it will take time to ensure only the blocking of illegitimate calls. In addition, procedures would need to be put in place to enable operators to discuss any actual blocking prior to its implementation, and to immediately undo blocking where applied erroneously. Microsoft would be happy to work with ILR to further study and test the use of AI tools in the context of fraudulent spoofing.

---

<sup>1</sup> Ofcom, [https://www.ofcom.org.uk/data/assets/pdf\\_file/0021/247503/CLI-guidance-annex.pdf](https://www.ofcom.org.uk/data/assets/pdf_file/0021/247503/CLI-guidance-annex.pdf) [https://www.ofcom.org.uk/data/assets/pdf\\_file/0021/247503/CLI-guidance-annex.pdf](https://www.ofcom.org.uk/data/assets/pdf_file/0021/247503/CLI-guidance-annex.pdf) (Nov. 15, 2022).

<sup>2</sup> German Telecommunications Act (TKG) § 120 (4), and further details provided <https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html>.

Deploy STIR/SHAKEN. Efforts to combat illegal spoofing through CLI rules, such as the blocking proposal of ILR and those outlined above, are likely to be only partially effective and will put at risk some legitimate calls. In the longer term, Microsoft recommends that ILR combat fraudulent spoofing by adopting industry standards-based, technological measures to authenticate CLI. In the US, Canada, and France, regulators have implemented the STIR/SHAKEN<sup>3</sup> framework for authenticating the accuracy and integrity of CLI data communicated between operators. Even if Luxembourg's current telecom infrastructure is not prepared to quickly implement STIR/SHAKEN within the country (i.e., networks have not yet transitioned from TDM to IP), this is not a reason to postpone STIR/SHAKEN implementation indefinitely. As described below, work is ongoing to develop a cross-border STIR/SHAKEN authentication framework that would enable providers to authenticate calls even in countries where there is no national STIR/SHAKEN deployment. ILR should encourage its service providers operating networks that are capable of reading STIR/SHAKEN tokens to participate in these cross-border CLI authentication programs so fraudulent calls into Luxembourg can be more effectively stopped.

Microsoft has joined other global service providers to create a new STIR/SHAKEN governance authority that, with the support of the telecom standards body ATIS, has developed a CLI authentication framework designed to operate across international borders. As it is not tied to a particular country, this new framework will allow STIR/SHAKEN to be available to voice service providers in countries where token-based CLI authentication has not been implemented on a national basis. It will also allow voice service providers that have IP networks to exchange authenticated traffic with other voice service providers that have implemented STIR/SHAKEN in their networks.

Specifically, a Cross Border Call Authentication Governance Authority (CBCA-GA) has been created by an initial group of international voice service providers to develop the policies and architecture for the STIR/SHAKEN deployment. National governing authorities, like ILR, will be able to evaluate the CBCA-GA's policies, and it is our hope that they will be able to treat the CBCA-GA as a trusted partner and make national systems interoperable to facilitate information sharing for cross-border CLI authentication in the future. The CBCA-GA has put in place processes to ensure that voice service providers meet strict requirements for membership in the CBCA-GA. The CBCA-GA has selected iconectiv as its policy administrator, which will be responsible for approving service providers and certification authorities, issuing tokens, verifying originating providers for terminating and gateway providers, and enforcing CBCA-GA policies.

Each service provider must provide the policy administrator with information necessary to authenticate the provider and determine they are legitimate and trustworthy. This includes evidence of the provider's legal status, contact details, authorization to provide communications services, and other information concerning their compliance and service history. Service providers are required to have processes in place to identify problem users and support traceback requests. The policy administrator will also make an evaluation of whether the service provider is technically capable of deploying SHAKEN. Once accepted, registered as a member and issued a token, an originating service provider can obtain a certificate for signing calls from a certification authority approved by the CBCA-GA policy administrator. Originating service providers will be suspended or removed from membership if they provide attestations for

---

<sup>3</sup> STIR, or "Secure Telephone Identity Revisited," is a set of standards established by the Internet Exchange Task Force (IETF) describing the mechanics of CLI authentication signaling. SHAKEN, or "Signature based Handling of Asserted information using toKENS," is a framework that defines the use of STIR and other elements to make up a complete ecosystem, as defined by the Alliance for Telecommunications Industry Solutions (ATIS) in a number of standards.

customers that do not have the right to use a particular telephone number or engage in other activities inconsistent with the CBCA-GA's policies.

In the future, we hope that there will be interoperability between national SHAKEN frameworks (such as the STI-GA in the U.S. and the STI-CA in Canada) and the CBCA-GA so that attestations from the CBCA-GA will be recognized by the governance authority in the terminating country, and vice versa. This would require interconnection between the two policy administrators to share read-only access to their lists of registered service providers and approved certification authorities. Such exchange of information will be based on ATIS's standard for cross-border use of SHAKEN (ATIS-1000087).

Cross-border STIR/SHAKEN is expected to launch on a limited basis this month, September 2023. A small number of voice service providers, including Microsoft, will provide attestations when sending traffic to each other that originates in countries without a SHAKEN framework already established.

ILR should encourage Luxembourg voice service providers with IP networks to implement STIR/SHAKEN on a voluntary basis so they can leverage this newly developed cross-border authentication framework. This would allow terminating providers in Luxembourg who are completing their transition to IP to use call attestation information to help shield their subscribers from illegally spoofed calls. Similarly, when originating calls, these providers could use STIR/SHAKEN to mitigate the increasing risk that their customers' calls will be blocked by terminating providers. Even if a solution is only temporary until a national framework is developed, these providers can leverage the use of CLI authentication among a selected group of domestic and foreign carriers to ensure the delivery of legitimate calls to both national and international destinations.

Initial interest in the project has been positive and additional voice service providers are expected to become members in the coming months. Microsoft would be pleased to work with ILR to discuss accessing the benefits of the non-jurisdictional governance authority so Luxembourg's consumers are protected from scam calls while ensuring they receive legitimate calls that may originate outside of Luxembourg.

## **Conclusion**

Microsoft applauds ILR's work to protect Luxembourg citizens and businesses from harmful and fraudulent calls. This is a critical issue that must be addressed using a number of tools that are currently – and prospectively – available to regulators and industry participants. As discussed herein, however, some of these currently available tools can inadvertently harm Luxembourg users by disrupting legitimate business models. Microsoft encourages ILR to implement solutions that protect consumers from harmful illegitimate calls and texts while also protecting legitimate businesses and their innovative communications solutions. Using STIR/SHAKEN to authenticate calls on a call-by-call basis is the most effective solution to combatting fraudulent activities, and Microsoft encourages ILR to begin the transition to STIR/SHAKEN now, as carriers become capable of authenticating calls, by opting into the cross-border STIR/SHAKEN governance authority.



Objet : **CP/T23/5 du 07/08/2023**

Steinsel,  
le 15 septembre 2023

Messieurs,

Dans le cadre de votre communication reprise en objet, et après discussions internes, nous voudrions exprimer notre point de vue concernant la nouvelle loi proposée.

Plusieurs points doivent être abordés afin de clarifier la situation pour les opérateurs :

**Discrimination potentielle envers les appels Wi-Fi mobile à l'étranger :**

Cette disposition pourrait pénaliser les utilisateurs de services de communication par Wi-Fi, créant ainsi une inégalité dans l'accès aux technologies de communication.

**Comment exactement « l'international » est à définir ?**

Le Luxembourg abrite de nombreuses entreprises internationales dont les sièges sociaux hébergent leurs infrastructures informatiques et de téléphonie en dehors du Luxembourg.

La question de la définition du terme "international" se pose particulièrement avec les fournisseurs de Cloud-PBX tels que 3CX, Starface, Allocloud, etc., qui, en raison de leur indisponibilité au Luxembourg, sont installés dans les centres de données internationaux de par exemple Microsoft, Google, AWS (Amazon), OVH, Hetzner, etc. Dans ce contexte, selon la définition adoptée, il est à craindre que l'employé basé au Luxembourg soit considéré comme "international".

La nouvelle loi pourrait entraîner des désagréments pour ces entreprises en obligeant leurs employés à passer par des opérateurs locaux, ce qui pourrait affecter leur efficacité et leur coût opérationnel.

Nous soutenons l'idée d'une loi visant à lutter contre le spam, et nous soutenons également celle-ci, mais nous souhaitons souligner quelques aspects à prendre en considération:

**Les utilisateurs en télétravail à l'étranger :**

La réglementation devrait prendre en compte leur situation pour garantir une communication sans entrave. Avec la version actuelle de la loi, toute communication originant d'un numéro luxembourgeois, mais initialisé par une personne localisé physiquement en dehors du Grand-Duché sera impactée.

De même, les utilisateurs de services de communication mobiles (FMU/FMC) doivent être pris en compte. Comment la loi affectera-t-elle leur expérience utilisateur et leurs coûts associés ?

**Les utilisateurs de Microsoft Teams,**

en particulier ceux utilisant les fonctionnalités de Routage Direct et de Connexion Opérateur. La loi devrait clarifier son impact sur ces services essentiels de communication d'entreprise.

En conclusion, bien que l'idée de lutter contre le SPAM soit louable, bloquer certaines fonctionnalités ne semble pas être la solution la plus adaptée, et cela pourrait entraîner une discrimination dans l'accès aux services de communication. Nous suggérons d'envisager l'adoption de protocoles tels que Stir/Sharken, en suivant l'exemple de la France, pour aborder le problème du SPAM de manière non discriminatoire.

Dans l'attente,

Recevez, Messieurs, nos salutations les meilleures.

La team Mixvoip S.A.





Institut Luxembourgeois de  
Régulation  
Monsieur Luc Tapella  
17, rue du Fossé  
L-2922 Luxembourg  
Luxembourg

**Dossier traité par :**  
Département Compliance Telecom

**N.réf. :** R/2023/002/R12

Luxembourg, le 15 septembre 2023

**Objet :** Votre consultation publique CP/T23/5 portant sur le projet de règlement relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg

Monsieur le Directeur,

Par la présente, POST tient à vous remercier pour l'occasion de pouvoir soumettre ses observations relatives à la consultation publique nationale portant sur le projet de règlement relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg.

En accord avec les propositions que POST vous a déjà faites lors de notre réunion de travail bilatérale du 30 juin 2023, et suite à votre correction publiée le 7 août 2023, POST souhaite vous demander de bien vouloir de prendre en compte les éléments suivants :

**1) Les numéros mobiles sont à exclure temporairement du champ d'application du présent règlement**

A l'heure actuelle, il existe des contraintes techniques qui ne permettent pas toujours de faire la distinction entre les appels entrants légitimes et les appels entrants frauduleux. En effet, le « Home Routing » est un feature indispensable afin de filtrer correctement les appels entrants et ainsi de ne pas bloquer des appels légitimes.

Or, la mise en place de ce feature repose sur la collaboration, et notamment l'adaptation des conditions contractuelles, entre les opérateurs nationaux et opérateurs partenaires étrangers.

Ces adaptations nécessitant du temps, POST souhaite vous demander que les numéros mobiles soient temporairement exclus du champ d'application du règlement.

**2) La responsabilité du blocage incombe au premier opérateur national réceptionnant les appels internationaux entrants**

Ce point semble crucial afin de garantir une meilleure efficacité du règlement. En effet, si l'appel international entrant transite en premier via un opérateur A pour ensuite être terminé sur le réseau de l'opérateur B, l'opérateur B n'est pas en mesure de déterminer



le caractère frauduleux ou légitime de l'appel. Dans ce cas de figure, seul l'opérateur A en est en mesure de le faire, de sorte que la responsabilité de bloquer les appels frauduleux incombe à cet opérateur et non pas à l'opérateur terminant l'appel.

De manière corollaire, si le premier opérateur réceptionnant l'appel entrant termine cet appel sur son réseau, la responsabilité lui incombe.

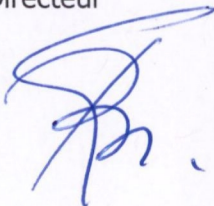
Sur base de ces observations, POST se permet de proposer les adaptations suivantes :

*Art. 1<sup>er</sup>. Le premier opérateur national réceptionnant, soit en vue de transit, soit de terminaison, ~~Les opérateurs fournissant des services de terminaison d'appel fixe et/ou mobile bloquent les appels~~ bloque tout appel* provenant de numéros géographiques luxembourgeois au départ d'un pays autre que le Grand-Duché de Luxembourg.

Mes équipes restent à la disposition des vôtres pour tout complément d'information.

Veuillez agréer, Monsieur le Directeur, mes meilleures salutations.

Gaston Bohnenberger  
Directeur



**Annexe :**

Support de slide POST de la réunion de travail du 30 juin 2023

# Verizon Response to ILR's proposal for International Fixed CLI blocking

18 September 2023

## Introduction and background

Verizon welcomes the consultation<sup>1</sup> by the Institut Luxembourgeois de Régulation (“**ILR**”) on the above mentioned subject. Outside of the United States, Verizon provides a broad range of global communication products and enterprise solutions, predominantly to large business and government customers. We are established in most European Union Member States, and provide services in over 150 countries worldwide.

Verizon Luxembourg (“**Verizon**”) does not serve consumers in Luxembourg and therefore our customers are not at risk of suffering the same harm as consumers as a result of scam and nuisance calls. The views expressed are specific to the market in Luxembourg and its regulatory regime and should not be considered as an expression of the views of Verizon in other jurisdictions where the market and regulatory environments may differ from those of Luxembourg.

Verizon supports the objective of ILR and we are fully committed in restoring customer trust in voice communication, notably by implementing measures to tackle nuisance calls whenever these measures are efficient and proportionate. In the context of the Luxembourgish market, Verizon considers that international Fixed CLI blocking seems to be an efficient and proportionate solution that could be relatively straightforward for operators to implement. [CONFIDENTIAL: .]

## Risk related to the proposed measure

Nonetheless we consider there is a risk that certain legitimate traffic could be blocked if the intervention was to be implemented in its current form. Whilst this will probably not impact providers in Luxembourg that do not have any traffic coming to Luxembourg with a national CLI, the proposal could cause a disruption to voice traffic terminated by operators in Luxembourg in the following circumstances:

---

<sup>1</sup> [Consultation publique nationale portant sur le projet de règlement relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg réf CP/T23/5](#)

- 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 means that the number of legitimate use cases where an international call is using a national presentation CLI is also increasing.

- 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 blurry 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 International Gateway Operator in the terminating country can't verify whether an inbound national calling number is the real originator of the call.

- 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.

## **AOB**

Finally, Verizon would like to highlight that the CEPT is also consulting on a similar recommendation and Verizon is planning to submit a reaction. We intend to share this reaction also with ILR.

Furthermore, we value to note that Verizon in general prefers to see harmonised solutions across the EU being developed where possible, that are fit-for-purpose. This would not only reduce the burden on international operators to be compliant with the relevant legislation across the EU, but also ensure faster implementation.

We are aware that circumstances can differ across EU Member States. In the case where harmonisation is not feasible, we call upon Member States to carefully test the necessity and proportionality of introducing measures, taking into account the declining market for voice communications. Referring to the (national) principles of good governance, this should lead to measures that are light-touch and do not go beyond what is necessary to reach the relevant objective.

\* \* \*



*Non Confidential*

***Twilio's Response to the ILR consultation CP/T23/5 on the "Draft regulation on the blocking of calls from geographic numbers originating in a country other than the Grand Duchy of Luxembourg"***

*(Projet de règlement relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg)*

18 September 2023



## 1. About Twilio

- 1.1. Twilio Ireland Limited is a provider of electronic communications services in Luxembourg, and has been granted rights over Luxembourg numbering resources by ILR.
- 1.2. As a leading global Communications Platform as a Service (CPaaS) provider, Twilio provides services to more than 285,000 enterprises globally and powers more than 1 trillion interactions between them and their customers every year.
- 1.3. Twilio's software allows customers to communicate with their customers over voice, SMS, messaging, or email thanks to the communications feature that companies have added into applications across a range of industries, from financial services and retail to healthcare and non-profits.
- 1.4. Twilio serves a number of global customers as well as Government organizations. Many of Twilio's customers are also small and medium-sized enterprises. Twilio's non-profit arm, Twilio.org, supports charitable organizations to deliver their communications needs, such as the Norwegian Refugee Council, a global NGO supporting refugees worldwide. Twilio is also a technology partner and supporter of the United Nation's Vaccine Alliance GAVI.

## 2. Introduction and key points

- 2.1. Twilio Ireland Limited (hereafter 'Twilio') welcomes ILR's consultation entitled "***Projet de règlement relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg***". Twilio takes the opportunity to raise some concerns about ILR's envisaged approach:
  - 2.1.1. In Twilio's view, there are several innovative, legitimate use cases for using domestic (in this case Luxembourgish) numbers for inbound international calls originating abroad, and the proposed ILR approach presents a high risk of blocking such legitimate calls.
  - 2.1.2. Twilio would like to point the ILR to more nuanced approaches contemplated notably by CEPT, but also by the UK regulatory authority Ofcom and the Irish ComReg.



2.1.3. The ILR would be well advised to align its approach with other regulators and CEPT administrations to ensure as much legal certainty as necessary and to avoid negatively affecting essential business processes and consumer choice.

### 3. **Legitimate use cases and risks associated with the ILR approach**

3.1. Twilio wishes to express its full support for the overarching goal of the ILR to combat the fraudulent use of numbers. Whilst harmful use of telecommunications is an unfortunate reality and should be actively combatted, legitimate innovative use cases of numbers, including Communications Platform as a Service – CPaaS – exist and are growing. CPaaS use cases are appreciated by businesses, government, and end-users. There are legitimate CPaaS use cases for presenting Luxembourgish CLI's with the caller being located abroad, for instance where (company-internal and external) call centres provide support for Luxembourgish customers, cloud-based conferencing platforms dial out to include additional participants, etc. There are also legitimate use cases for using temporary CLIs, for instance to ensure that subsequent calls are properly answered, to protect the identity of both the caller and called individual etc. Users wishing to make calls with Luxembourgish CLIs may also include government agencies (e.g. EU institutions), non-government organisations, charities, etc.

3.2. Twilio therefore believes that exemptions from the envisaged drastic blocking rule should be possible, to support legitimate use cases. Any measures, be they industry agreed, regulatory in nature, or even legislative in nature, should not result in hampering innovation, restricting competition or negatively affect important end-users. In addition, conflicts with the Luxembourg electronic communications legislation<sup>1</sup> should be excluded, in particular as regards the provisions ensuring end-to-end connectivity (notably Art 3 (2) 3°, Art 19 (1) 9° - the law also contains other references to 'connectivité de bout en bout').

### 4. **Other Regulatory Body approaches (Ofcom, ComReg, CEPT)**

4.1. Twilio wishes to highlight a number of ongoing work items in other jurisdictions. The UK regulator Ofcom recently conducted a consultation on the introduction of CLI authentication. In its introductory remarks, Ofcom explicitly states that action needs to be

---

<sup>1</sup> Loi du 17 décembre 2021: <https://legilux.public.lu/eli/etat/leg/loi/2021/12/17/a927/jo>





taken aimed at reducing harm caused by scam, nuisance and other harmful calls/texts in the UK - and at the same time clarifies that Ofcom stands to support legitimate and innovative use cases which are beneficial for end-users, and for competition.

- 4.2. Perhaps most relevant to the ILR approach is CEPT's recent ECC Draft Recommendation 23/03: "Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers". In this Draft Recommendation, the ECC highlights several scenarios of legitimate use cases which it recommends CEPT administrations, including ILR, to consider when taking measures that could lead to the blocking of legitimate numbers. In particular, Twilio notes and highly welcomes that the ECC Draft Recommendation points out that CEPT administrations should "...ensure that any measures adopted do not jeopardise the handling of legitimate calls or block nationally permitted exceptions" (p.4).
- 4.3. In its scenario 4: "Call to a foreign number with call forwarding to a national number", CEPT advises that in order not to impact legitimate voice calls, CEPT administrations may consider solutions to verify that the call is actually originated in Country A. To that end, in order to identify a voice call that should not be blocked, CEPT states that it could be useful to:
  - 4.3.1. Either introduce a whitelist to include the fixed/geographic numbers pertaining to Country A which are permitted to be used over such cloud-based solutions as CLI for incoming international voice calls. In such a case, operators should not block, or suppress the CLI of incoming international voice calls where the CgPn is included in a whitelist; or
  - 4.3.2. Impose an obligation on or recommend to providers of cloud-based solutions to implement a dedicated interface<sup>[1]</sup> in Country A such that calls originated by an end-user in Country A with a national number from Country A as CLI would be received through this dedicated interface which could be the same connection used to convey calls originating from the national service provider.
- 4.4. Both provisions are much more nuanced - and in Twilio's view more appropriate - than the approach ILR is envisaging.
- 4.5. As for the dedicated interface for the verification of originating calls, one of the most advanced examples of such a methodology would be the implementation of Stir/Shaken.



Twilio wishes to highlight that it was deeply involved in the design and implementation of STIR/SHAKEN in the United States. Whilst STIR/SHAKEN has produced material improvements so far in the United States, it has not quite performed as well as expected in some areas. As an example, extensions to STIR/SHAKEN, like the DIV passport, are required to have call authentication work with forwarded calls and that has yet to be supported widely. Additionally, with exemptions for calls not being forwarded using IP-technologies, not all traffic is being authenticated leading to more complicated tracebacks. STIR/SHAKEN does not replace the need for a system enabling the reporting of misuse as well as rapid and reliable traceback to the call originator. STIR/SHAKEN is a mechanism to help enable that, but is not the only mechanism that may be appropriate to achieve this goal. Bona fide Communications Providers are themselves the victims of sophisticated entities intent on misusing telecommunications services, and these entities may use services paid for (rather than relying on spoofing third parties' numbers) and constantly adapt their practices in ways that are not easy for Communications Providers to identify. As a consequence, the US Federal Communications Commission (FCC) is now placing additional emphasis on the identification of customers and on users/victims reporting harmful activities and call analytics, which can lead to additional improper blocking or mislabelling of legitimate calls. Given the recurring problems with false-positives affecting legitimate users, interest in the US is also growing for pursuing other technology options (including analytics and artificial intelligence) to deal both with the identification of harmful users and to ensure that false-positives do not interrupt critical business processes of legitimate users.

## 5. **Recommended measures**

- 5.1. In Twilio's view, the most important capability to introduce to deal with harmful activity is to rapidly and reliably determine, based on a traceback, whether a harmful actor is using a number, and to take action against harmful use all the while ensuring that legitimate use is not unduly impeded. Indeed, Twilio's experience shows that the ability to rapidly and reliably perform a traceback to the entity that is in reality originating a call/text is crucial in effectively combating harmful activity, regardless of whether the call/text originates from an entity that uses a spoofed number, or from an entity that has legitimately been given a



number in use. This is the case because harmful activity, including automated calling/text, can and does occur not only by entities spoofing numbers, but also by entities that are given numbers in use on a bona fide basis. Ensuring that legitimate use is not unduly impeded, and rapid redress where legitimate use is impeded, is a necessary feature of any envisaged action, be it industry agreed, regulatory, or legislative in nature.

- 5.2. Vigorous law enforcement against the actual scammers (which are abusing not only citizens and businesses as end-users, but also operators of electronic communications services), also, needs to be part of the package of measures, in addition to technical measures imposed on operators of electronic communications networks and services.
- 5.3. Twilio is aware that the CEPT ECC NaN working groups (in particular NaN2 (*Number Portability and Switching, Trust in Numbering, and Network Technology Regulatory Issues*) and NaN1 (*future of numbering issues*) have in the past addressed CLI spoofing, and are currently working on deliverables such as:
  - draft ECC Recommendation on incoming international voice traffic with suspected spoofed national E.164 numbers (NaN2 working group)  
<https://cept.org/ecc/groups/ecc/wg-nan/nan2/client/meeting-calendar/>  
The NaN2 working group also has a meeting scheduled on SMS Sender ID.
  - draft ECC Report on Numbering for cloud-based communication services (NaN1 working group)  
<https://cept.org/ecc/groups/ecc/wg-nan/nan1/client/meeting-calendar/>
- 5.4. This work is actively being pursued, with meetings scheduled, and a consultation ongoing. It would be unfortunate if individual authorities, such as ILR, would take radical decisions that will render a coordinated international approach impossible. Twilio appreciates that ILR is actively engaged in relevant discussions at CEPT ECC level and would welcome its continued efforts in ensuring that a common approach is taken in such a critical area.
- 5.5. Twilio is available to discuss the matters at hand directly with the ILR, to clarify its concerns, explain the legitimate use cases of its customers, jointly identify practicable solutions, etc. Please do not hesitate to reach out to:

Twilio Ireland Limited

Address: 3 Dublin Landings, North Wall Quay, Dublin 1, Dublin, Ireland D01 C4E0



Attention: Twilio Global Regulatory Affairs

Email: [regulatory-notice@twilio.com](mailto:regulatory-notice@twilio.com)

---

[1] In this Draft ECC Recommendation, a dedicated interface means the implementation by an undertaking of a dedicated SIP interface or alternative trunk type interface to serve another undertaking to ensure that calls from end-users of the latter undertaking originate on the national network.