

FCC regulation on foreign voice traffic

Filippo Cauci

October 14, 2021

FCC regulation and foreign voice traffic

- Voice traffic generated overseas is collected by International carriers in different countries ۲
- Traffic is delivered to US domestic operators through International Carriers with which they have direct ٠ interconnections
- International carriers collect traffic both from their retail arms/domestic operators as well as from other ۰ international carriers



- FCC regulation impacting foreign voice traffic with CLI belonging to USA
- Identified traffic use cases affected by FCC regulation: 1) US subscriber roaming abroad. In this case calls are generated in the visited network (2G/3G coverage or CS fallback) with CLI belonging to USA numbering plan. 2) US call center with remote location
- As transit carriers we expect traffic generated by our retail arms and directly connected domestic operators as «trusted»

i³ forum



Steps to comply with FCC regulation

- The certification and filing deadline to become registered in FCC's Robocall Mitigation Database (RMD) was **June 30th, 2021**
- Initially from September 28th, 2021 the US transit carriers were supposed to accept traffic only from foreign Transit Service Providers (TSP) for CLI belonging to North American Numbering Plan (NANP) that appear in the FCC's RMD (see Note)
- Possible incremental steps to comply with FCC regulation may be realized:
 - 1. By delivering to US operators retail traffic collected by directly connected domestic operators on **separate trunks** provided that this traffic is intended to be checked for **robocall mitigation** (i.e. robocall mitigation program requirements are met)
 - 2. By using **delegated certificates** to sign calls, US carriers can verify the authenticity of CLIs that can be guaranteed, and both accept incoming calls with CLI = NANP and transfer calls with 'Attestation = A' to be presented as 'trustable and verified CLI' to the Callee. This solution requires STIR support in the network.
 - 3. By adopting **STIR/MIXER approach**. The GSMA is preparing a key management procedure to exchange key material between GSMA members to extend trust to other secure domains like FCC governed STIR/SHAKEN.
 - 4. By deploying i3Forum **CLI Safe Zone** initiative, so that once call enters the "safe zone" CLI is certified and it is transferred unaltered to final destination. This solution require STIR extension support in the network



Note

FCC Fifth Further Notice released on Oct. 1st suspended this prohibition up to when a decision will be taken on how to treat foreign originated traffic



i³ forun



Building The International CLI Safe Zone

Component of an End-to-End Industry Solution



- CLI Spoofing is a major cause of concern for international wholesale providers
- Fraudsters manipulate CLI to carry out malicious robocalling marketing campaigns, SCAM calls, and implement OBR and bypass frauds (leveraging international call flows)
- Domestic operators and regulatory authorities are focusing on national solutions and implementations targeting robocalling and SCAM calls (i.e. STIR/SHAKEN)
- The i3forum focuses on the international carrier domain & fighting CLI Spoofing through carrier collaboration
- Our goal is to prevent, detect, and mitigate against CLI spoofing and manipulation throughout all international interconnections
- Our approach is to build and gradually extend a global Safe Zone where CLI is secured by participating international wholesale providers
- Once a call enters our trusted domain, CLI is protected and the carrier space secured (CLI confirmed)
- Eventually the International CLI Safe Zone will interwork with domestic solutions creating an end-to-end trusted domain



i³ forum

Do you want to learn more?

- i3forum's «FCC Robocalls Order: Impacts on International Voice Traffic to USA» Rel. 1.0 provides the i3 forum's perspective on FCC robocalls order issued in 2020 impacting international voice traffic directed to USA
- Report available at:

https://i3forum.org/blog/2021/06/15/fcc-robocallsorder/

 i3forum's Technology and Fight against Frauds WGs are actively investigating robocalling and CLI spoofing through the collaboration with main standard bodies, industry associations and regulators INTERNATIONAL INTERCONNECTION FORUM FOR SERVICES OVER IP (13 FORUM) (www.i3torum.org) Source: Working Group "Technology" i3 forum keyword: Voice, Robocall, Spoofing, CLI FCC Robocalls Order: Impacts on International Voice Traffic to USA

(Release 1.0) June 2021 This document provides the i3 forum's perspective on FCC robocalls order issued in 2020 impacting international voice traffic directed to USA.

The scope includes the description of FCC order sections affecting voice traffic generated outside USA, timing and filing requirements set by regulation and actions required by wholesale operators to continue delivering traffic towards USA fixed and mobile subscribers. It also describes possible enhancements that could be adopted by not US based operators in order to protect voice calling party identity from being tampered or manipulated along the call path, with the aim to deliver to end subscribers voice calls with calling identity 'certified' and trusted.

It does not intend to duplicate other existing specifications or documents on the same issue, but to complement these documents with the perspective of the International Carrier members of i3forum.





i³ forum Thank you

www.i3forum.org

Separated trunks for trusted traffic

- As an alternative to combat spamming traffic delivered in the US via international path, the proposition is to classify retail originated traffic (which includes both US roaming subscribers and retail home subscribers) as <trusted> when delivered by International Carriers
- Retail traffic will be separated and delivered by International Carriers on dedicated trunks enabled with the US Operators
- Robocall mitigation checks will be performed on retail traffic





i³ forui



© i3froum | 2021

Developments in GSMA – STIR/MIXER



Path 2: "x5u" URL points to IR.21 service at IP-NNI edge (a "trust proxy")

