INTERNATIONAL INTERCONNECTION FORUM

FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.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.

Table of Contents

1. Scope and objective of the document

The goal of this document is to provide a common understanding, by the international carrier community and for the international carrier community, into the FCC's robocalling regulations and their impact on international carriers managing voice traffic terminating to the US. Our intent is to clear up any confusion and highlight any issues that are critical and meaningful to international carriers. This paper should provide a reference for international carriers describing what the regulations are and why they are important to us (central reference point describing what it is and why it's important from the perspective of international carriers).

This document is not intended to provide specific directions, actions, or guidance for international carriers in terms of compliancy issues or questions regarding FCC regulations or mandates. Each carrier should work closely with their legal departments in terms of compliancy issues and or questions.

2. Symbols and Acronyms

ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CLI	Calling Line Identification
CNAM	Caller NAMe
CVT	Call Validation Treatment
FCC	Federal Communications Commission
RMD	Robocall Mitigation Database
NANP	North American Numbering Plan
SHAKEN	Signature-based Handling of Asserted information using toKENs
STIR	Secure Telephone Identity Revised
TRACED	Telephone Robocall Abuse Criminal Enforcement and Deterrence

3. References

[1] FCC, Second Report and Order, October 2020.
Available at: https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf

[2] FCC, Caller ID Authentication Best Practices, December 2020.
Available at: https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf

[3] ATIS, Robocalling and Communication ID Spoofing Whitepaper, February 2021.
Available at: https://access.atis.org/apps/group_public/download.php/57909/ATIS-I-0000081.pdf

[4] FCC, Opening of Robocall Mitigation Database, filing istructions and deadlines, April 2021.
Available at: https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf

[5] i3forum, Calling Line Identification (CLI) spoofing, Rel. 1.0, October 2020.
Available at: https://i3forum.org/blog/2020/11/04/i3forum-calling-line-identification-cli-spoofing-report/

4. Introduction

In 2019 the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) was issued by US Congress. This bill implemented a forfeiture penalty for violations of the prohibition on certain robocalls (see [5] par. 5.3.2 for Robocalling definition). It also required voice service providers to develop call authentication technologies and FCC to promulgate rules establishing when a provider may block a voice call based on information provided by the call authentication framework.

In 2020 FCC issued the Second Report and Order on Call Authentication [1] affecting all US domestic voice traffic as well as foreign generated voice traffic with calling identity belonging to portions of the North American Numbering Plan (NANP) that pertain to the US. For international wholesale operators the latter includes two main traffic use cases:

1. US subscriber roaming abroad; in this case calls are generated in the visited network (2G/3G coverage or CS fallback) with calling identity belonging to USA numbering plan
2. US call center with overseas remote location; in this case calls are generated with calling identity belonging to USA numbering plan

The goal of such regulation is to combat robocalling by being able to identify the real source of illegal traffic thanks to call authentication technologies. Should these technologies not be available on a specific source provider, robocall mitigation program adopted by the provider, together with the collaboration of the intermediate and terminating providers to traceback illegal calls along the call path, will lead to identify the real source of robocalls, so that proper actions will follow immediately after.

Section 5 of this document describes how FCC Second Report and Order on Call authentication affects foreign originated voice traffic, while Section 6 provides timing and filing instruction for Robocall Mitigation Database (RMD) registration according to FCC Public Notice announcing its establishment [4].

Section 7 provides information for wholesale operators on how to deliver traffic directed to USA through terminating US operators after the deadlines set by FCC. Actions required to international wholesale operators are based both on the analysis of FCC regulation as well as on the feedback i3forum directly received by two major terminating US operators. The fundamental change of international wholesale operator liability driven by FCC regulation is depicted in Section 8.

Finally Section 9 describes some medium/long-term enhancements that could be adopted by operators (separated trunks, delegated certificates, STIR/MIXER and CLI Safe Zone) in order to increase the attestation level of voice traffic classified as “trusted” by originating operator.

5. FCC regulation and foreign voice traffic

In FCC Second Report and Order on Call Authentication a foreign voice service provider is defined as “any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country” (see [1], par. 92).

The FCC requires all voice service providers to implement STIR/SHAKEN framework as call authentication technology on their IP portion of network (STIR/SHAKEN works only on IP networks) by June 30, 2021. A service provider may obtain an extension of the deadline, but during the extension period it must apply a robocall mitigation program or apply an alternative method that has the purpose of protecting users from unauthenticated calls. It is important to be registered in the RMD, since the commission “prohibit intermediate providers

and terminating voice service providers from accepting voice traffic directly from any voice service provider that does not appear in the database" (see [1], par. 86).

These rules also apply to foreign voice service providers that use portions of NANP that pertain to the United States to send voice traffic to residential and business subscribers in the United States. This means that foreign voice service providers must follow the same certification requirements as domestic voice service providers in order to be listed in the database. In particular, to be listed in the database, these providers must certify either that they have implemented STIR/SHAKEN or comply with the robocall mitigation program requirements outlined above by "tak[ing] reasonable steps to avoid originating illegal robocall traffic and committing to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls" (see [1], par. 86, 92).

6. Timing and filing requirements

FCC issued a Public Notice announcing the establishment of the Robocall Mitigation Database (RMD) portal for certifications regarding robocall mitigation programs and providing guidance on filing procedures [4].

The portal is available at: https://fccprod.servicenowservices.com/rmd?id=rmd_welcome.

The deadline to file certifications is *June 30, 2021*. From *September 28, 2021* intermediate and terminating voice service providers must only accept traffic from providers that appear in the FCC's certification database.

7. Actions required to international wholesale operators

Even though FCC regulation applies only to voice traffic originated abroad with calling identity belonging to USA numbering plan, terminating operators in USA may require their interconnected partners to register into the Robocall Mitigation Database (RMD) in order to continue delivering any international voice traffic to US fixed and mobile subscribers. According to the feedback received by two major terminating US operators the reason behind this is that operators might not be able to discriminate or policy voice traffic based on the calling identity when traffic subject to FCC regulation (e.g. call generated by US outbound roamers) is mixed up with other international traffic.

Therefore international wholesale operators that wish to continue delivering voice traffic directed to USA through any terminating US operator are supposed to register into the RMD as intermediate providers. By registering into the RMD, operators accept the "terms & conditions" set by FCC. In particular, should any robocall complaint involve their network, they accept:

- to collaborate to the traceback activity in order to identify source of illegal traffic
- to stop delivering traffic received from their interconnected partner identified as sender of illegal traffic

Each international wholesale operator has to check binding legal obligations behind RMD registration and take proper action towards its customer operators.

Should the international wholesale operator decide to register into RMD so as to continue delivering traffic to USA after deadlines set by FCC, there are alternative mechanisms that could be adopted in the mid-long term in order to improve the attestation level of calls directed to USA, even without being part of STIR/SHAKEN framework (see Section 9).

8. FCC regulation and fundamental change of carrier liability

The main purpose of the FCC TRACED Act is to provoke a paradigm shift in carrier liability. In previous years, the US government (legislators/regulators) has made combating illegal robocalls a top consumer protection priority. Therefore, the new rulings include means to provide the FCC with the legal means to traceback hostile sources of traffic and impose fines. Consequently, foreign carriers must also commit to cooperating with the FCC, US law enforcement, and the Industry Traceback Consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls. For international voice traffic, foreign carriers will also become part of these rulings and the registrations in FCC's RMD should be understood in part as a waiver for US intermediate and terminating carriers to accept traffic from foreign carriers using US numbering resources. Implicitly, it becomes the responsibility of the foreign carrier to justify the use of their service for the transfer of legitimate calls to the US. In case of illegal robocalls and possibly including privacy violations, the foreign carrier will be contested by the FCC, with the ultimate result that US intermediate and terminating carriers will be forced to block all inbound US traffic from such foreign carrier. This is a fundamental change from current practices, as this traceback makes the originator of the traffic liable for providing services to hostile traffic sources.

9. Possible enhancements to deliver international calls to USA

FCC Public Notice on Caller ID Best Practices [3] includes the possibility to manage international voice traffic with alternative mechanisms aiming to assist with interoperability when STIR/SHAKEN is not available. Adoption of these mechanisms could lead to apply A attestation level to calls whose caller identity is classified as "trusted" by originating operator. The basic assumption is that there is a high level of trustworthiness between terminating US provider and its international partners.

It follows that there are some enhancements that could increase effectiveness, efficiency and scalability of the solution. These could be progressively adopted by operators in order to increase the attestation level of selected voice traffic.

9.1. Separated trunks

As a potential medium-term solution to combat Robocall traffic delivered in the USA via international path, the proposition is to classify retail originated traffic (which includes voice traffic generated by US subscribers roaming abroad as well as retail home subscribers) as 'trusted' when delivered by the international carrier that directly collects traffic from the retail operator.

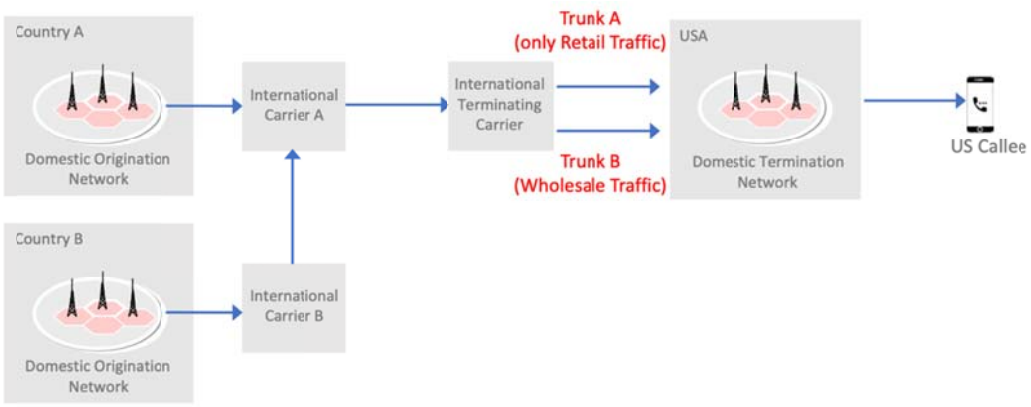

Fig. 1 – Separated trunks for the delivery of "trusted" traffic

It is of utmost importance that retail traffic that is placed in separated trunks is "true originated traffic" i.e. coming from the radio network. Such traffic can be candidate for A attestation traffic (see [3], par. 3.2 for attestation levels definition). Traceback is supported by having the retail operator directly connected to international carrier delivering traffic to US operators (no intermediate hops). Registration in the RMD is still requested.

9.2. Delegated certificates

Delegated certificates solution focuses on an entity within the FCC governed framework, "the delegator", to delegate its certificates to an entity outside the FCC governed framework, the "delegatee".

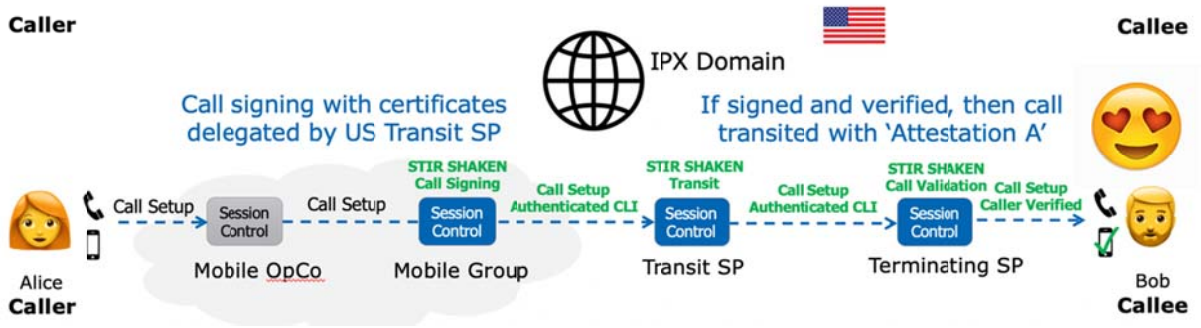

Fig. 2 – Call setup with Delegated Certificates

There needs to be a high level of trust between the two entities. This solution is traceback compliant, but the delegator will always be held responsible for the behaviour of the delegatee by the FCC.

9.3. STIR/MIXER and CLI Safe Zone

The STIR/MIXER solution is a proposal to interconnect the GSMA secure domain (to be created) with the FCC governed STIR/SHAKEN domain. The idea is that both domains make their public key certificates available to each other and that there is bilateral trust between the issuers (roots) of both certificates. GSMA members would than only deal with GSMA procedures to obtain certificates. Traceback and obtaining the right attestation for calls is blended in this solution.

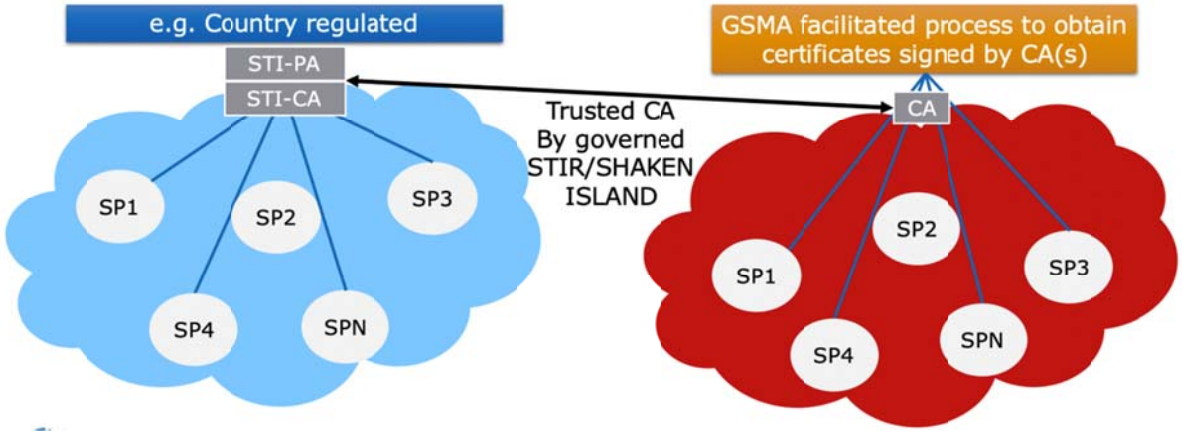

Fig. 3 – Trusted domains and CA

The CLI Safe Zone is an i3forum proposal to create a bubble within the international voice carrier community where the calling identity is guaranteed to the be authentic. When the call leaves the safe zone at the carrier on the USA edge A attestation level can be applied.

Fig. 4 – CLI Safe Zone concept

This will be possible thanks to the creation of a secure domain among international carriers involving their directly connected retail operators. The basic assumption is that the secure domain and FCC domain will make their public key certificates available to each other and there is bilateral trust between the issuers (roots) of both certificates.