

Telecom Business Network ROBOCALL MITIGATION PROGRAM

Below is the Robocall Mitigation Plan filing for Telecom Business Network. This plan will be submitted to the FCC's Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices.

Monitoring

Telecom Business Network has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

If Telecom Business Network detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. and take appropriate action.

Appropriate action may include:

- Validating that the originating party is authorized to use the TN.
- Suspending calling party's ability to originate, route, or terminate calls on Telecom Business Network.

Traceback Cooperation

Telecom Business Network commits to responding in a timely manner and supporting all traceback requests from the FCC, law enforcement, and the [Industry Traceback Group \(ITG\)](#).

Robocall Mitigation Solution Overview

- General information
 - Robocall scoring is based on the annual +100B carrier calls that processes FraudCentral.io as part of the Caller Name service.
 - STIR/SHAKEN Transaction Detail Records (TDRs) are now being added as an additional data source.
 - Each call is assessed through the Fraudcentral.io model, leading to constantly refreshed view of call behavior and probability of a given number currently being used for robocalling.
 - Active numbers are assessed by the model for behavioral attributes typically associated with robocalling including:
 - Neighbor spoofing events
 - Sudden spikes in volume, such as driven by call spoofing
 - Do-Not-Originate (DNO) numbers are also deemed to be robocalls if they are the calling party number. This is sourced from industry (e.g., US Telecom) and directly from enterprises.
 - The service covers both US domestic and international TNs.

- Calls originating from your network (i.e., Robocall Protection)
 - Provides detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the calling number is invalid, unallocated, on a Do-Not-Originate list.
 - If the platform detects a suspected robocalling patterns Telecom Business Network will take appropriate action which may include suspending or terminating the subscriber.
 - Supports a real time query to service to determine if a number originating on your network could be a robocall. Such calls can be blocked, or the terminating party can be notified via CNAM.
 - For each new instance of robocalling using the Operating Service Provider (OSP)TNs, an alert is sent to the OSP in near real time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM , through an overlay such as “ROBOCALLER”. The CNAM alerting helps address instances of spoofing of TNs that are not going through the OSP that owns the number.

- Termination (i.e., Robocall Mitigation)
 - Supports a real-time query to service to determine if a number terminating on your network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (i.e., all Communications Service Providers (CSPs)that do not have STIR/SHAKEN and all CSPs *with* STIR/SHAKEN, but who do not have a direct and vetted end user relationship.)
 - Such calls can be blocked or the called party can be notified via CNAM.