

Robocall Mitigation Program for TELEPATH COMMUNICATIONS CORPORATION

Overview of the Mitigation Plan

TELEPATH COMMUNICATIONS CORPORATION has developed a comprehensive Robocall Mitigation Plan, which will be submitted to the FCC's Robocall Mitigation Database. Our plan is dynamic, allowing for adjustments in response to evolving laws, regulations, and industry best practices.

Active Monitoring and Reporting

Our system is designed to scrutinize high-volume traffic across our voice network, pinpointing patterns indicative of robocalls. We employ monitoring tools that alert us to unusual call patterns, traffic spikes, or the use of non-validated Telephone Numbers (TNs), which are often telltale signs of illegal robocalls.

In instances where illegal robocalls are suspected, or if there is any indication of illegal robocalling or spoofing activities, we undertake thorough investigations. Our actions include:

Confirming the legitimacy of the originating party's use of the TN.

Temporarily or permanently disabling the calling party's ability to initiate, route, or terminate calls on our network, if necessary.

Collaboration on Traceback Requests

We pledge to promptly respond and provide full cooperation for traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG).

Cross-Referencing: Verify calling numbers against:

- The FCC consumer complaint database.
- The Do Not Originate (DNO) list.

Alert Generation: Automatically trigger alerts for any of the following:

- Invalid or unallocated calling numbers.
- Numbers listed on a DNO list.
- Numbers flagged in the FCC consumer complaint database.

Action: Confirm whether the caller attempted to originate unlawful robocalls and respond accordingly by issuing warnings or terminating service.

Compliance Review: Regularly evaluate the system and reporting criteria to ensure alignment with current FCC regulations.

General Information:

Robocall scoring based on over 100 billion carrier calls processed annually as part of the Caller Name service.

Incorporation of STIR/SHAKEN Transaction Detail Records (TDRs) as an additional data source.

Continuous assessment of each call through our model, updating the likelihood of a number being used for robocalling.

Focus on identifying attributes like neighbor spoofing and unexpected call volume spikes.

Inclusion of Do-Not-Originate (DNO) numbers sourced from the industry and enterprises.

Calls Originating from Our Network (Robocall Protection):

Detailed reports identifying suspected illegal robocalls.

Real-time service queries to determine if an originating number could be involved in robocalling, with options to block such calls or alert the recipient.

Immediate alerts to the Operating Service Provider (OSP) for new instances of robocalling using OSP TNs.

Call Termination

Real-time service queries to ascertain if an incoming call could be a robocall, offering protection to our subscribers from unverified sources.

Options to block such calls or inform the recipient through CNAM notifications.

Our approach aims to robustly safeguard both our network and our customers from the risks associated with illegal robocalls, while adhering to the latest industry standards and regulations.