

TELE-DATA COMMUNICATIONS CORPORATION

ROBOCALL MITIGATION PROGRAM

Below is the Robocall Mitigation Plan filing for TELE-DATA COMMUNICATIONS CORPORATION. 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

We monitor and analyze high-volume voice network traffic to detect and identify patterns associated with robocalls. Our systems generate alerts for unusual spikes, irregular traffic patterns, or the use of non-validated Telephone Numbers (TNs), helping to identify potential illegal robocall activity.

If we detect patterns indicative of illegal robocalls or suspect that illegal robocalling or spoofing is occurring on our network, we take steps to identify the responsible party. This includes investigating those using our network to originate, route, or terminate such calls.

Depending on the findings, appropriate actions may include:

- Verifying that the originating party is authorized to use the TN.
- Suspending the party's ability to originate, route, or terminate calls on the IT Pros of MS LLC network.

Traceback Cooperation

TELE-DATA COMMUNICATIONS CORPORATION commits to responding in a timely manner and supporting all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG). We have an expert Network Operations Center (NOC). Our NOC team will respond to Tracebacks within 24 hours.

General information

1. Robocall scoring leverages the analysis of +100B annual carrier calls processed by Bulk Solutions as part of its Caller Name service.
2. STIR/SHAKEN Transaction Detail Records (TDRs) are now integrated as an additional data source to enhance analysis.
3. Each call is evaluated using the Bulk Solutions model, providing a continuously updated view of call behavior and assessing the likelihood that a given number is being used for robocalling.
4. Do-Not-Originate (DNO) numbers, sourced from industry organizations (e.g., US Telecom) and directly from enterprises, are flagged as robocalls if they appear as the calling party number.

5. Termination services include a real-time query feature to identify whether a number terminating on the network may be a robocall. This safeguards subscribers from calls originating from networks that cannot provide authoritative caller attestation, including Communication Service Providers (CSPs) without STIR/SHAKEN or those with STIR/SHAKEN who lack a verified end-user relationship. Such calls can be blocked or flagged to notify the called party.