

SOTEK SOLUTIONS'S ROBOCALL MITIGATION PROGRAM 2024-2025

DESCRIPTION OF ROBOCALL MITIGATION PROGRAM

As part of SOTEK Solutions' submission to the Robocall Mitigation Database, this document outlines the steps SOTEK has taken to avoid originating illegal robocall traffic and comply with FCC regulations.

SOTEK collaborates with its upstream service provider, Vitelity, which has fully implemented the STIR/SHAKEN authentication framework and operates a comprehensive robocall mitigation program. We are committed to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

I. Efforts to Avoid Originating Illegal Robocalls

SOTEK leverages the capabilities of its upstream provider, Vitelity, to mitigate the risk of illegal robocalls. Vitelity has made substantial investments in network upgrades and advanced systems to combat illegal robocalls. These systems include:

- **Call Analytics and Monitoring:** Statistical measures such as average call duration, Answer Seize Ratio (ASR), and call volume are used to detect and flag suspicious call traffic.
- **Randomizer for Least Cost Routing (LCR):** For customer traffic routed via LCR, a random number authentication system prevents calls from proceeding unless two randomly generated digits are entered correctly by the calling party, effectively blocking machine-generated calls.
- **Automatic Number Identification (ANI) Management:** Originating telephone numbers exhibiting abusive behavior, such as repeated failed attempts, are identified and blocked.
- **Proactive Blocking Measures:** Calls from phone numbers on Do-Not-Originate (DNO) lists, such as those maintained by US Telecom and Neustar, are proactively blocked.

Through the analysis of Call Detail Records (CDRs), industry fraud notifications, and third-party reports, Vitelity identifies and mitigates potential unlawful robocalling.

II. SOTEK's Know Your Customer (KYC) Program

SOTEK is committed to a robust Know Your Customer (KYC) process for all new and existing customers. This program includes:

- Verifying customer identities and their intended use cases for phone system services.
- Monitoring customer traffic patterns to identify and address potential misuse.

- Ensuring customers understand and comply with legal and ethical standards for call origination.

These measures prevent SOTEK from being used, intentionally or unintentionally, for illegal or spoofed call traffic.

III. Commitment to Responding to Traceback Requests

SOTEK remains fully committed to cooperating with the Commission, law enforcement, and the industry traceback consortium by:

- Responding to all traceback requests within 24 hours.
 - Providing all requested information necessary to identify and stop illegal robocallers.
 - Taking corrective action as needed to address misuse of our services by customers.
-

Conclusion

By partnering with Vitelity's robust mitigation program and implementing a proactive KYC process, SOTEK Solutions ensures compliance with FCC requirements and actively contributes to the prevention of illegal robocalls.