

CTS Technology Solutions, LLC

Robocall Mitigation Policy

Last updated 12/16/2024

1. Establish Compliance Policies

- **Review and Understand Regulations:** CTS staff will familiarize themselves with the TRACED Act, the FCC's rules, and industry standards (e.g., STIR/SHAKEN). Personnel are to understand the requirement for STIR/SHAKEN implementation for all voice service providers & conduct ongoing continuing education for new regulations.
- **Develop Anti-Robocall Policy:** CTS has drafted this policy for robocall mitigation that includes guidelines for identifying and blocking robocalls, compliance with Do Not Call (DNC) lists, and the implementation of call authentication protocols.

2. Set Up STIR/SHAKEN Implementation

- **Work with Tier 1 Providers:** Collaborate with all our upstream Tier 1 carriers to ensure STIR/SHAKEN is enabled for call authentication.
- **Verify Call Authentication:** Ensure that the calls from our customers are authenticated with a secure signature to prevent fraudulent calls. This includes implementing measures to reject calls that fail STIR/SHAKEN verification.
- **Monitor Compliance:** Regularly check if calls are being passed with valid STIR/SHAKEN tokens. Ensure that calls from our customers are properly signed with appropriate attestation levels.

3. Robocall Detection Systems

- **Implement Call Monitoring Tools:** Utilize monitoring tools and call analytics to detect patterns typical of robocalls (e.g., high-volume calling, short-duration calls, invalid numbers).
- **Block Suspicious Traffic:** Set up systems to automatically block or flag suspicious calls, including those originating from suspicious or invalid phone numbers, based on defined risk thresholds.
- **Track Complaints and Reports:** Continuously monitor complaints about robocalls, either from our customers or external sources (e.g., the FCC), and take corrective actions as necessary.

4. Proactive Customer Management

- **Verify Customer Legitimacy:** Before onboarding new customers, CTS will perform a background check to ensure they are legitimate businesses and do not have a history of engaging in illegal robocalling practices.

- **Customer Education:** Educate our customers about the importance of complying with robocall mitigation rules. Provide guidelines on legal robocalling (e.g., with consent and appropriate registration) and penalties for violations.
- **Monitor Customer Usage:** Set up monitoring systems to track calling patterns of individual customers. Look out for signs of potential abuse or suspicious calling behavior that could indicate robocalling.

5. Collaboration with Industry Partners

- **Participate in Industry Databases:** Work with industry databases such as the Robocall Mitigation Database (RMD) and share information about our mitigation efforts. This can help you maintain visibility and credibility as a responsible reseller.
- **Cooperate with Law Enforcement:** In the event that any of our customers are found to be engaging in illegal robocalling, CTS will cooperate with law enforcement agencies or regulatory bodies to address the issue.

6. Customer Access to Robocall Mitigation Solutions

- **Offer Call Blocking and Filtering Solutions:** Provide our customers with tools and services to filter robocalls and block unwanted calls. For example, offer services that block spam or fraudulent calls before they reach the customer.
- **Assist with Do-Not-Call List Compliance:** Ensure our customers are aware of the National Do Not Call Registry and provide tools to comply with DNC regulations to prevent unwanted robocalls.

7. Audit and Reporting

- **Regular Audits of Traffic:** Conduct regular internal audits of traffic patterns to ensure there are no signs of abusive or fraudulent activity. CTS will evaluate the effectiveness of our mitigation strategies.
- **Report Mitigation Efforts:** Provide periodic reports on our mitigation activities to regulatory bodies, our upstream providers, and any customers as required. CTS will keep thorough records of actions taken to mitigate robocalls.

8. Take Corrective Action When Necessary

- **Investigate Complaints:** When receiving a complaint about robocalls originating from our network, CTS will investigate the issue thoroughly. If a customer is found to be at fault, CTS will warn them or take corrective action, such as suspending service.
- **Terminate Service for Non-Compliance:** If a customer repeatedly violates robocall regulations, CTS will consider terminating service as a last resort. This will only be done if all other attempts to resolve the issue have failed.