

Robocall Mitigation Plan for 210 IT

Overview:

At 210 IT, we are committed to combating illegal robocall traffic and ensuring compliance with regulatory obligations. As part of our robocall mitigation program, we have implemented specific measures to prevent the origination, carrying, or processing of illegal robocall traffic. This plan outlines the reasonable steps we have taken, in collaboration with our SIP Trunk provider, to effectively mitigate robocall threats.

Compliance with Regulatory Obligations:

210 IT acknowledges and adheres to existing filers' prior obligations regarding robocall mitigation. We recognize the importance of complying with regulatory standards and ensuring that our communications services align with all relevant laws and regulations.

Know Your Customer (KYC):

At 210 IT, we prioritize caller identity verification and operational legitimacy. Here's how we ensure a secure communication environment:

- **Subscriber Vetting and Caller Identity Validation:**
 - We collect and review entity-identifying information to establish an authenticated relationship with our customers.
 - Our goal is to determine whether a customer is subject to any enforcement actions that restrict their calling capabilities (e.g., bans on telemarketing calls).
 - Whenever possible, we validate the legitimacy of the entity's asserted calling numbers.
- **Contractual Provisions:**
 - Our contractual agreements explicitly prohibit customers from initiating illegal robocalls.
 - If we detect suspicious robocall activity, we issue warnings to the customer.
 - Persistent violation of our policies may result in service termination.

New Customer Screening:

210 IT follows a direct sales process for new customers, which include:

- **Business Verification:** We verify business activity, physical location, and creditworthiness for every customer.
- **Geographic Focus:** All our customers are located in the United States and Canada.
- **Tier 1 Carriers:** We port existing numbers to and from Tier 1 carriers, ensuring robust mitigation strategies.

Active Customers

For all our active customers:

- **Device Control:** Only registered devices are permitted for use with our services.
- **Rate Limit and Alarms:** Each customer operates within a rate limit. If a customer's concurrent call limit is reached, alarms are triggered to ensure smooth operations.

Implementation of STIR/SHAKEN:

210 IT utilizes Bandwidth as our SIP Trunk provider, which fully implement the STIR/SHAKEN framework. STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using toKENs) is a set of protocols designed to combat illegal robocalls by verifying the authenticity of caller information.

Bandwidth Configuration:

In close collaboration with our SIP Trunk provider, we enable the following features for all 210 IT customers in the Bandwidth Portal to enhance our robocall mitigation efforts:

- **STIR/SHAKEN Inbound Verification Results:** This feature allows us to verify the authenticity of inbound calls using STIR/SHAKEN protocols, significantly reducing the risk of illegal robocalls.
- **Inbound Parameters Enhanced Verification Status:** By closely monitoring and analyzing inbound call parameters, we ensure an enhanced verification status. This capability enables us to promptly detect and mitigate suspicious call activity.

- **Transit Identity Header Service:** Our service provides essential information about call transit identity, empowering us to identify and proactively block suspicious calls.

Conclusion:

At 210 IT, we are committed in our dedication to protect our clients from unsolicited and fraudulent calls by taking proactive measures against the threat of illegal robocalls. By employing STIR/SHAKEN protocols and leveraging Bandwidth's functionalities, we uphold regulatory compliance while delivering a reliable and secure communication experience.

This Robocall Mitigation Plan reflects our dedication to upholding the integrity of our services and ensuring peace of mind for our valued customers.
