

Fortress IT Solution LLC Robocall Mitigation Policy

I. Purpose and Objective

This Robocall Mitigation Policy (RMP) outlines the comprehensive strategies and procedures implemented by Fortress IT Solution LLC to prevent, detect, and mitigate illegal and unwanted robocalls originating from or traversing its networks. This policy is established in compliance with the Federal Communications Commission's (FCC) mandates, particularly those related to the Robocall Mitigation Database (RMDb) and STIR/SHAKEN caller ID authentication framework. The primary objective is to protect consumers from fraudulent and abusive calls, maintain the integrity of telecommunications networks, and ensure Fortress IT Solution LLC's continuous compliance with all applicable FCC regulations.

II. Scope

This policy applies to all voice services provided by Fortress IT Solution LLC, including those where Fortress IT Solution LLC acts as a Voice Service Provider (VSP), as defined by the FCC. This encompasses any service interconnected with the Public Switched Telephone Network (PSTN) that furnishes real-time, two-way voice communications to an end-user using North American Numbering Plan (NANP) resources, as well as the carrying or processing of traffic that traverses the PSTN.

III. Policy Statements and Procedures

Fortress IT Solution LLC is committed to implementing and maintaining robust robocall mitigation practices, which include, but are not limited to, the following:

A. STIR/SHAKEN Implementation and Attestation Strategy

Fortress IT Solution LLC recognizes the critical role of STIR/SHAKEN in combating caller ID spoofing and illegal robocalls.

- **OUR SERVICE PROVIDER VOIP.MS currently signs all our calls and has fully implemented the STIR/SHAKEN protocol.**

B. Customer Vetting Practices

Fortress IT Solution LLC implements rigorous customer vetting practices to prevent or minimize the origination of illegal robocalls through its voice services.

1. **Identity Confirmation:** The vetting process aims to confirm the legitimacy of all voice service subscribers (residential or business/commercial) by collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.
2. **Ongoing Vetting:** Vetting occurs throughout the service provisioning process, including appropriately sizing facilities to claimed intended use, executing required service agreements, and granting telephone number resources.
3. **Contractual Obligations:** All service agreements and acceptable use policies explicitly state that services should not be used for illegal robocalls or deceptive/fraudulent activity. Fortress IT Solution LLC reserves the authority to suspend or terminate voice service for violations of these terms.

C. Telephone Number Validation

Fortress IT Solution LLC has established procedures to confirm the calling customer's right to use a telephone number in connection with their subscribed voice service(s).

1. **Authorized Usage:** A subscriber is permitted to use a telephone number as their caller identity only if the number is directly managed by Fortress IT Solution LLC or obtained via an underlying partner.
2. **Screening Mechanisms:** For single-line voice service subscribers, switching equipment is configured to accept calls only from the number assigned to that subscriber. For multi-line telephone systems, Fortress IT Solution LLC screens all originating calls to ensure the originating number matches one of the numbers assigned to the subscriber.

D. Traceback Cooperation

Fortress IT Solution LLC is committed to prompt and full cooperation with the FCC, law enforcement agencies, and the Industry Traceback Group (ITG) on all traceback requests and investigations.

1. **Dedicated Resources:** Sufficient resources are dedicated to promptly complete and provide responses to all traceback requests, ideally within 24 hours of receipt.
2. **Single Point of Contact:** A single point of contact for receiving all traceback requests is identified and documented.
3. **Contractual Requirements:** Fortress IT Solution LLC incorporates language in its carrier interconnection and service agreements requiring traceback cooperation from all parties involved in voice service calls exchanged, specifically requiring parties to promptly identify the upstream provider or originating customer of a suspected illegal robocall.

E. Network Monitoring and Analytics

Fortress IT Solution LLC continuously monitors network usage and examines Call Detail Records (CDRs) to identify suspicious call activity or patterns indicative of illegal robocalls.

1. **Key Indicators:** Particular attention is given to:
 - Higher than normal subscriber traffic volume, including large bursts or inconsistent volumes.
 - Originating calls of short duration and low call completion percentages.
 - Originating calls with sequential called number dialing patterns.
 - Repeated calls to Do Not Call Registry numbers or invalid numbers.
 - Calls to unassigned or unallocated NPA-NXXs.
2. **Advanced Analytics:** Fortress IT Solution LLC leverages advanced call analytics systems, including real-time dynamic traffic analysis (SIP Analytics), to identify and mitigate robocalls at origination. This includes the use of blacklisting/whitelisting, CAPTCHA gateway services, and phone number reputation lookup.
3. **Third-Party Vendors:** The use of third-party analytics vendors, such as TransNexus, for "Telecom Fraud Prevention" and "Robocall and Telephone Denial of Service (TDoS) Prevention" services, is detailed within the RMP.

F. Call Blocking Mechanisms

Fortress IT Solution LLC implements effective mechanisms for blocking illegal traffic.

1. **Prohibited Calls:** This includes blocking calls from unassigned, unallocated, or invalid numbers, as well as calls from numbers on the Do Not Originate list, as permitted by FCC rules.
2. **Analytics-Informed Blocking:** The determination of which traffic to block is informed by internal analytics systems, third-party analytics vendors, and directives from authorities.
3. **Screening and Diversion:** When a call is identified by a blacklisted attribute, it can either be blocked outright or diverted to a CAPTCHA gateway for Interactive-Voice-Response screening to block calls placed by autodialers.

G. Know Your Upstream Provider Procedures

As an Intermediate Provider, Fortress IT Solution LLC maintains a detailed "know-their-upstream-provider program."

1. **Assessment and Assurance:** This program outlines procedures for assessing and ensuring that any upstream providers are equally committed to monitoring their networks and preventing the transmission of illegal robocalls.
2. **Contractual Language:** Robocall prevention language is incorporated into contracts with upstream provider entities.
3. **Documentation:** The RMP lists current immediate upstream providers along with their contact information.

H. International Call Originators

If Fortress IT Solution LLC is not currently an international voice services provider, its RMP explicitly states this. If it begins selling services to international call originators using North American Numbering Plan resources in the future, it commits to developing best practices for vetting such customers and performing telephone number validation on all international originated calls. Foreign providers sending traffic with U.S. numbers in the caller ID directly to U.S. gateways are required to file in the RMDB to avoid having their calls blocked.

IV. Compliance and Enforcement

Fortress IT Solution LLC is committed to maintaining continuous compliance with all FCC RMDB requirements.

1. **FCC Registration Number (FRN) and CORES:** Fortress IT Solution LLC will maintain an active FCC Registration Number (FRN) via the Commission Registration System (CORES). All information submitted to CORES will be kept current and updated within 10 business days of any changes.
2. **RMDB Account and Certification:** An account will be maintained on the FCC's Robocall Mitigation Database website, and all required certifications will be submitted, including the status of STIR/SHAKEN implementation and the comprehensive Robocall Mitigation Plan.
3. **Annual Recertification and Fees:** Fortress IT Solution LLC will recertify annually to the accuracy of its company's information in the RMDB on or before March 1st of each year, accompanied by the required filing fee.
4. **Timely Updates:** Any changes to information submitted directly in the RMDB will be updated within 10 business days.
5. **Consequences of Non-Compliance:** Fortress IT Solution LLC understands that non-compliance can lead to severe repercussions, including mandatory blocking of traffic by other carriers and substantial financial penalties.
6. **Security Measures:** Fortress IT Solution LLC will implement multi-factor authentication for accessing the RMDB as required by the FCC.

V. Policy Review and Updates

This Robocall Mitigation Policy is a living document and will be reviewed and updated regularly to ensure its continued effectiveness and alignment with evolving FCC regulations, industry best practices, and Fortress IT Solution LLC's operational changes.

VI. Point of Contact & Other Contact Information

Fortress IT Solution LLC Point of Contact:

Jonathan D. Madeira
107 Highland Road
Hershey, PA 17033
jonathan@fortressitsolution.com
(717) 500-6265 (main)
(717) 856-1915 (cell)

Upstream Provider Point of Contact:

VOIP.ms
2480, Boulevard des Entreprises,
Suite 200
Terrebonne, Quebec J6X 4J8
1.877.786.4767
sales@voip.ms
support@voip.ms