



Robocall Mitigation Program

As per 47 CFR § 64.6305 - Robocall mitigation and certification.(a) Robocall mitigation program (RMP) requirements[4] are:

- To take reasonable steps to avoid originating robocall traffic.
- To commit to responding to a request from the Industry Traceback Group to investigate suspected robocalls.
- To cooperate in investigating and stopping any illegal robocallers.

Therefore, Constructure Technologies, LLC in order to comply with FCC regulations and to continue fighting Illegal Robocalls has implemented the following Robocall Mitigation Program.

- Fraud detection implemented on IP network where possible
- Implement call blocking when suspicious activity detected
- Network and SIP traffic monitoring

Steps to avoid originating robocall traffic

As part of the Robocall Mitigation Program, Constructure Technologies has implemented several measures to prevent Illegal Robocalls from originating from its customers and network.

- Know your Customers
- Contractual agreements
- Analyze and Monitor Network Traffic
- Investigate and Mitigate Suspicious Calls and Calling Patterns

Know your Customers

Constructure Technologies Customers are businesses that must sign a Master Services Agreement and agree to the Services Terms and Conditions. By doing so, they must provide their physical location and contact person(s) and a representative signing the MSA.

Constructure Technologies' on-boarding and turn-up process include helping customers improve their communications solutions, which leads to Constructure Technologies being aware of Customer's size and requirements. In turn, these help Constructure Technologies estimate Customer's working threshold parameters, which in turn will translate into infrastructure and customer specific settings.

Contractual agreements

Constructure Technologies has included clear language in its Terms and Conditions that would mitigate the generation of illegal robocall traffic origination. All existing and new Customers agree to these Terms and Conditions as part of the Master Services Agreement. Terms and Conditions sections relevant to this RMP read as follows:

- Fraudulent/Unauthorized Use of Service. Customer shall not use or permit others to use the Services in a manner that is fraudulent or unauthorized. Constructure Technologies may, without notice and without liability, interrupt all Customer's communications to prevent or terminate fraudulent and/or unauthorized activities provided Constructure Technologies reasonably believes that such activities have occurred or, with reasonable certainty, are about to be undertaken.
- Legal Compliance. Customer and Constructure Technologies shall comply with all applicable laws, rules and regulations relating to the responsibilities assumed by Customer and Constructure Technologies under this Agreement.
- For services provided by Constructure Technologies under the regulation of the Federal Communications Commission(FCC),Constructure Technologies may produce Call Detail Records(CDRs) and Direct inward dial numbers (DIDs) involved in calls included in call traceback requests from the FCC or the appointed Industry Traceback Consortium. Customer agrees to sharing this information with the FCC or the appointed Industry Traceback Consortium in accordance with MSA.

Analyze and Monitor Network Traffic

Constructure Technologies continuously monitors traffic and blocks suspected unlawful or fraudulent traffic, including robocalling and international toll fraud.

Investigate and Mitigate Suspicious Calls and Calling Patterns

Constructure Technologies mitigates suspicious calls by analyzing the usage patterns and limiting the number of concurrent channels based on the customer's size and usage on a per-customer basis. Thresholds are constantly monitored and adjusted to help better detect suspicious usage patterns such as those associated with short calling, illegal robocall, and toll fraud.

Cooperating with Traceback Requests

As being part of the Telecommunications industry, Constructure Technologies has always taken Illegal Robocalls seriously as a threat to its customers and the general public and has taken several measures over the years to prevent such traffic from originating from its network.

Traceback Requests Process

Constructure Technologies is committed to promptly responding to traceback requests from the FCC or the designated Traceback Consortium("the commission"), and for this, Constructure Technologies has created the following process:

1. Upon initial request from the commission, Constructure Technologies will initiate a high-priority Issue in Constructure Technologies' support system.
 - If contact is via email, Constructure Technologies will forward the email to the support system, which in turn will generate a ticket and provide a receipt to the commission representative. Constructure Technologies will ensure the Issue is marked high-priority.
 - If contact is via phone call, Constructure Technologies will create the high-priority Issue based on the phone transcript and include the commission representative information.
2. Constructure Technologies will use reasonable means to validate the commission representative's request before initiating the investigation.
3. Constructure Technologies will investigate the requested traceback and report back to the commission representative with the outcome.
 - If traceback results are negative or inconclusive, the investigation will be closed and documentation in Issue updated.
 - If traceback results are positive, then Constructure Technologies will initiate remediation and mitigation measures.
 - o Remediation - Network Origination: if Constructure Technologies network is originating the traffic, traffic will be blocked from reaching other networks.
 - o Remediation - Customer origination: if a Customer is originating the traffic, Constructure Technologies will request the Customer to investigate the issue promptly. Constructure Technologies will provide the Customer with the call information gathered to help speed the investigation. If the Customer fails to take any remediation or if Constructure Technologies confirms the traffic to be illegal, Constructure Technologies will block the Customer's outgoing traffic except for emergency services and notify the Customer.
4. Final report to the commission: Constructure Technologies will provide the commission with the required information.

Constructure Technologies main Point of Contact for robocall related issues In accordance with FCC's § 64.6305 Robocall mitigation and certification(b)(4)(v)[6], Constructure Technologies has provided the name, title, department, business address, telephone number, and email address of Constructure Technologies main Point of Contact for robocall related issues that will be receiving traceback inquiries from the FCC and the Industry Traceback Consortium.

Name: Joseph Keegan
Title: Principal & CTO
Address: 425 Broadhollow Road Suite 425
City: Melville
State: NY
ZIP Code: 11747
Phone #: 631-396-7777
Email: operations@constructuretech.com

This document Status This document is subject to change and submission to the Commission's Robocall Database website will be updated within 10 business days of any modification in accordance with 47 CFR § 64.6305(b)(5)[7]

File last edited on 2/26/2024