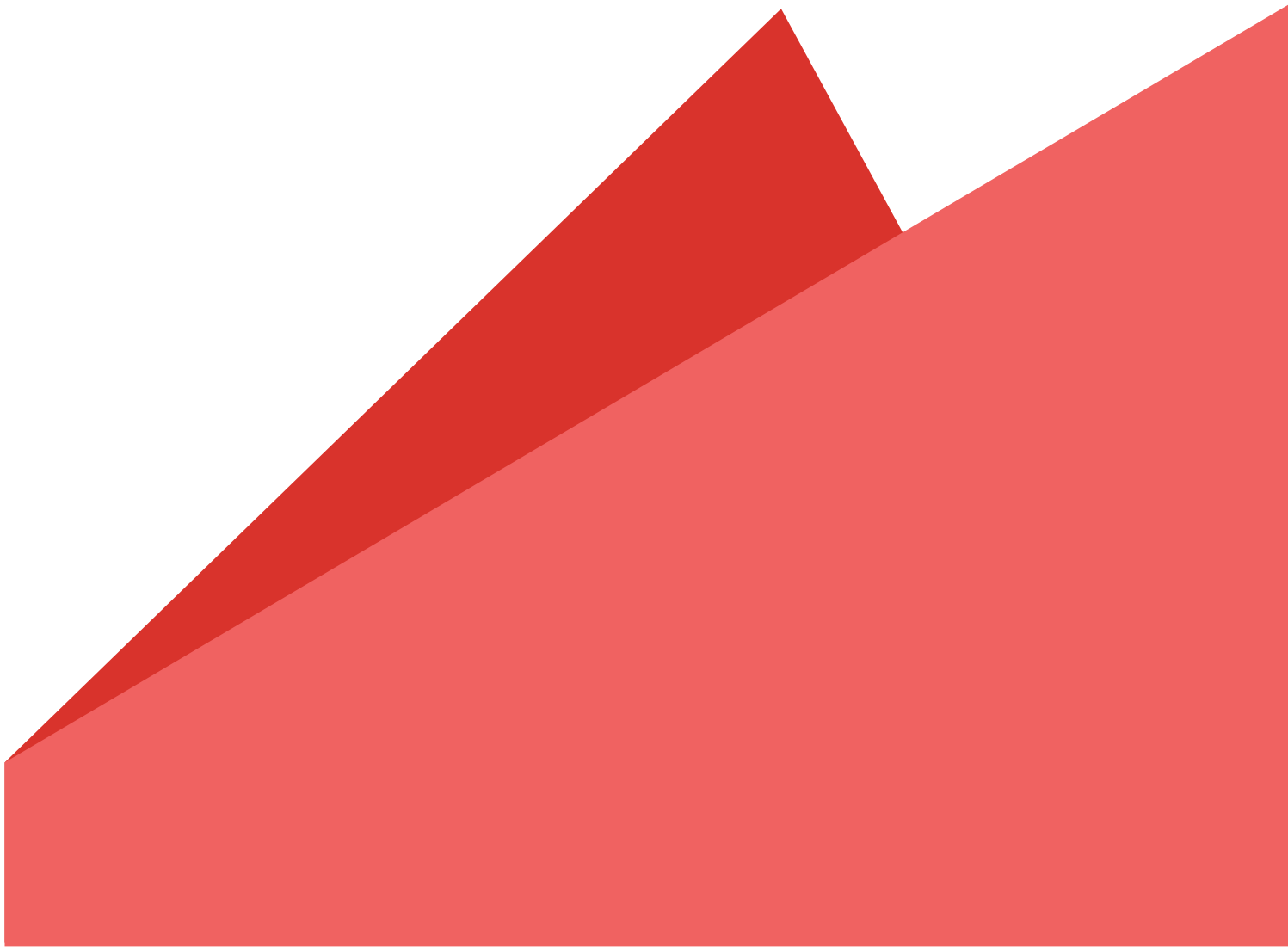




Robocall Mitigation Program

Rev #39444



INDEX

STIR/SHAKEN Implementation Status	3
Robocall Mitigation Program	3
Steps to avoid originating robocall traffic	3
Cooperating to Traceback Requests	4
This document Status	5
References	6

STIR/SHAKEN Implementation Status

Nexacomm LLC ("Nexacomm") lacks control over the network infrastructure necessary to implement STIR/SHAKEN.

Instead, all of our upstream providers have filings in the Robocall Mitigation Database, have complete STIR/SHAKEN implementations and have a robocall mitigation programs in place. All of Nexacomm's customers have binding contracts and their connections and usage are constantly monitored to prevent robocalls and other types of abuse or fraud.

Robocall Mitigation Program

As per 47 CFR § 64.6305 - Robocall mitigation and certification.(a) Robocall mitigation program (RMP) requirements are: [1]

- 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, Nexacomm 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, Nexacomm has implemented several measures to prevent Illegal Robocalls from originating from its customers and network.

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

Know your Customers

Nexacomm Customers are businesses that must sign a Master Services Agreement and agree to the Services Terms and Conditions[2]. By doing so, they must provide their physical location and contact person(s) and a representative signing the MSA.

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

Contractual agreements

Nexacomm 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:

7.1. Fraudulent/Unauthorized Use of Service. Customer shall not use or permit others to use the Services in a manner that is fraudulent or unauthorized. Nexacomm LLC may, without notice and without liability, interrupt all Customer's communications to prevent or terminate fraudulent and/or unauthorized activities provided Nexacomm LLC reasonably believes that such activities have occurred or, with reasonable certainty, are about to be undertaken.

8.1. Legal Compliance. Customer and Nexacomm LLC shall comply with all applicable laws, rules and regulations relating to the responsibilities assumed by Customer and Nexacomm LLC under this Agreement.

8.6. For services provided by Nexacomm LLC under the regulation of the Federal Communications Commission(FCC), Nexacomm LLC 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 to 8.1.

Know your Upstream Providers

Nexacomm only routes incoming and outgoing voice traffic through carriers that have Complete STIR/SHAKEN implementations and have a robocall mitigation programs in place.

These providers filing must appear in the Robocall Mitigation Database and that filing mustn't be de-listed pursuant to an enforcement action.[3]

Nexacomm also only accepts incoming traffic from registered carriers with whom it has a contract in place and will reject any unknown traffic.

Analyze and Monitor Network Traffic

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

Investigate and Mitigate Suspicious Calls and Calling Patterns

Nexacomm 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.

These measures also apply to ensure that the immediate upstream provider is not using it to carry or process a high volume of illegal traffic.[4]

Cooperating to Traceback Requests

As being part of this industry, Nexacomm 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

As a result, Nexacomm is committed to promptly responding to traceback requests from the FCC or the designated Traceback Consortium("the commission") within 24 hours of the receipt of the request[5], and for this, Nexacomm has laid the following process:

1. Upon initial request from the commission, Nexacomm will initiate a high-priority Issue in Nexacomm's support system.

1. If contact is via email, Nexacomm will forward the email to the support system, which



in turn will generate a ticket and provide a receipt to the commission representative. Nexacomm will make sure the Issue is marked high-priority.

2. If contact is via phone call, Nexacomm will create the high-priority Issue based on the phone transcript and include the commission representative information.

2. Nexacomm will use reasonable means to validate the commission representative's request before initiating the investigation.

3. Nexacomm will investigate the requested traceback and report back to the commission representative with either outcome.

1. If traceback results are negative or inconclusive, the investigation will be closed and documentation in Issue updated.

2. If traceback results are positive, then Nexacomm will initiate remediation and mitigation measures.

1. Remediation and mitigation: Network origination: if Nexacomm's network is originating the traffic, traffic will be blocked from reaching other networks.

2. Remediation and mitigation: Customer origination: if a Customer is originating the traffic, Nexacomm will request the Customer to investigate the issue promptly. Nexacomm will provide the Customer with the call information gathered to help speed the investigation. If the Customer fails to take any remediation or Nexacomm confirms the traffic to be illegal, Nexacomm will block the Customer's outgoing traffic except for emergency services and notify the Customer.

4. Final report to the commission: Nexacomm will provide the commission with the required information.

Nexacomm's main Point of Contact for robocall related issues

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

Name: Bruce Reeves

Title: Director of Support Services

Street: 116 West 23rd Street. 5th Floor.

City: New York

State and Zip Code: NY,10011

Telephone Number: +13472921970

Email: support@nexacomm.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 03/15/2024. Revision #39444

References

1. 47 CFR § 64.6305 - Robocall mitigation and certification.(a) Robocall mitigation program requirements.
2. Nexacomm : Terms and Conditions : <https://www.nexacomm.com/terms-and-conditions/>
3. 47 CFR § 64.6305(g)(1)-(g)(4) - Robocall mitigation and certification
4. Amendment to 64.6305 - 89 FR 4833 - Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor
5. Amendment to 64.6305 - 89 FR 4833 - Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor
6. 47 CFR § 64.6305 - Robocall mitigation and certification(b)(4)(v)
7. 47 CFR § 64.6305 - Robocall mitigation and certification.(b)(5)



nexaCOMM

www.nexacomm.com