

Robocall Mitigation Program Description

Syringa Networks, LLC

1. Provider Identification and Scope

This Robocall Mitigation Program Description is submitted by **Syringa Networks, LLC** (“Syringa”) pursuant to **47 C.F.R. § 64.6305**. This document describes the practices and procedures Syringa has implemented to prevent and mitigate the origination, transit, and processing of illegal robocalls on its network, consistent with its role in the call chain and applicable Commission rules.

Syringa may modify, enhance, or otherwise update the practices described herein as its business, capabilities, or regulatory obligations evolve.

2. Role in the Call Chain

Syringa operates as a voice service provider, consistent with its certification in the FCC Robocall Mitigation Database. Syringa does not knowingly originate, carry, or process illegal robocalls and maintains controls designed to reduce the risk that its network is used for unlawful calling activity.

3. Customer Due Diligence (“Know Your Customer”)

Syringa maintains customer due-diligence practices designed to confirm the identity, legitimacy, and intended use of service by new and existing customers.

These practices include, as appropriate:

- Collection and review of customer identifying information prior to service activation;
- Verification of business formation, service address, and contact information for business customers;
- Confirmation, where applicable, of a customer’s right to use the telephone numbers presented on calls;
- Review of customer information when services are added or materially modified; and
- Contractual provisions prohibiting the use of Syringa’s network for illegal robocalling activity.

If Syringa identifies customer behavior that appears inconsistent with lawful use of service, Syringa may investigate, warn the customer, require corrective action, and, if necessary, suspend or terminate service.

4. Upstream Provider Due Diligence (“Know Your Upstream Provider”)

Syringa maintains processes to assess voice traffic received from upstream providers.

These processes include, as appropriate:

- Confirming that upstream providers maintain a certification in the FCC Robocall Mitigation Database;
- Requiring upstream providers to maintain reasonable robocall mitigation practices;
- Contractual prohibitions against transmitting illegal robocalls; and
- Escalation, investigation, and termination of upstream relationships if unlawful or suspicious calling activity persists.

Syringa does not knowingly accept traffic from providers that are not properly registered or that refuse to address identified robocall risks.

5. Robocall Detection and Mitigation Measures

Syringa employs a combination of technical and operational measures to identify and mitigate potentially unlawful robocalling activity, including:

- Use of call authentication solutions consistent with STIR/SHAKEN requirements;
- Use of call analytics and reputation-based indicators to identify suspicious calling patterns;
- Identification and blocking of calls originating from invalid, unallocated, or Do-Not-Originate numbers, consistent with Commission guidance;
- Investigation of traffic associated with elevated risk indicators; and
- Escalation, warning, and termination procedures for customers or upstream providers that appear to be associated with unlawful robocalling activity.

These measures are applied in a manner consistent with Syringa’s role in the call chain and the characteristics of the traffic being processed.

6. STIR/SHAKEN Implementation

Syringa has implemented STIR/SHAKEN in the IP portions of its network consistent with applicable Commission rules and policies. Syringa utilizes industry-standard call authentication solutions to authenticate calls as appropriate for its role and maintains responsibility for compliance with STIR/SHAKEN requirements, including certificate governance and call signing obligations.

7. Traceback Cooperation

Syringa cooperates fully with traceback requests from the Federal Communications Commission, law enforcement agencies, and the registered industry traceback consortium.

Syringa has designated a point of contact responsible for receiving and responding to traceback requests and commits to responding to such requests within **24 hours**, consistent with Commission expectations. Syringa investigates identified traffic and takes appropriate action to mitigate unlawful robocalling activity when warranted.

8. Cooperation with Regulators and Law Enforcement

Syringa cooperates with federal and state regulators and law enforcement authorities to prevent and mitigate illegal robocalls. This cooperation may include:

- Responding to valid law enforcement inquiries;
 - Providing relevant non-proprietary information related to suspected unlawful robocalling activity; and
 - Implementing additional mitigation measures when required by Commission rule or order.
-

9. Ongoing Evaluation

Syringa periodically reviews the effectiveness of its robocall mitigation practices and updates its procedures as necessary to address evolving risks, operational changes, and regulatory requirements.