

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Submitted to the FCC Robocall Mitigation Database pursuant to 47 CFR § 64.6305

Legal Business Name:	STG Technologies LLC
FCC Registration No. (FRN):	0038579207
Business Address:	403 North Charles Street, Suite 200, Baltimore, Maryland 21201
Robocall Mitigation Contact:	Stone Graham, Director of IT Operations and Development Stone@stgtechnologies.net
Provider Type / Call-Chain Role:	Voice Service Provider without a STIR/SHAKEN obligation (non-facilities-based reseller)
Effective Date:	June 25, 2026

1. Overview and Provider Role

STG Technologies LLC (“the Company”) is a non-facilities-based voice service provider that resells interconnected voice services to its end-user customers using the network and numbering resources of its underlying wholesale carrier. The Company’s customers are businesses that use the service for their own internal and ordinary business voice communications. The Company does not operate its own physical network facilities and does not act as a gateway provider or an intermediate provider. As a non-facilities-based reseller that does not control the network segments on which calls are authenticated, the Company is a Voice Service Provider without an independent STIR/SHAKEN obligation. This Robocall Mitigation Program (the “Program”) describes the specific, reasonable steps the Company takes to avoid originating illegal robocall traffic, consistent with its obligations under 47 CFR § 64.6305 and the FCC’s robocall-mitigation and Know-Your-Customer requirements.

2. Caller ID Authentication (STIR/SHAKEN) Status

Because the Company is a non-facilities-based reseller and does not control the IP network segments on which calls are signed, the Company does not independently operate a STIR/SHAKEN caller ID authentication infrastructure and does not carry an independent STIR/SHAKEN implementation obligation. Calls originated by the Company’s customers are carried over the network of the Company’s underlying wholesale provider, which performs STIR/SHAKEN authentication on its network. Accordingly, the Company certifies as a Voice Service Provider without a STIR/SHAKEN obligation and performs the robocall-mitigation measures described below.

3. Know Your Customer (KYC) and Customer Vetting

The Company applies affirmative, effective measures to know its customers and vets and approves each customer before activating service. Because the Company serves a limited population of business customers using voice service for their own ordinary communications, the Company is able to review each prospective customer individually prior to turn-up. The Company’s onboarding diligence includes:

- Collecting and retaining each customer’s legal business name, physical business address, and primary contact information prior to activation;

- Verifying the legitimacy of the business and confirming, where appropriate, its good standing and the nature and intended use of the requested service;
- Confirming that the customer's intended traffic is ordinary business voice communication and not high-volume automated or unlawful calling;
- Activating service only after this review is completed satisfactorily; and
- Retaining customer identification and onboarding records consistent with applicable FCC retention requirements.

4. Acceptable Use and Contractual Safeguards

Each customer is bound by a written service agreement and acceptable-use policy that expressly prohibit the origination of illegal calls, including unlawful robocalls, illegally spoofed caller ID, and traffic that violates the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule (TSR), the Truth in Caller ID Act, or applicable Do-Not-Call rules. Customers are required to obtain and maintain any consents legally required for their traffic and to use only telephone numbers they are authorized to use. Violation of these terms is grounds for immediate suspension or termination of service.

5. Traffic Monitoring and Red-Flag Detection

The Company employs a two-layer approach to monitoring the traffic it originates. First, the Company relies on the analytics, alerts, and traceback notices provided by its underlying wholesale provider, which operates the network and observes traffic at carrier scale. Second, the Company conducts its own review of call detail records (CDRs) and call reporting generated by its hosted PBX platform (3CX) to identify anomalies. Indicators that trigger review include:

- Sudden or unexplained spikes in call volume or short-duration call patterns;
- High volumes of calls with low answer rates or abnormal completion ratios;
- Complaints, traceback notices, or provider alerts indicating suspected illegal traffic; and
- Caller ID values inconsistent with numbers assigned to or authorized for the customer.

Upon identifying suspicious traffic, the Company investigates promptly and takes appropriate action, up to and including suspension or termination of the offending customer and notification of the Company's underlying provider.

6. Traceback Cooperation (24-Hour Commitment)

The Company is committed to responding fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the Industry Traceback Group (the FCC-designated registered traceback consortium). The Company will cooperate with such entities in identifying, investigating, and stopping any party using the Company's service to originate illegal calls, and will take effective mitigation action against any customer identified as a source of illegal traffic, including suspension or termination of service.

7. Enforcement and Remediation

Where the Company determines that a customer has originated illegal traffic or breached the acceptable-use policy, the Company takes graduated, effective action appropriate to the severity and recurrence of the conduct. Such action may include formal notice, mandatory remediation, temporary suspension, and permanent termination of service. The Company maintains records of mitigation actions

taken to support FCC oversight and law-enforcement inquiries.

8. No Prior Robocall-Related Actions

As of the effective date of this Program, neither the Company nor its controlling personnel has been the subject of a formal Commission, law enforcement, or regulatory action or investigation relating to the origination of illegal robocall traffic within the prior two years.

9. Recordkeeping, Updates, and Recertification

The Company maintains records of its KYC determinations, traffic-monitoring reviews, and mitigation actions consistent with applicable FCC retention requirements. The Company will update its Robocall Mitigation Database filing within ten (10) business days of any material change to the information contained in this Program, and will recertify its filing annually as required by the Commission's rules.

10. Designated Point of Contact

Questions regarding this Robocall Mitigation Program, and traceback or law-enforcement requests, may be directed to: Stone Graham, Director of IT Operations and Development, STG Technologies LLC, Stone@stgtechnologies.net.

This Robocall Mitigation Program Description is submitted by STG Technologies LLC in connection with its filing in the FCC Robocall Mitigation Database. The information herein is true and accurate to the best of the Company's knowledge. Certification of this filing is provided electronically by the Company's authorized officer through the Robocall Mitigation Database submission portal.