

Robocall Mitigation Program Description

EDG Security & Fire Systems LLC

Effective Date: September 17, 2026

1. Company and Service Description

EDG Security & Fire Systems LLC ("EDG") is a non-facilities-based voice service provider that provides VoIP services to business end users. EDG uses wholesale voice service providers, including Skytel and other wholesale voice service providers, for underlying voice network and PSTN connectivity. EDG does not own or control the underlying carrier network infrastructure used to provide PSTN connectivity.

2. STIR/SHAKEN Implementation

EDG does not independently implement STIR/SHAKEN on the underlying carrier networks used to originate calls because EDG does not control the network infrastructure necessary to perform STIR/SHAKEN authentication. EDG relies on its wholesale voice service providers for applicable caller-ID authentication and carrier-level call authentication functions. EDG will cooperate with its wholesale providers and the Federal Communications Commission, law enforcement, and the industry traceback consortium regarding applicable traceback and caller-ID authentication matters.

3. Customer Onboarding and Account Controls

- EDG obtains and maintains identifying and contact information for customers before providing voice service and uses that information to identify the customer responsible for a voice account.
- EDG reviews customer requests for voice service, telephone numbers, and calling functionality and may request additional information when an account or requested usage presents a heightened risk of illegal robocalling or spoofing.
- EDG's service terms prohibit illegal robocalling, unlawful spoofing, fraud, and use of EDG's services for unlawful communications activity.
- EDG may restrict, suspend, or terminate voice service when it identifies activity that violates applicable law, service terms, or the requirements of its wholesale providers.

4. Traffic and Usage Monitoring

- EDG reviews customer accounts and voice-service activity for indicators of potentially abusive or unauthorized use, including unusual calling volume, significant changes in traffic patterns, repeated complaints, or other activity inconsistent with the customer's stated use of the service.
- EDG investigates customer complaints and alerts received from its wholesale voice providers concerning suspected robocalling, spoofing, or other abusive traffic.
- When suspicious activity is identified, EDG may investigate the customer and traffic source and may restrict or suspend the affected service while the matter is reviewed.

5. Call Analytics and Upstream Provider Coordination

EDG relies on monitoring and fraud/abuse controls available through its voice-service platform and its wholesale voice providers. EDG also uses information and alerts supplied by its upstream providers to identify potentially problematic traffic. EDG maintains awareness of the wholesale providers through which its voice traffic is carried and will provide appropriate customer and traffic information to those providers when required for abuse investigation or traceback.

6. Traceback and Law-Enforcement Cooperation

EDG commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, consistent with applicable law. EDG will cooperate with such entities and with its wholesale voice providers in investigating and stopping illegal robocall traffic. EDG will provide available customer, account, and traffic information reasonably necessary to identify the source of suspected illegal traffic.

7. Ongoing Program

EDG will periodically review its customer onboarding, traffic-monitoring, abuse-response, and wholesale-provider procedures and will update those procedures as necessary to address emerging robocalling and spoofing risks and applicable FCC requirements.

Important: This document should be submitted only if the practices described above accurately reflect EDG's actual operations. The FCC requires a robocall mitigation plan to describe specific reasonable steps the provider actually undertakes; a generalized statement that a mitigation program exists is not sufficient.