

Robocall Mitigation Plan: Grux

1. Introduction and Objectives

Grux is a cloud-based engagement platform designed to enhance business workflows for modern teams. As part of its feature set, Grux provides call center capabilities that allow users to originate and receive calls via the Public Switched Telephone Network (PSTN). Grux is committed to preventing the origination of illegal robocalls on its platform and ensuring full compliance with the TRACED Act and FCC rules.

2. STIR/SHAKEN Implementation Status

Certification Category: No Implementation (Exemption Claimed)

Grux certifies that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

- **Basis for Exemption:** Grux operates as a pure software-based application (SaaS) that lacks control over the underlying network infrastructure necessary to perform the "technological act" of signing calls.
- **Detailed Justification:** Grux originates all calls via a wholesale integration with **REDIRECTED**, a third-party carrier. Because Grux does not own or operate IP-based switches, Session Border Controllers (SBCs), or the core signaling network, it cannot independently inject digital signatures into the call headers. Technical implementation occurs upstream at the carrier level (47 CFR § 64.6305).

3. Know Your Customer (KYC) Protocols

To mitigate the risk of illegal robocalling, Grux implements strict "Know Your Customer" procedures for all users accessing call center features:

- **Business Verification:** New customers must provide valid business registration information, including their legal entity name and physical address.
- **Account Vetting:** Each account is manually reviewed or programmatically vetted to ensure the user is a legitimate business entity before PSTN calling capabilities are enabled.
- **Organization Matching:** For contacts and calls, Grux uses domain matching and customer profile creation to link interactions to verified organizational accounts.

4. Traffic Monitoring and Prevention

Grux uses internal analytics and coordination with its upstream provider to monitor for suspicious calling patterns:

- **Anomaly Detection:** The system tracks customer-specific interaction history, including call frequency and duration, to identify potential autodialer abuse or illegal spoofing.
- **Restricted Access:** Users are restricted from using PSTN resources for any activity that

violates the platform's terms of service, which strictly prohibit fraudulent messaging or deceptive identity practices.

- **Upstream Compliance:** Grux relies on **REDATECTED** carrier-grade analytics to identify and block traffic that meets the criteria for illegal robocalling at the network level.

5. Traceback Response Commitment

Grux fully commits to cooperating with the FCC, law enforcement, and the Industry Traceback Group (ITG):

- **24-Hour Response:** Grux will respond to all traceback requests within 24 hours of receipt.
- **Cooperation:** Grux will assist investigators in identifying the specific end-user responsible for any calls identified as illegal or fraudulent and will take immediate action, up to account termination, against bad actors.

6. Mitigation Contact Information

For all robocall mitigation and traceback inquiries, please contact:

- **Name:** REDATECTED
- **Title:** REDATECTED
- **Email:** REDATECTED
- **Address:** REDATECTED