

Company Name: Communication Dynamics Ltd
Date: February 23rd, 2026

1. Introduction and Network Architecture

Communication Dynamics Ltd ("the Company") is a non-facilities-based voice service provider. We are committed to preventing our network and services from being used to originate or transmit illegal robocalls, caller ID spoofing, and related fraudulent communications.

Because the Company does not own or operate the underlying telecommunications switches or SIP signaling infrastructure necessary to cryptographically sign calls, we have claimed an exemption from directly implementing the STIR/SHAKEN framework. We rely entirely on our facilities-based upstream provider, DIDWW, to route our traffic to the U.S. Public Switched Telephone Network (PSTN) and to apply STIR/SHAKEN attestation to our customers' calls on our behalf.

Although we cannot implement STIR/SHAKEN directly, we maintain a strict, multi-layered Robocall Mitigation Program to ensure our services are not abused by illegal robocallers.

2. Traceback Cooperation Commitment

As required by FCC rules, Communication Dynamics Ltd unequivocally commits to responding fully and within 24 hours to all traceback requests from the Federal Communications Commission (FCC), U.S. law enforcement agencies, and the official Industry Traceback Group (ITG).

We actively maintain up-to-date contact information in the FCC Robocall Mitigation Database. If a traceback request is received regarding traffic that originated from one of our customers, we will immediately investigate, identify the responsible end-user, provide the necessary information to the requesting body, and take appropriate mitigation steps, including blocking the traffic if it is determined to be illegal.

3. "Know Your Customer" (KYC) Procedures

To prevent bad actors from accessing our services, Communication Dynamics enforces strict identity verification protocols before onboarding any new customer. Our KYC procedures include:

- Identity Verification: Collecting and verifying the customer's legal business name, physical address, email, phone number, and official corporate registration documents.
- Payment Verification: Requiring verifiable payment methods that match the corporate identity (e.g., matching credit card names or bank transfer origins).
- Use Case Vetting: Requiring prospective customers to describe their intended use case for our voice services (e.g., B2B sales, customer support, standard business telephony).

We do not onboard customers whose stated use cases align with high-volume, unsolicited telemarketing.

4. Traffic Monitoring and Pattern Analysis

The Company continuously monitors outbound calling traffic to identify anomalies that may indicate illegal robocalling or unauthorized caller ID spoofing. We monitor for metrics typical of robocalling campaigns, including but not limited to:

- High volumes of call attempts in a short timeframe.
- Exceptionally low Average Length of Call (ALOC).
- Unusually low Answer Seizure Rate (ASR) / call completion rates.
- Calls originating from invalid, unassigned, or Do Not Call (DNC) registered numbers.

If our automated or manual monitoring detects suspicious traffic patterns, the account is flagged for immediate administrative review.

5. Terms of Service and Contractual Enforcement

Communication Dynamics Ltd's Terms of Service and Acceptable Use Policy (AUP) explicitly prohibit the use of our platform for illegal robocalling, telemarketing fraud, and illegal caller ID spoofing (violating the Truth in Caller ID Act). All customers must agree to these terms prior to using our services.

If a customer is found to be violating these terms, either through our internal monitoring, a notification from our upstream provider (DIDWW), or a traceback request from the ITG, we take immediate action. Mitigation actions include:

- Suspending the customer's ability to originate calls.
- Terminating the customer's account entirely.
- Cooperating with upstream providers and authorities to prevent the bad actor from returning.