

Speakup B.V.

Robocall Mitigation Program Description

Speakup B.V., a company organized under the laws of the Netherlands (“Speakup”), hereby submits this Robocall Mitigation Program Description as required for filing in the Robocall Mitigation Database. Speakup certifies under Option 3 that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network, and that all calls it originates are subject to a robocall mitigation program consistent with 47 C.F.R. § 64.6305(a).

Speakup is a Dutch voice-over-IP (VoIP) and telecommunications provider that delivers hosted voice services to business customers, primarily in the Netherlands and Europe. Speakup obtains U.S. telephone numbers through a U.S.-based voice service provider that has fully implemented the STIR/SHAKEN authentication framework on its network. Speakup does not directly originate or terminate calls on the U.S. public switched telephone network (PSTN); all U.S.-bound calls originated by Speakup’s customers are handed off to this U.S. gateway provider, which applies STIR/SHAKEN authentication and delivers those calls to the PSTN.

As a foreign voice service provider without access to U.S. numbering resources and without eligibility to obtain a Service Provider Code (SPC) token from the STIR/SHAKEN Governance Authority, Speakup is exempt from the STIR/SHAKEN implementation requirements under 47 C.F.R. § 64.6304(b). Nevertheless, Speakup has implemented a comprehensive robocall mitigation program as described below.

1. Traceback Cooperation

Speakup is a company incorporated and operating under the laws of the Netherlands and is subject to Dutch and European Union law. Speakup does not maintain a direct relationship with U.S. traceback entities. In practice, traceback requests relating to calls originated by Speakup’s customers are expected to be received through Speakup’s U.S. gateway provider, which is the point of entry for these calls into the U.S. PSTN.

Upon receiving a traceback inquiry from its gateway provider, Speakup will investigate the matter and respond within a reasonable timeframe consistent with its existing lawful interception and abuse-handling processes. Speakup will provide, to the extent permitted under applicable Dutch and EU law, the identity of the originating customer account and any other information reasonably necessary to trace the origin of the call in question. Speakup can be reached for abuse and traceback inquiries at abuse@speakup.nl.

Speakup will cooperate with its U.S. gateway provider and, where appropriate and consistent with applicable Dutch and EU legal requirements, with U.S. authorities in investigating and stopping any illegal robocallers that use its service to originate calls. Requests from Dutch or European authorities through proper legal channels will be handled in accordance with Speakup’s established lawful interception procedures.

2. Know Your Customer (KYC) Procedures

Speakup applies thorough due diligence procedures to assess and manage the risk associated with customers before onboarding them onto its platform. These procedures are designed to verify the legitimacy of prospective customers and evaluate the nature and intended use of their voice traffic. Speakup's KYC procedures include the following components:

- **Identity Verification.** All prospective customers must submit verifiable business information, including legal business name, registered business address, contact details, and Chamber of Commerce (KvK) registration or equivalent regulatory identification. Speakup verifies this information prior to provisioning any services.
- **Traffic Profile Assessment.** Speakup evaluates the type and volume of voice traffic a prospective customer intends to generate, the nature of the customer's business, and the end users the customer serves. Customers requesting U.S. telephone numbers are subject to additional scrutiny regarding the intended use of those numbers and the expected call patterns.
- **Contractual Obligations.** Speakup's customer agreements include specific provisions prohibiting the origination of illegal robocall traffic. Customers are contractually required to comply with all applicable laws and regulations governing voice communications, including U.S. laws regarding robocalls and caller ID spoofing. Violation of these provisions may result in immediate suspension or termination of service.
- **Ongoing Monitoring.** Speakup conducts ongoing review of its customer base. Customers who are the subject of traceback requests, complaints, or other indications of illegal calling activity are investigated and may be suspended or terminated in accordance with Speakup's acceptable use policies.

3. Traffic Monitoring and Analytics

Speakup monitors voice traffic on its platform to detect suspicious patterns that may indicate illegal robocalling or fraudulent activity. Speakup's monitoring practices include:

- **Call Detail Record (CDR) Analysis.** Speakup reviews call detail records to identify anomalous traffic patterns, including unusually high call volumes from a single account, high volumes of short-duration calls, calls to a wide array of called numbers from a single source, and other patterns commonly associated with robocalling or traffic pumping.
- **Threshold-Based Alerting.** Speakup has implemented monitoring thresholds that trigger alerts when traffic from a customer account deviates significantly from established baselines. These alerts are reviewed by the operations team, and appropriate action is taken based on the severity and nature of the deviation.
- **Caller ID Validation.** Speakup verifies that customers are using only telephone numbers that have been legitimately assigned to them through Speakup's number inventory. Calls with caller ID values that do not match assigned numbers are rejected by the platform.

4. Call Blocking and Enforcement Actions

Speakup takes enforcement action against customers who are identified as originating or facilitating illegal robocall traffic. Enforcement actions include:

- **Immediate Blocking.** When Speakup identifies traffic that is reasonably believed to be illegal robocall traffic, Speakup will immediately block the offending traffic and, where appropriate, suspend the customer's ability to place outbound calls pending investigation.
- **Account Suspension and Termination.** Customers who are found to have originated illegal robocall traffic, who fail to cooperate with traceback investigations, or who repeatedly generate traceback requests are subject to suspension or permanent termination of their service agreement.
- **Documentation and Tracking.** All incidents involving suspected illegal robocall traffic, traceback requests, and enforcement actions are documented in Speakup's internal ticketing system for record-keeping and trend analysis.

5. Relationship with U.S. Gateway Provider

Speakup's U.S.-bound voice traffic is routed through a U.S.-based gateway provider that has fully implemented the STIR/SHAKEN authentication framework on its network and is responsible for authenticating calls as they enter the U.S. PSTN. Speakup cooperates with its gateway provider in addressing any issues related to call authentication, traceback requests, or illegal traffic originating from Speakup's customer base.

Speakup provides its U.S. gateway provider with accurate caller ID information for all calls originated by its customers, enabling the gateway provider to properly sign calls under the STIR/SHAKEN framework. Speakup does not permit its customers to manipulate or spoof caller ID information in violation of applicable law.

6. Commitment to Ongoing Compliance

Speakup is committed to maintaining and improving its robocall mitigation practices on an ongoing basis. Speakup will review and update this Robocall Mitigation Program Description as necessary to reflect changes in its operations, technology, or applicable regulatory requirements. Speakup will also monitor developments in robocall mitigation best practices and implement additional measures as appropriate.

Nick Bouwhuis
Speakup B.V.
Date: 2026-03-26