



Robocall Mitigation Program

Sonetel AB (publ)

Version 2.0 -- February 26, 2026

1. Purpose of This Document

Sonetel AB (publ) ("the Company") has established a robocall mitigation program in accordance with the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) and the Federal Communications Commission's rules regarding robocall mitigation (47 CFR 64.6305), in order to curb the origination of illegal robocalls from its network.

The Company has not implemented STIR/SHAKEN authentication framework on any portion of its network. However, all calls that originate from the Company's network are subject to the robocall mitigation program described in this document.

Additionally, the Company's terms and conditions require that calls to and from the service be initiated by humans with the purpose of business communication. Scripted or otherwise automated calls are prohibited.

This document describes the Company's practices and procedures for mitigating illegal robocalls, including customer verification, traffic monitoring, enforcement actions, and cooperation with industry traceback efforts.

2. Provider Classification

The Company is a foreign voice service provider registered in Sweden (Org. No. 556486-8851). The Company provides cloud-based voice communication services to customers worldwide and functions as a gateway and intermediate provider for voice traffic that may terminate in the United States.



The Company operates a SIP-to-SIP platform. It does not maintain direct interconnection with the U.S. Public Switched Telephone Network (PSTN). All U.S.-terminated traffic is routed through downstream U.S.-based carriers that maintain PSTN interconnection and are responsible for STIR/SHAKEN authentication on those calls.

The Company's primary services include virtual phone numbers, call forwarding, and business telephony features.

3. STIR/SHAKEN Position

The Company has not implemented the STIR/SHAKEN call authentication framework and does not originate STIR/SHAKEN attestations.

As a foreign voice service provider, the Company is not eligible to obtain a Service Provider Code (SPC) token or certificate from the U.S. Secure Telephone Identity Policy Administrator (STI-PA), and therefore cannot implement the STIR/SHAKEN framework. Pursuant to 47 CFR 64.6305, the Company has instead implemented the robocall mitigation program described in this document.

The Company relies on its downstream U.S.-based carriers to apply STIR/SHAKEN authentication to calls that enter the U.S. telephone network.

The Company asserts caller identity on outbound calls using the P-Asserted-Identity header (RFC 3325), populated with the customer's verified caller ID. Only caller IDs that have been verified through the Company's customer verification process are used.

In lieu of STIR/SHAKEN implementation, the Company maintains the robocall mitigation practices described in this document.

4. Procedures for Robocall Mitigation

4.1 Point of Contact

The Company has designated a point of contact for receiving and responding to notifications of suspected illegal robocall traffic. Contact details are provided in Appendix 1.

The designated contact is available to receive traceback requests, law enforcement inquiries, and notifications from industry bodies regarding suspected illegal traffic originating from or transiting through the Company's network.

4.2 Traceback Response

The Company cooperates with the Industry Traceback Group (ITG) and responds to traceback requests within 24 hours of receipt.

Upon receiving a traceback request, the Company will:

- Acknowledge receipt of the request;
- Identify the source account or traffic path associated with the reported call(s);
- Take appropriate enforcement action, which may include immediate suspension of the responsible account; and
- Provide the requesting party with relevant information to support continuation of the traceback, to the extent permitted by applicable law.

Traceback requests should be directed to the contact information provided in Appendix 1.

4.3 Investigation Procedures

When the Company receives a notification of suspected illegal robocall activity, it follows one of three investigation paths depending on the traffic source:

Traffic originated by a Company customer: The Company identifies the responsible account using internal call records. The account is subject to immediate suspension pending investigation. If the investigation confirms illegal activity, the account is permanently terminated.

Traffic originated by an upstream partner: The Company forwards the notification to the originating partner for investigation and remediation, while monitoring for continued abusive traffic from that source.

Spoofed traffic (not originated by or through the Company): The Company informs the notifying party that the traffic did not originate from or transit through its network, and provides any available information that may assist in identifying the actual source.

5. Customer Verification and Risk Controls

The Company maintains a customer verification program designed to confirm the identity and legitimacy of customers before they are permitted to place outbound calls or activate phone numbers.

Identity Verification. All customers are required to provide verifiable identity information during registration. The Company screens new accounts using multiple data points, including geographic consistency checks, payment verification, and document review. Accounts that present risk indicators are subjected to enhanced due diligence, which may include additional document requirements or manual review by compliance personnel.

Business Verification. Business customers are subject to additional verification, including cross-referencing of publicly available business records.



Enhanced Verification for Increased Capacity. Customers requesting increased calling capacity or access to premium services must complete additional identity verification beyond the standard requirements.

Ongoing Monitoring. The Company monitors customer accounts for changes in usage patterns that may indicate misuse. Significant changes in calling behavior, payment activity, or account configuration may trigger re-verification of the customer's identity.

6. Automated Security and Monitoring

The Company operates multiple automated systems that continuously monitor traffic and account activity to detect and prevent misuse of its platform. These systems run at intervals ranging from real-time to daily, depending on the type of monitoring performed.

Call Velocity and Volume Monitoring. Automated systems monitor for abnormal call volumes, including high call rates from individual accounts, unusually high numbers of parallel calls, and rapid-fire calling patterns. Accounts that exceed established thresholds may be automatically blocked.

Fraud Pattern Detection. Automated systems analyze call detail records and account activity to detect common fraud patterns, including repeated calls to the same destination, calls to known high-risk destinations, and calling patterns consistent with robocalling or toll fraud.

Payment and Financial Fraud Prevention. Automated systems monitor for payment-related abuse, including reuse of payment methods associated with previously blocked accounts, credit overuse, and suspicious payment patterns across multiple accounts.

Account Abuse Detection. Automated systems identify and block new accounts that exhibit characteristics associated with known fraudulent accounts, including reuse of phone numbers, IP addresses, or payment methods previously linked to abusive activity.

Signup Fraud Prevention. The Company employs controls at the point of registration to prevent mass account creation from a single source.

Where automated monitoring systems detect a confirmed threat, the account is blocked automatically without manual intervention. For lower-confidence detections, alerts are generated for review by operations personnel.

7. Subscriber Account Limitations

All subscriber accounts are subject to default limitations on calling capacity. These limitations include restrictions on the number of concurrent calls, call duration, and calling volume.

Default limitations are applied to all new accounts upon registration. Customers may request increased capacity, subject to the enhanced verification requirements described in Section 5.

Accounts that have been inactive for an extended period are subject to additional security measures before reactivation, including re-verification of the account holder's identity and removal of stored payment methods.

8. Service Limitations

The Company maintains platform-level controls that restrict or prohibit the use of certain features that present elevated risk for abuse. These controls are applied universally and are not dependent on individual account assessment.

The Company reserves the right to restrict, modify, or disable specific service features at any time in response to identified patterns of misuse.

9. Partner and Upstream Oversight

The Company routes voice traffic through a limited number of established telecommunications providers. These providers are expected to comply with applicable telecommunications regulations in their respective jurisdictions, including regulations related to robocall mitigation.

The Company monitors traffic from and to its partner carriers. If the Company identifies patterns of abusive or illegal traffic associated with a specific partner, the Company will notify the partner and may suspend or terminate the traffic exchange if the issue is not resolved.

The Company cooperates with its upstream and downstream partners in investigating suspected illegal traffic and responding to traceback requests.

10. Enforcement Policy

The Company maintains a zero-tolerance policy for the use of its platform to originate illegal robocalls.

Accounts found to be involved in illegal robocalling, caller ID spoofing for fraudulent purposes, or any other form of telecommunications fraud are subject to immediate suspension and termination without prior notice. The Company is not required to provide advance warning before taking enforcement action.

The Company reserves the right to:

- Immediately suspend or terminate any account suspected of involvement in illegal robocalling;
 - Block specific traffic patterns, destinations, or call types associated with abusive activity;
 - Retain call records and account information for use in law enforcement investigations; and
 - Report confirmed illegal activity to relevant regulatory authorities and industry bodies.
-

11. Governance and Compliance

Annual Review. This document is reviewed and updated at least annually, prior to the Company's recertification in the FCC's Robocall Mitigation Database. Additional reviews are conducted following significant changes in the regulatory environment or in the Company's operations.

Document Retention. The Company retains records of traceback requests, enforcement actions, and customer verification activities in accordance with applicable legal requirements.

12. Revision History

Version	Date	Description
v1.0	June 15, 2021	Original filing.
v2.0	February 26, 2026	Comprehensive update for recertification. Added provider classification, expanded STIR/SHAKEN position, formalized traceback response commitment, expanded customer verification and KYC descriptions, documented automated security and monitoring capabilities, added partner oversight and enforcement policy sections, established governance framework.



Appendix 1: Contact Information

Designated Point of Contact

Name	Henrik Thome
Title	Chief Executive Officer
Email	regulations@sonetel.com
Phone	+1 857 207 3900

Company Address

Sonetel AB (publ)
Mailbox 647
114 11 Stockholm
Sweden

FCC Registration

FCC Registration Number (FRN)	0031029523
Robocall Mitigation Database ID	MD0002234

Sonetel AB (publ) -- Robocall Mitigation Program v2.0 -- February 26, 2026