

Rebtel Networks AB
Robocall Mitigation Plan
Updated February 20, 2026

This document provides the information required by Section 64.6305 of the Commission's rules and explains the specific reasonable steps Rebtel Networks AB ("Rebtel") is taking to avoid carrying or processing illegal robocall traffic on its calling platform as part of its robocall mitigation plan as required by Section 64.6305.

Rebtel will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), Rebtel will update its submission in the Robocall Mitigation Database within 10 business days of any change to the applicable information it must provide in the Robocall Mitigation Database, including its Robocall Mitigation Plan.

In general, Rebtel's customers do not originate high volume calls and Rebtel has not received any indications suggesting that Rebtel and its services are used to originate robocalls. While Rebtel therefore does not consider its services at high risk of originating illegal robocalls, as noted below it is committed to working with the Commission, law enforcement, and the industry traceback consortium to combat illegal robocalling.

I. PREVENTING ILLEGAL ROBOCALLS TO BE CARRIED OR PROCESSED ON REBTTEL PLATFORM

Rebtel has deployed policies and systems designed to detect and prevent fraudulent traffic, robocalls, calling line identity ("CLI") spoofing, and other unwanted activities on its platform, including the following.

Rebtel has in place enforceable terms of use and an acceptable use policy (e.g., including undertakings by the customer to comply with applicable law and not to use the services for illegal purposes), which define the circumstances by which Rebtel will deny, suspend, or terminate services to a customer.

Rebtel, as part of its customer onboarding process, undertakes various commercially reasonable precautions to verify a given customer's identity.

Rebtel requires the presence of a CLI to allow calls to be connected through its platform. In case of no CLI, the caller must authenticate their identity with a registered phone number and PIN.

Rebtel engages in real-time network monitoring to identify suspicious usage patterns or activities that deviate from normal and acceptable usage patterns, such as:

- large bursts of calls in a short timeframe
- sequential dialling patterns
- low average call duration
- low call completion ratios
- invalid numbers placing a large volume of calls
- a large volume of complaints related to a suspect line
- unlawful foreign-based spoofing

Rebtel runs screening processes daily in addition to real-time alerts to detect suspicious traffic. Rebte's NOC team, available 24/7, investigates calls that are flagged as potentially being illegal and takes measures to mitigate or block that traffic on its platform, including the use of blocklists.

Rebtel uses internal tools and third-party services to assess the viability of a caller and callee using a rule-based approach. This also includes the collection and analysis of diverse data points such as phone number type, device, carrier, ISP, VPN, etc.

Rebtel employs state-of-the-art verification products from Sinch, which verifies that the individual trying to use Rebte's service is de facto controlling the phone number being used and thus entitled to use that telephone number. In addition, as a provider of prepaid services, the customer payment process involves the collection and validation of certain customer information by Rebte's payment processors and Rebte's internal risk and fraud management systems.

Rebtel also monitors the Commission's guidance regarding robocalls. If Rebte becomes aware that a voice service provider or intermediate service provider is the recipient of a cease-and-desist letter from the Commission with respect to illegal robocall traffic, Rebte will consider whether to take steps to stop carrying traffic from the offending provider, as allowed under the Commission's rules.

II. ACTIONS RELATING TO UPSTREAM PROVIDERS

Rebtel shall take reasonable and effective steps to ensure that the immediate upstream provider ("IUP") of Rebte is not using it to carry or process a high volume of illegal traffic.

Rebtel shall purchase and use the carrier services from a few and carefully selected IUPs that are well recognized and reputed in the carrier market. Rebte shall not accept traffic from an IUP unless there is a written agreement in place. Rebte shall verify and only accept calls from an IUP if that IUP's filing appears in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action.

If Rebte is to engage with and accept traffic from a new IUP then Rebte shall perform a due diligence analysis of that IUP for the purpose of determining the risks of receiving illegal traffic from the IUP and otherwise to determine the general STIR/SHAKEN compliance level of the IUP. Such due diligence analysis may include collecting and verifying key details such as, registered address, office address, federal tax id and similar information. Furthermore, Rebte Head of Procurement and Legal Department shall be offered the opportunity to ask questions to the contemplated new IUP for understanding and verifying the IUP's efforts to combat illegal robocall traffic and general compliance level.

If Rebte is made aware that an IUP carries or transmits a high volume of illegal traffic Rebte shall promptly investigate and take necessary measures to effectively handle the situation, including working closely with the aforesaid IUP, enhanced monitoring and, unless an acceptable solution is timely reached, discontinue the use of the services of that IUP.

III. TRACEBACK COMMITMENT (<24-HOURS RESPONSE)

Rebtel commits to continue to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (currently U.S. Telecom's Industry Traceback Group) within 24 hours of receipt of such a request, and otherwise to cooperate

with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

IV. MANDATORY BLOCKING OF CALLS

Rebtel commits to, when acting as a downstream provider, to block traffic received directly from all IUPs that are not registered in the Robocall Mitigation Database.

In addition, RebteI commits to fully and timely comply with any request from the Commission to block illegal traffic, the aforesaid includes having the technical and organisational capabilities to promptly execute to the blocking request.

V. INFORMATION REGARDING PRINCIPALS, AFFILIATES, SUBSIDIARIES, AND PARENT COMPANIES

Rebtel is a wholly-owned direct subsidiary of, and controlled by, RebteI AB. No individual or entity controls RebteI AB. The only individuals or entities that hold a 10 percent or greater direct ownership interest in RebteI AB are Minority Invest II AB, Magnus Larsson, FHW Holding AB, and Askdalen Holding AB (all Swedish individuals or companies). RebteI has one subsidiary, RebteI Canada Inc., which is a Canadian company. RebteI Canada Inc. and the entities with a 10 percent or greater interest in RebteI AB do not provide communications services. In addition, RebteI's Executive Management Team includes: Thomas Skoglund, Chief Executive Officer and Chief Financial Officer; Johan Dahlqvist, Chief Technology Officer; Svante Pagels, Chief Product Officer; and Julia Loschinia, Head of Growth.
