

Robocall Mitigation Plan

This Robocall Mitigation Plan is for Telernet, LLC with headquarters located at 1822 51st Street, Brooklyn, NY 11204.

We currently use Bandwidth (RMD0003709) and Skyswitch (RMD0002940) as trusted third-party vendors for analytics, call authentication, and traffic monitoring. Vendors are contractually obligated to maintain FCC-compliant robocall mitigation and provide reporting to Telernet. Oversight measures include periodic audits and performance reviews of vendor compliance.

Enforcement Actions

Telernet was removed from the Robocall Mitigation Database on August 25, 2025, In the Matter of Robocall Mitigation Database Filers, Order at 4, para. 7, for failure to correct filing deficiencies of inadequate or insufficiently detailed KYC policy and failure to provide current contact information including contact email address. We attempted to correct the deficiencies and were granted Provisional Re-Instatement to the RMD. On November 19, 2025, the Enforcement Bureau notified us that our actions were not sufficiently detailed. We again attempted to correct the deficiencies both in the RMD and our RMP and remained Provisionally Instated. On January 14, 2026, the Enforcement Bureau again notified us that the action or investigation we were subject to that precipitated our removal from the RMD on August 25, 2025, was not sufficiently detailed. We appreciate the FCC's guidance and have provided a further updated description to ensure the action is sufficiently described. The description is currently pending review and approval by the FCC Enforcement Bureau: On August 25, 2025, In the Matter of Robocall Mitigation Database Filers, Order at 4, para. 7, Telernet was removed from the RMD by the FCC Enforcement Bureau for deficiencies in our description of our KYC policies and for failure to update our contact email information. Prior notices to the previous email address were not received because the address was incorrect. We corrected the email address and provided additional KYC policy information in our RMP and follow the NANC Call Authentication Trust Anchor Working Group's recommended best practices. We have been Provisionally reinstated to the RMD and are pending final reinstatement.

We use the affirmative and effective measures detailed below to prevent the origination or transit of illegal robocalls.

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Traceback

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

STIR/SHAKEN

Our network does not have the capability to implement STIR/SHAKEN and we rely on our carrier partners Bandwidth.com (RMD0003709) and Skyswitch (RMD0002940) to sign our calls. Bandwidth provides TNs and SIP trunks to our customers while Skyswitch provides a hosted platform (we resell their platform), acting as the first party in the call origination. Both partners are fully compliant with STIR/SHAKEN, therefore they certify our customer originations. We have completed our STIR/SHAKEN implementation with the STI-PA under OCN 403L and Bandwidth.com will use our own certificate through Telonium (STI-CA) to sign our calls upon completion.

All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

We use software provided by Bandwidth.com and Skyswitch to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

Combining behavioral analytics, caller authentication and verification, our solution features:

- ☐ **Fraud Detection:** Detection of high volume robocalling, spoofing and spam call activity.
- ☐ **Subscriber Notification:** Caller ID Name override to warn subscribers of suspicious calls.
- ☐ **Call Blocking Support:** Accurate identification enabling you to block fraudulent phone calls as per the TRACED Act (2019)
- ☐ **Business Number Verification:** Register legitimate business numbers to prevent unintentional call blocking.
- ☐ **Caller ID Name Service:** Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

In addition, we have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

“Any call originated on the Telernet, LLC network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the Telernet, LLC network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”