

Crystal Broadband Networks, Inc.

Robocall Mitigation Plan (RMP)

Objective

Crystal Broadband Networks, Inc. ("CBN") establishes this Robocall Mitigation Plan to comply with the TRACED Act and all current rules and requirements of the Federal Communications Commission (FCC), including 47 CFR § 64.6305.

I. Company Overview

Crystal Broadband Networks, Inc. ("CBN") is a small, long-established provider of broadband and cable TV services to subscribers across rural communities in Kentucky, Ohio, and West Virginia.

CBN provides interconnected VoIP and voice services to residential and small business customers and does not provide wholesale call origination services.

Crystal Broadband Networks, Inc. is registered with the FCC and operates under Operating Company Number (OCN) 900L.

CBN's customer base consists primarily of residential and small business subscribers with typical consumer call volumes.

II. STIR/SHAKEN Status

Crystal Broadband Networks, Inc. has obtained an Operating Company Number (OCN) and has received approval from STI-PA and is working toward implementation of the STIR/SHAKEN framework on its network.

At this time, STIR/SHAKEN has not yet been fully implemented, and therefore CBN files in the FCC Robocall Mitigation Database under the Robocall Mitigation Program certification, as permitted under 47 CFR § 64.6305.

CBN is actively evaluating technical solutions to support STIR/SHAKEN implementation in accordance with FCC requirements for IP-based voice networks.

Until STIR/SHAKEN is fully implemented, CBN relies on the robocall mitigation procedures described in this plan to prevent illegal robocall traffic from originating on its network.

III. Prohibition Against Illegal Robocalling

All CBN services are subject to our published Terms of Service (TOS) and Acceptable Use Policy (AUP), which strictly prohibit:

- The use of services to originate or facilitate illegal robocalls
- Altering or spoofing caller ID with false or misleading information
- Violations of local, state, or federal law, including fraudulent or deceptive activity
- Use of VoIP services for mass calling campaigns without authorization

CBN reserves the right to immediately suspend or terminate services found to be associated with illegal robocall activity.

IV. Know Your Customer (KYC) Procedures

CBN implements strict vetting procedures for new and renewing customers.

These include:

Residential Restrictions

No large-capacity call paths are assigned to residential customers.

Business Verification

Businesses requesting higher-capacity calling services must provide a tax identification number and verification of legitimate business purpose.

Location Verification

CBN representatives may inspect business locations to ensure the number of users is consistent with expected calling volume.

Account Security

Customer identity verification procedures and personally identifiable information checks are used when establishing or modifying service accounts to prevent fraudulent activity.

V. Know Your Upstream Provider (KYUP) Procedures

CBN only exchanges traffic with upstream providers that:

- Maintain a valid certification in the FCC Robocall Mitigation Database
- Contractually agree to maintain robocall mitigation programs
- Cooperate with traceback investigations

CBN actively monitors upstream providers and will block or refuse traffic from providers that transmit illegal robocall traffic or are removed from the Robocall Mitigation Database.

VI. Network Monitoring and Analytics

CBN continuously monitors call traffic to detect potential robocall activity.

Monitoring methods include:

Real-Time Monitoring

Network engineers monitor call detail records, PBX logs, and traffic analytics systems.

Traffic Pattern Analysis

Traffic is evaluated for abnormal calling patterns including:

- Excessive short-duration calls
- Unusually high call attempts per second
- Call completion rates inconsistent with normal user behavior
- Large bursts of outbound calls to sequential numbers
- Traffic patterns associated with high complaint or scam call activity

Mitigation Response

When suspicious or illegal robocall patterns are detected, CBN will:

- Immediately suspend the customer's ability to place outbound calls
- Investigate the customer's traffic activity
- Require explanation and remediation from the customer
- Terminate service if violations are confirmed

CBN does **not provide services to call center, dialer platforms, or entities engaged in high-volume automated calling campaigns.**

VII. Traceback and Enforcement Cooperation

CBN actively cooperates with traceback requests from:

- Federal regulators
- Law enforcement agencies
- The Industry Traceback Group (ITG)

CBN responds to traceback requests **within 24 hours or within the timeframe required by applicable regulations** and provides relevant call detail records and supporting information necessary to investigate suspected illegal robocall activity.

VIII. Certification Alignment

This Robocall Mitigation Plan corresponds to CBN's certification in the FCC Robocall Mitigation Database.

CBN commits to updating both its certification and this mitigation plan if its STIR/SHAKEN implementation status changes or if additional mitigation procedures are adopted.

IX. Record Retention

CBN maintains sufficient records to support robocall mitigation enforcement and traceback investigations.

These records may include:

- Customer account records
- Call detail records
- Traffic monitoring logs
- Internal investigation records

Such records are retained for a period of at least two (2) years to support investigations and comply with regulatory requirements.

X. Responsible Contact for Robocall Mitigation

Crystal Broadband Networks, Inc. designates the following individual as the primary point of contact responsible for implementation and enforcement of this Robocall Mitigation Plan and for responding to traceback requests and regulatory inquiries.

Name: Prasanna Balasundaram

Title: Network Manager

Organization: Crystal Broadband Networks, Inc.

Email: prasanna@crystalbn.com

Phone: 606-663-3439

This individual is authorized to coordinate internal investigations and provide responses to traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Group.

XI. Disclosure of Enforcement History

CBN certifies that neither the company nor any entity with which it shares common ownership, management, directors, or control has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation regarding illegal robocalling or spoofing within the last two years