



Robocall Mitigation Program Description 12.3.2025

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Crown Enterprises

FCC Robocall Mitigation Database Filing – Partial STIR/SHAKEN Implementation December 2025

1. Overview

Crown Enterprises is a Managed Services Provider (MSP) and communications solutions provider that originates voice calls exclusively through **Bandwidth.com**, a certified, fully STIR/SHAKEN-compliant Voice Service Provider (VSP). Crown Enterprises does **not** have direct IP-to-IP interconnection capabilities with the PSTN and therefore cannot implement STIR/SHAKEN within its own network. In accordance with **47 CFR § 64.6304(a)**, our organization qualifies for the FCC exemption permitting reliance on an upstream VSP to perform STIR/SHAKEN authentication on our behalf.

All calls we originate on Bandwidth's network receive the appropriate **STIR/SHAKEN attestation (A, B, or C)** and Bandwidth inserts the required authentication headers before transmission.

For all calls **not authenticated** by Bandwidth (if any), Crown Enterprises operates a comprehensive **robocall mitigation program** consistent with **47 CFR § 64.6305(a)**, including reasonable steps to prevent the origination of illegal robocall traffic and a commitment to respond within **24 hours** to traceback requests.

2. Applicability of FCC Exemption (STIR/SHAKEN)

Rule Citation

Crown Enterprises is exempt under:

47 CFR § 64.6304(a)

"Exemption for a voice service provider that relies on another voice service provider for caller ID authentication."

Justification for Exemption

- All outbound calls use **Bandwidth.com**, a fully STIR/SHAKEN-enabled provider.
- Bandwidth performs **all authentication and SIP header signing**.
- Crown Enterprises does not operate a SIP interconnect or IP multimedia subsystem.
- The FCC's STIR/SHAKEN Orders (WC Docket No. 17-97) explicitly allow downstream providers to rely on upstream carriers for authentication where the downstream provider is not positioned to deploy STIR/SHAKEN directly.

Reference:

FCC Fourth Report and Order – WC Docket 17-97

<https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf>

Bandwidth STIR/SHAKEN Compliance:

<https://www.bandwidth.com/legal/stir-shaken/>

3. Robocall Mitigation Procedures (47 CFR § 64.6305(a))

Crown Enterprises maintains a comprehensive mitigation program for any call paths not signed by Bandwidth. Our program includes:

a. Reasonable Steps to Prevent Illegal Robocalls

- **Know Your Customer (KYC):**
Each client requesting outbound calling must be verified through business registration, identity validation, and service agreement review.
- **Know Your Use Case (KYUC):**
Customer call-flow intent, traffic patterns, contact lists, and campaign types are reviewed prior to enabling calling services.
- **Outbound Traffic Monitoring:**
Using Bandwidth analytics, Autotask PSA logs, and internal monitoring systems to identify:
 - High-volume spikes
 - Short-duration patterns
 - Sequential dialing
 - Abnormal ANI usage
- **Blocking and Suspension:**
Immediate disablement of outbound call capabilities for any customer showing signs of illegal or suspicious traffic.

4. Traceback Cooperation

Crown Enterprises commits to:

- Responding fully to traceback requests from the **FCC**, **law enforcement**, or the **Industry Traceback Group (ITG)** within **24 hours**, as required by **47 CFR § 64.6305(a)**.
- Maintaining detailed logs of outbound call activity.
- Cooperating with traceback investigators, including forwarding SIP logs, call records, and customer information (consistent with applicable law).

Crown Enterprises has **never refused** a traceback request.

5. Complaint Intake & Escalation

We maintain the following channels for receiving abuse complaints:

- support@ce-technology.com
- Abuse ticket categorization in Autotask
- Direct engineer and management review

Complaints are triaged within **one business day** and escalated to management for rapid remediation.

6. Prior Enforcement or Wrongdoing

There has been **no enforcement action, investigation, or finding of wrongdoing** by the FCC, law enforcement, or any regulatory authority related to illegal robocalls or call authentication.

The only recent activity was an **administrative request** from the FCC to update our existing Robocall Mitigation Database filing under the new 2024–2025 rules.

We provided the required documents and were **provisionally restored**.

No violations were alleged or found.

7. Network Security & Access Controls

We implement the following controls to prevent unauthorized or malicious calling:

- Multi-factor authentication (MFA)
 - Access control and least-privilege principles
 - Firewall restrictions on outbound SIP
 - Logging and auditing of all call-routing configurations
 - Internal review for any customer adding new outbound caller IDs or DID ranges
-

8. Ongoing Compliance and Review

Our robocall mitigation program is reviewed quarterly and updated as FCC rules change. Crown Enterprises is committed to:

- Maintaining compliance with **47 CFR § 64.6305(a)**
 - Ensuring all calls traversing Bandwidth's network receive proper STIR/SHAKEN authentication
 - Preventing illegal robocall traffic from originating on our systems
 - Cooperating fully with traceback and enforcement efforts
-

Certification

Crown Enterprises certifies that the above Robocall Mitigation Program is accurate, complete, and compliant with FCC requirements for the Robocall Mitigation Database under Option 2: Partial STIR/SHAKEN Implementation.

Signed:

Mark Williams
CEO, Crown Enterprises
Date: 12/3/2025