



# ConnX Robocall Mitigation and STIR/SHAKEN Compliance Plan

Version 3.0

# Version Control

| Version Number | Author of Change | Date          | Changes/Comments                 |
|----------------|------------------|---------------|----------------------------------|
| 1.0            | Mark Beranek     | Jan 1st 2026  | Initial Document Creation        |
| 2.0            | Mark Beranek     | Mar 1st 2026  | Revisions to Stir/Shaken         |
| 3.0            | Heather Palmucci | April 13 2026 | Added Know Your Customer section |
|                |                  |               |                                  |

## Table of Contents

|                                             |    |
|---------------------------------------------|----|
| Version Control.....                        | 2  |
| Introduction.....                           | 4  |
| Regulatory Context.....                     | 4  |
| ConnX Robocall Mitigation Architecture..... | 5  |
| STIR/SHAKEN Implementation .....            | 7  |
| Robocall Mitigation Program .....           | 8  |
| Monitoring and Reporting.....               | 8  |
| Upstream Provider KYC Procedures.....       | 11 |
| Summary .....                               | 16 |

## Introduction

ConnX is committed to supporting the Federal Communications Commission (FCC) mandate to protect consumers and enterprises from unwanted robocalls and call spoofing. Leveraging a combination of Ribbon Communications, Cisco Webex Calling, AudioCodes Session Border Controllers (SBCs), and partnerships with major PSTN providers such as AT&T and PureIP, ConnX delivers a comprehensive solution for call authentication, fraud detection, and spam blocking.

ConnX also integrates TransNexus robocall mitigation and fraud detection platforms, which interact with both Ribbon and AudioCodes SBC infrastructure to provide advanced real-time call analysis and mitigation. This document defines how ConnX implements and enforces these protections in compliance with FCC requirements, including the STIR/SHAKEN framework.

ConnX is a provider of managed cloud PBX and SBC services and utilizes third parties to support PSTN access.

## Regulatory Context

The FCC requires voice service providers to:

1. Implement STIR/SHAKEN standards on IP-based voice networks.
2. Establish robocall mitigation programs to block unlawful or fraudulent calls.
3. Report compliance with the Robocall Mitigation Database (RMD).

ConnX meets these obligations by integrating best-in-class vendor solutions including Ribbon Communications, Cisco, AudioCodes SBC platforms, TransNexus robocall mitigation technology, and PSTN provider partnerships that provide robust call authentication, spam detection, and policy enforcement.

# ConnX Robocall Mitigation Architecture

## 1. Cisco Secure Voice and Policy Enforcement

- **Cisco Unified Border Element (CUBE):** Enables integration with advanced call filtering services (e.g., Mutare Voice Traffic Filter) to screen inbound PSTN calls.
- **Webex Calling Caller ID Validation:** Implements STIR/SHAKEN authentication and displays verification status to end users.
- **Block Lists & Anonymous Call Rejection:** Administrators can configure global block lists and reject anonymous/private calls directly within Cisco platforms.

---

## 2. Ribbon Communications Call Security

- **Ribbon Session Border Controllers (SBCs):** Enforce granular call screening and blocking rules based on caller ID, origin, destination, and risk assessment.
- **TransNexus:** SIP trunk and SBC platforms exchange call metadata for scoring calls to further support Robo call prevention and support Stir/Shaken tagging to up steam carriers

---

## 3. AudioCodes SBC Robocall Mitigation and TransNexus Integration

ConnX also deploys AudioCodes Mediant SBC platforms as part of its enterprise edge and carrier interconnect infrastructure. AudioCodes SBCs provide advanced call routing, signaling control, and security enforcement that support robocall mitigation programs and integration with TransNexus fraud prevention systems.

Key capabilities include:

- **SIP Signaling Inspection and Filtering**  
AudioCodes SBCs analyze SIP signaling metadata including caller identity, headers, call rate patterns, and source networks to detect suspicious call activity.
- **STIR/SHAKEN Support**  
AudioCodes SBCs support the signing and verification of STIR/SHAKEN

Identity headers, allowing ConnX to authenticate outbound calls and validate inbound calls before delivery to enterprise platforms.

- **Transnexus Integration**

AudioCodes SBCs can interface with TransNexus systems through SIP signaling control and policy enforcement mechanisms. TransNexus provides real-time robocall detection, reputation analysis, and call scoring. When high-risk calls are detected, mitigation policies can be dynamically applied by the SBC, including blocking, call diversion, or additional verification.

- **Dynamic Call Blocking Policies**

Based on TransNexus risk scoring, AudioCodes SBCs can enforce mitigation actions such as:

- Blocking suspected robocalls
- Rate limiting suspicious call sources
- Redirecting calls to verification systems or IVR screening
- Logging events for regulatory reporting

- **Enterprise Edge Protection**

AudioCodes SBCs deployed at the enterprise edge provide an additional layer of call security, ensuring that robocall mitigation policies are enforced before calls reach customer PBX or collaboration systems.

## 4. Webex Calling STIR/SHAKEN and Spam Blocking

- **Caller ID Validation:** Webex Calling natively supports STIR/SHAKEN, blocking or labeling calls that fail attestation.
- **Control Hub Policies:** Administrators can configure system-wide call blocking, including spam/fraud detection, number patterns, or country codes.
- **End-User Controls:** Webex App users can block external numbers, report spam, and enable anonymous call rejection.
- **Third-Party Integration:** Mutare's Voice Traffic Filter can be deployed via Cisco CUBE to add AI-driven threat detection, reputation databases, and CAPTCHA-based bot mitigation.

## 5. PSTN Provider Partnerships (e.g., AT&T Active Armor)

ConnX leverages major PSTN provider services to extend robocall mitigation beyond enterprise borders:

- **AT&T Active Armor and Call Protect**  
Provides carrier-level blocking and labeling of suspected robocalls before they reach ConnX networks.
- **STIR/SHAKEN Enforcement at Carrier Level**  
AT&T and other PSTN providers sign and validate calls within their networks, complementing ConnX's own authentication services.
- **Caller Reputation Services**  
Providers like AT&T share spam detection intelligence with ConnX systems, enabling faster threat identification and enhanced mitigation.
- **Layered Defense**  
By combining PSTN-level filtering with ConnX's enterprise security stack (Ribbon, AudioCodes, Cisco, TransNexus), customers benefit from multi-tiered protection across the call path.

## STIR/SHAKEN Implementation

The product development team ConnX leverages Ribbon, Cisco, AudioCodes, Webex, TransNexus and PSTN provider technologies to fully comply with the STIR/SHAKEN call authentication framework.

- **Signing**  
Outbound calls originating from ConnX networks are digitally signed using SBC platforms including Ribbon and AudioCodes to verify caller identity.
- **Verification**  
Inbound calls are checked for valid signatures; unverified calls are flagged or blocked based on defined mitigation policies.
- **Reputation Scoring**  
TransNexus, Orchestra One, AudioCodes and Ribbon signaling analytics, and PSTN provider intelligence enhance STIR/SHAKEN by assigning dynamic risk scores, while Cisco/Webex display attestation levels (A, B, C) to end users.

## Robocall Mitigation Program

Product ConnX deploys a multi-layered mitigation strategy:

### **Real-Time Threat Detection**

Ribbon and AudioCodes SBCs combined with TransNexus Call Defense, Mutare Voice Traffic Filter, AudioCodes SBC analytics, and PSTN provider intelligence continuously monitor call patterns.

### **Dynamic Block Lists**

Cisco, Webex, Ribbon, AudioCodes, TransNexus and AT&T services enforce administrator-managed and automated blacklists.

### **TransNexus Policy Enforcement**

TransNexus systems analyze call metadata and provide dynamic mitigation recommendations which can be enforced at SBC layers including Ribbon and AudioCodes.

### **End-User Empowerment**

Webex App provides user-level controls for spam blocking and anonymous call rejection.

### **Outbound Number Protection**

AudioCodes and Ribbon SBC's with TransNexus Reputation Defense, AudioCodes SBC validation controls, PSTN provider caller ID branding, and Cisco/Mutare integration prevent spoofing of ConnX customer numbers.

## Monitoring and Reporting

ConnX monitors call traffic patterns and mitigation effectiveness through analytics generated by SBC platforms, TransNexus systems, and PSTN provider reporting. These systems provide visibility into:

- Suspicious calling patterns
- Blocked or mitigated robocalls
- STIR/SHAKEN attestation statistics
- Caller reputation scoring

ConnX maintains documentation of its robocall mitigation program and updates its Robocall Mitigation Database certification in accordance with FCC requirements.

## Overview

This Know Your Customer (KYC) Policy establishes procedures to identify, verify, and monitor customers and upstream providers using ConnX and Pure IP voice services. The policy ensures compliance with FCC robocall mitigation requirements, including 47 CFR § 64.1200(n) and § 64.6305. ConnX maintains documented procedures to identify, verify, risk-assess, and continuously monitor all end-user customers prior to and during service provision.

## Scope

### **The ConnX policy applies to:**

- All end-user customers utilizing ConnX-based services
- All upstream providers and carriers interconnected via Pure IP routing
- All internal personnel responsible for onboarding, compliance, and traffic monitoring

## Regulatory Basis

### **This policy is designed to comply with:**

- 47 CFR § 64.1200(n)(4) – Requirement to know end-user customers
- 47 CFR § 64.1200(n)(5) – Requirement to know upstream providers
- 47 CFR § 64.6305(d), (e), (f) – Robocall mitigation plan disclosure requirements

## Mandatory Customer Identification Controls

The controls outlined in this section ensure ConnX "knows its end users" in a manner consistent with § 64.1200(n)(4). Prior to service activation, ConnX requires collection of:

- Legal name and any DBA
- Physical address (no P.O. boxes unless supplemented)
- Valid contact information
- Government-issued identification (individuals)
- Business registration and EIN (entities)

- Authorized representative credentials

## Verification Standards

### **Verification is conducted using:**

- Independent database validation (state registration, EIN where applicable)
- Identity authentication procedures
- Contact verification (email/phone confirmation)
- Manual compliance review for exceptions

## Intended Use Disclosure Requirements

### **Customers must provide:**

- Detailed use case description
- Call origination type (inbound/outbound/mixed)
- Use of automated dialing or prerecorded content
- Estimated traffic volumes and destinations

## Risk-Based Controls

### **ConnX applies a formal risk scoring model:**

- Low Risk: minimal outbound traffic, established operations
- Medium Risk: moderate outbound activity
- High Risk: high-volume outbound or regulated verticals

### **High-risk customers are subject to Enhanced Due Diligence (EDD), including:**

- Additional documentation review
- Campaign-level scrutiny
- Senior compliance approval

## Continuous Monitoring and Detection

### **Using ConnX analytics, the Company monitors:**

- Call Detail Records (CDRs)
- Short duration call ratios
- Answer Seizure Ratios (ASR)
- Traffic spikes and anomalies
- Complaint and traceback data

## Enforcement Framework

### **ConnX enforces compliance through:**

- Immediate investigation triggers
- Traffic blocking or throttling
- Suspension or termination of service
- Escalation to regulators or traceback entities where required

## Upstream Provider KYC Procedures

### **Provider Verification**

ConnX performs due diligence and continuous oversight of all upstream providers delivering traffic into its network. The controls defined in this section ensure ConnX "knows its upstream providers" consistent with § 64.1200(n)(5). ConnX fully documents and implements its mitigation program consistent with § 64.6305 requirements.

Before interconnection via Pure IP and other carriers :

- Verify provider identity, licensing (if applicable), and reputation

- Confirm participation in industry traceback efforts (e.g., US Telecom ITG)
- Review robocall mitigation plan filings (FCC database) ☐
- Legal entity identification
- Jurisdictional registration verification
- Operational and compliance contacts

### **Technical Validation**

- Validate STIR/SHAKEN implementation status
- Ensure proper SIP header integrity and traceability via ConnX routing

### **Contractual Requirements**

- Require contractual commitments to:
  - Prohibit illegal robocalls
  - Maintain their own KYC procedures
  - Cooperate with traceback and enforcement

### **Ongoing Monitoring**

- Monitor inbound traffic from upstream providers for:
  - High complaint ratios
  - Invalid or spoofed caller ID patterns
- Restrict or block traffic from non-compliant providers

### Documentation & Robocall Mitigation Plan

#### **ConnX will perform the following to ensure the KYC procedures are adhered to by the following:**

- Documenting all KYC procedures in its robocall mitigation plan
- Maintaining records of customer verification and monitoring activities
- Updating procedures as FCC rules evolve

## Role of ConnX and Pure IP

### **ConnX Platform:**

- Provides customer onboarding workflows and verification tracking
- Enables traffic monitoring, analytics, and anomaly detection
- Supports enforcement actions (blocking, suspension)

### **Pure IP Infrastructure:**

- Ensures end-to-end SIP transparency and traceability
- Enables validation of upstream providers and call paths
- Supports STIR/SHAKEN authentication frameworks
- Works together with ConnX to ensure end to end authentication

## Traceback and Cooperation

### **ConnX support traceback cooperation utilizing the following steps:**

- Responds promptly to traceback requests
- Maintains sufficient records to identify call originators
- Cooperates with industry traceback groups

## Technology Enablement

### **ConnX Platform:**

- Centralized KYC recordkeeping
- Real-time analytics and alerting
- Automated enforcement capabilities

### **Pure IP Network:**

- SIP-level traceability
- Caller ID validation
- STIR/SHAKEN integration

## Record Retention

ConnX maintains and retains all KYC-related documentation, including customer verification records, monitoring logs, and enforcement actions, for a period of no less than five (5) years, consistent with industry best practices and to ensure audit readiness and timely response to regulatory and traceback inquiries.

**ConnX retains the following:**

- KYC documentation
- Monitoring logs
- Enforcement actions
- Provider verification records

**Audit Checklist**

ConnX affirms that its KYC procedures are comprehensive, enforced, and fully aligned with FCC robocall mitigation requirements. These procedures ensure accountability across all customers and upstream providers and provide demonstrable compliance during regulatory review or audit.

**End-User KYC Audit**

**Audit Requirements:**

**ConnX Support and Controls:** ConnX supports end-user KYC compliance by:

- Providing structured onboarding workflows that require mandatory data fields before activation
- Storing and centralizing all customer documentation for audit retrieval
- Enabling tagging and classification of customers by risk level
- Integrating traffic analytics with customer profiles to correlate behavior with onboarding data
- Generating alerts when customer activity deviates from declared use cases

## **Upstream Provider Audit**

### **Audit Requirements:**

**ConnX Support and Controls:** ConnX enables upstream provider compliance by:

- Maintaining provider profiles with associated compliance documentation
- Mapping inbound traffic to specific upstream providers for traceability
- Monitoring provider-specific traffic patterns and performance metrics
- Flagging anomalies such as high volumes of unsigned or suspicious traffic
- Supporting rapid identification and isolation of problematic providers

## **Monitoring & Enforcement Audit**

### **Audit Requirements:**

**ConnX Support and Controls:** ConnX provides monitoring and enforcement capabilities by:

- Delivering real-time traffic analytics and dashboards
- Detecting anomalies such as traffic spikes, low answer rates, or robocall signatures
- Enabling configurable alert thresholds and automated triggers
- Allowing immediate enforcement actions including blocking, routing changes, and throttling
- Maintaining logs of all actions taken for compliance and audit purposes

## **Documentation Audit**

### **Audit Requirements:**

**ConnX Support and Controls:** ConnX supports documentation and audit readiness by:

- Serving as a centralized repository for KYC records and compliance documentation
- Maintaining historical logs of customer onboarding, monitoring, and enforcement actions
- Enabling quick retrieval of records for audit or regulatory inquiries
- Providing reporting capabilities that demonstrate compliance trends and actions taken

## Summary

ConnX maintains a comprehensive robocall mitigation program using a layered security model including:

- STIR/SHAKEN call authentication
- SBC-based call inspection and enforcement (Ribbon and AudioCodes)
- Robocall analytics and mitigation using TransNexus
- Enterprise call control platforms (Cisco Webex Calling)
- Carrier-level protections from PSTN providers
- Know Your Customer procedures

These measures enable ConnX to authenticate legitimate calls, detect suspicious call patterns, and block or mitigate unlawful robocalls consistent with FCC regulations.