

ROBOCALL MITIGATION PLAN

ConnectX Global Services LLC, doing business as MyConnectX

Provider type	Domestic interconnected VoIP reseller serving business end users
FCC Registration Number	0038875381
Principal and responsible officer	Newman G. Rincon, Owner
Robocall mitigation contact	newman@myconnectx.com (832) 369-6711
Primary business address	5002 Glenmont Dr, Houston, Texas 77081
Underlying voice platform	RingLogix LLC d/b/a CarrierOfRecord.IO - RMD0002349
Effective date	September 13, 2026

1. Purpose and scope

This Plan describes the affirmative and effective measures used by ConnectX Global Services LLC ("ConnectX") to prevent its services from being used to originate illegal robocalls or unlawfully spoof caller identification information. It applies to all voice customers, telephone numbers, users, administrators, and outbound calls furnished under the MyConnectX brand.

ConnectX provides hosted, interconnected VoIP service to business end users. ConnectX does not operate a gateway service, does not act as a non-gateway intermediate provider, and does not offer wholesale voice origination to other providers. International calling is blocked unless separately authorized.

2. STIR/SHAKEN status and network responsibility

ConnectX is a pure reseller of the hosted VoIP platform supplied by RingLogix LLC. ConnectX does not own or control the switching, session border controller, certificate, or other network infrastructure necessary to implement STIR/SHAKEN, and it does not possess an SPC token or STIR/SHAKEN certificate. Accordingly, ConnectX is a voice service provider without its own STIR/SHAKEN implementation obligation because it lacks control over the necessary network infrastructure.

RingLogix, the originating wholesale network provider, is listed in the FCC Robocall Mitigation Database as RMD0002349 and reports complete STIR/SHAKEN implementation. RingLogix performs caller ID authentication on the calls it originates onto the public network pursuant to its own FCC obligations. ConnectX supplies RingLogix with customer identity, telephone-number authorization, and traceback information sufficient to support appropriate attestation decisions.

RMD filing position: Voice Service Provider filing; domestic provider; voice service provider without a STIR/SHAKEN implementation obligation; no STIR/SHAKEN implementation by ConnectX. The basis is ConnectX's lack of control over the network infrastructure necessary to implement STIR/SHAKEN, as recognized in 47 CFR 64.6305(d)(2)(i) and FCC 24-120.

3. Know Your Customer program

ConnectX provides service only after identifying the customer and evaluating whether the requested service and anticipated calling activity are consistent with a legitimate business purpose. Anonymous, fictitious, or unverifiable customer accounts are not permitted.

Customer information and verification

- Legal business name, any DBA, service and billing addresses, main telephone number, business email domain, website when available, and the name and contact information of an authorized representative.
- Entity registration or other reliable business records are reviewed when reasonably available. Additional documentation, including tax identification or government-issued identification, may be requested when identity or authority cannot otherwise be verified.

- The intended use of the service, expected number of users, calling pattern, service locations, and any use of automated dialing, prerecorded messages, telemarketing, lead generation, or high-volume outbound calling are reviewed before activation.
- ConnectX documents the customer relationship and retains account, order, assignment, support, billing, and investigation records sufficient to identify the customer and respond to traceback requests.

Telephone-number authorization and caller ID

- Customers may present only telephone numbers assigned, ported, or otherwise validated for their use through ConnectX and RingLogix.
- Arbitrary caller ID substitution, impersonation, number spoofing, and presentation of invalid, unallocated, or unauthorized numbers are prohibited.
- ConnectX provides RingLogix with information needed to trace each assigned number to the responsible customer and to assess the customer's authorization to use the calling number.

4. Customer rules and acceptable use

Use of MyConnectX voice service is conditioned on compliance with the Telephone Consumer Protection Act, Telemarketing Sales Rule, federal and state do-not-call requirements, caller ID and spoofing laws, consent requirements, and all other applicable robocall and telemarketing rules. Customers may not use the service to transmit illegal robocalls, scam calls, abusive calls, or calls intended to defraud, harass, or mislead.

- Customers must maintain all consent, registration, do-not-call suppression, and campaign records required for their calling activity.
- Customers must promptly answer ConnectX compliance inquiries and provide evidence supporting the legitimacy of their traffic and their right to use each calling number.
- ConnectX may restrict dialing, suspend service, block numbers or destinations, or terminate service immediately when traffic is unlawful, presents an imminent risk, or the customer does not cooperate with an investigation.

5. Traffic monitoring and analytics

ConnectX relies on network controls and analytics supplied by RingLogix and supplements them with account-level review of complaints, unusual usage, support activity, and other risk indicators. RingLogix represents that its platform monitors outbound traffic and can block or alert on suspicious calls, including calls using invalid, unallocated, do-not-originate, unauthorized, or poor-reputation calling numbers.

ConnectX reviews indicators that may include:

- Sudden or unexplained increases in outbound call volume, very short-duration calls, repeated sequential dialing, or traffic inconsistent with the customer's stated business purpose.
- Consumer complaints, traceback requests, carrier notifications, number-reputation alerts, high answer-seizure ratios, or repeated calls to numbers on suppression lists.
- Use of multiple or recently changed calling numbers, presentation of numbers not assigned to the customer, credential compromise, or calling outside the customer's normal locations and hours.

6. Investigation, blocking, and remediation

When suspicious traffic is identified, ConnectX will:

- 1 Preserve relevant customer, number-assignment, call-detail, support, and alert records.
- 2 Contact the customer and require a prompt explanation and supporting evidence.
- 3 Coordinate with RingLogix to trace the traffic, restrict affected credentials or numbers, and block suspected illegal traffic where warranted.
- 4 Suspend or terminate service if the traffic is likely unlawful, if the customer fails to cooperate, or if suspicious activity continues after warning.
- 5 Document the decision, remediation, and any notice or information provided to the FCC, law enforcement, the Industry Traceback Group, RingLogix, or another carrier.

7. Traceback response and cooperation

ConnectX commits to respond fully and in a timely manner to all traceback requests from the Federal Communications Commission, law enforcement, and the registered Industry Traceback Group, and to cooperate in investigating and stopping illegal robocallers that use its service. ConnectX targets a response within 24 hours when sufficient information is available and will always respond within the deadline stated in the request.

- The responsible contact monitors newman@myconnectx.com and can be reached at (832) 369-6711.
- ConnectX will identify the responsible end-user customer, the telephone number used, relevant account details, and the upstream/originating network provider, subject to lawful process and applicable privacy requirements.
- ConnectX will promptly coordinate with RingLogix at compliance@ringlogix.com and preserve records necessary to trace the call to the originating customer.
- No contractual or technical arrangement may be used to delay or avoid cooperation with the FCC, law enforcement, the Industry Traceback Group, or downstream providers investigating unlawful traffic.

8. Training, records, and governance

- Personnel responsible for sales, provisioning, support, and administration are instructed to escalate suspected spoofing, scams, unlawful automated calling, account compromise, and traceback requests to the Owner.
- ConnectX retains records adequate to identify customers and investigate traffic for at least two years after account closure or for any longer period required by applicable law, legal hold, or contractual obligation.
- The Owner reviews this Plan at least annually and after a material network, provider, ownership, product, or regulatory change. RMD information will be updated within 10 business days of a change and recertified annually by March 1.

9. Enforcement and investigation history

As of the effective date of this Plan, ConnectX, its principal, and any entity under common ownership, management, directors, or control have not been prohibited from filing in the RMD and have not, during the preceding two years, been the subject of a formal FCC, law-enforcement, or regulatory action or investigation with findings of actual or suspected wrongdoing related to illegal robocalling, spoofing, or a deficient RMD filing. ConnectX will revise its RMD filing within 10 business days if this statement changes.

10. Regulatory references

- 47 CFR 64.1200(n)(4): affirmative, effective measures to prevent customers from originating illegal calls, including customer knowledge and due diligence.
- 47 CFR 64.6305(d): voice-service-provider robocall mitigation, certification, program description, traceback cooperation, and filing information.
- FCC 24-120, paragraphs 17-19 and note 82: the wholesale originating provider, rather than a reseller lacking control of the necessary network infrastructure, bears the STIR/SHAKEN implementation obligation.
- FCC Public Notice DA 26-72, Appendix A: 2026 RMD filing guidance, including KYC, analytics disclosure, annual recertification, and ten-business-day updates.
- RingLogix LLC, RMD0002349, and RingLogix reseller mitigation guidance last updated February 13, 2026.

Program owner	Newman G. Rincon, Owner
Approval	Approved as company policy upon submission of the related RMD certification.