

Robo Call Mitigation Plan

Company Identification

- Entity Name: Syndeo Networks Inc
- Entity Type: Private Sector, Corporation
- FRN: 0021039672
- Contact Organization: Syndeo Networks
- Contact Position: CEO
- Contact Name: Amit Patel
- Contact Address: 320 Cardinal DR Suite 300, St Charles, Illinois 60175, United States
- Contact Email: compliance@syndeonetworks.com
- Contact Phone: 6304574218

Compliance Contact

Amit Patel, CEO

compliance@syndeonetworks.com

apatel@syndeonetworks.com

630-457-4218

Robocall Mitigation Program

We use call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.

The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number is invalid, unallocated, or on a Do Not Originate list.

We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

STIR/SHAKEN

We have registered with the STI-PA using OCN 656G. We have our own STIR/SHAKEN certificate issued by theTransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.

Compliance with Traceback requests

Syndeo Networks will cooperate with traceback requests received from other carriers, industry groups, and any/all law enforcement agencies by providing available call logs and CDRs to and from endpoints that utilize Syndeo's phone network. Traceback requests can be sent via email to: traceback@syndeonetworks.com Called in and submitted tickets via a support representative calling: 630.457.4218

Know Your Customer

Syndeo does not utilize third-party verification service to verify all customers. Syndeo voice services are bundled with Syndeo internet service. Business's name and address is verified at the time of installation by Syndeo Staff.

Syndeo's client base is comprised of low-risk local business and residential customers that Syndeo has worked with on a personal client by client basis. Syndeo confirms the identity of customers and potential use of service by collecting information such as physical business location, contacts person(s), federal tax ID, intended use of systems/services, and nature of the potential customer's business. Approval of any potential customers that exist outside of Syndeo's immediate geographical region would be subject to additional scrutiny as to intent of service use.

Monitoring

Syndeo sets alarm profiles on its Session Border Controller for customer and carrier connections that alerts staff if suspicious traffic volume is detected on its network. Additionally, Syndeo's upstream SIP partners monitor calls for suspicious behaviors and block calls identified as malicious. 4. Call Limits Syndeo limits total # of simultaneous calls per customer trunk which in turn limits the potential for significant origination.

Taking Action to Mitigate Illegal Traffic

Syndeo will take action to block illegal originating traffic when notified by the appropriate authorities or if suspicious/illegal traffic is detected by Syndeo's own monitoring solutions/processes.

Customer Acceptable Use Policy

Syndeo requires all new customers to sign an acceptable use policy that explicitly states that use of service must comply with all applicable laws.

FCC Findings

Perfect! I found it - **RMD0010687 SYNDEO NETWORKS, INC** appears in DA 25-694 (August 6, 2025 order). Here's the corrected response for Syndeo Networks:

Response to Question Regarding Regulatory Actions/Investigations:

Yes.

(1) **Law enforcement or regulatory agencies involved:** Federal Communications Commission (FCC) Enforcement Bureau

(2) **Date action commenced:** March 29, 2024 (initial notice of deficiency); December 10, 2024 (Show Cause Order)

(3) **Current status:** Syndeo Networks, Inc. was removed from the FCC Robocall Mitigation Database pursuant to FCC Enforcement Bureau Order DA 25-694 (adopted August 6, 2025). The company has completed all required corrective actions and is seeking reinstatement.

(4) **Summary of findings:** Syndeo Networks, Inc. was removed from the Robocall Mitigation Database for failure to update its RMD certification and robocall mitigation plan by the February 26, 2024 deadline as required by amended 47 CFR § 64.6305. The non-compliance occurred because update notifications from the FCC Wireline Competition Bureau (sent March 29, 2024) and the Enforcement Bureau Show Cause Order (issued December 10, 2024, with a December 31, 2024 compliance deadline) were sent to a contact email address associated with



Syndeo Networks, Inc.
PO Box 833
St. Charles, IL. 60175
Phone: (630) 457-4218
Fax: (630) 457-4240
www.syndeonetwork.com

a former employee who had departed the company. The company failed to implement proper email forwarding and monitoring procedures during the personnel transition, resulting in missed FCC communications. No findings of illegal robocalling practices, TCPA violations, or involvement with illegal robocall traffic were made against Syndeo Networks, Inc.

(5) **Final determinations:** The FCC Enforcement Bureau issued Order DA 25-694 (released August 6, 2025) removing Syndeo Networks, Inc. from the Robocall Mitigation Database. As a result, all intermediate providers and voice service providers were required to cease accepting traffic directly from Syndeo Networks, Inc. within two business days of the order release. The order specifies that Syndeo Networks, Inc. shall not refile in the RMD without prior consent from both the FCC Wireline Competition Bureau and Enforcement Bureau.

Syndeo Networks, Inc. has since: (a) updated all contact information in its filing with current, actively monitored email addresses monitored by multiple personnel; (b) completed all outstanding RMD certification updates including the robocall mitigation plan with all required information under 47 CFR § 64.6305; (c) implemented internal procedures ensuring FCC correspondence is routed to multiple responsible parties; and (d) established quarterly reviews of regulatory contact information to prevent future lapses. The company remains fully compliant with all STIR/SHAKEN requirements and robocall mitigation protocols and is now seeking reinstatement to the Robocall Mitigation Database.