Robocall Mitigation Program Policy

STATUS	Submission
EFFECTIVE DATE	11/19/2026
REVIEW DATE	11/19/2026
ISSUING AUTHORITY	Center24 LLC, Compliance Department
DOCUMENT OWNER	Ashfaq Ahmad, Compliance Officer
APPLIES TO	All voice service operations of Center24 LLC (FRN: 0039199732)
PURPOSE	Robocall Mitigation Plan for filing in the FCC Robocall Mitigation Database (47 CFR § 64.6305)

Contents

1.0 Policy Statement 2
2.0 Scope and Company Profile 3
3.0 STIR/SHAKEN Implementation Status 3
3.1 Current Status 3
3.2 Implementation Plan 3
3.3 Attestation Practices 4
4.0 Robocall Mitigation Program: Reasonable Steps 4
4.1 Know Your Customer (KYC) 4
4.2 Upstream Provider Vetting 5
4.3 Traffic Monitoring and Analytics 5
4.4 Response to Suspected Illegal Traffic 5
5.0 Traceback Cooperation 5
6.0 Roles and Responsibilities 6
7.0 Training, Recordkeeping and Review 6
8.0 Robocall Mitigation Database Certification and Filing 6
9.0 Enforcement 7

1.0 Policy Statement

Center24 LLC (the "Company") is a voice service provider offering interconnected Voice over Internet Protocol (VoIP) service in the United States. The Company is committed to preventing the origination of illegal robocalls and spoofed calls on its network. This Robocall Mitigation Program Policy (the "Policy") sets out the reasonable steps the Company takes to avoid originating illegal robocall traffic, as required by 47 CFR § 64.6305, and supports the Company's certification in the FCC Robocall Mitigation Database ("RMD").

2.0 Scope and Company Profile

This Policy applies to all voice traffic originated by or on behalf of the Company and its customers, and to all employees, contractors and vendors involved in provisioning, routing or supporting that traffic.

Company Information

Item	*Detail*
Legal name	Center24 LLC
Business address	1209 MOUNTAIN ROAD PL NE STE R ALBUQUERQUE NM 87110
FCC Registration Number (FRN)	0039199732
499 Filer ID	839477
Provider type	Voice service provider (interconnected VoIP); originates calls for end-user customers
Robocall mitigation contact	Abdullah, abdullah@center24.co
Formation date	October 2026

3.0 STIR/SHAKEN Implementation Status

The Company is in the process of implementing the STIR/SHAKEN caller ID authentication framework and will certify accurately the current status of that implementation in the RMD. Pending full implementation, all calls the Company originates remain subject to this Policy.

3.1 Current Status

As of November 20, 2026, the Company has fully implemented the STIR/SHAKEN framework. The Company will select the certification option in the RMD that matches its actual status and will update its filing within ten (10) business days of any change to the information submitted, as required by the FCC's rules.

3.2 Implementation Plan

- Obtain an Operating Company Number (OCN) and a direct-access request to the STI Policy Administrator (iconectiv) for a Service Provider Code token. Status: in-process.

- Obtain a digital certificate from an STI Certification Authority approved by the STI Governance Authority. Status: in-process.
- Deploy an STI Authentication Service and STI Verification Service.
- Sign originated SIP calls with the appropriate attestation level (A, B or C) and verify calls received where applicable.
- Target completion date for full implementation: Nov 30, 2026.

3.3 Attestation Practices

The Company assigns attestation levels only as follows: **A (Full)** where the Company has authenticated the customer relationship and verified the customer's authority to use the calling number; **B (Partial)** where the customer is authenticated but number authority is not verified; and **C (Gateway)** where the call origin cannot be authenticated. Attestation decisions are logged and reviewable.

4.0 Robocall Mitigation Program: Reasonable Steps

The Company takes the following specific, reasonable steps to avoid originating illegal robocall traffic.

4.1 Know Your Customer (KYC)

Consistent with 47 CFR § 64.1200(n)(4), the Company knows its customers and the nature of their traffic before and after service activation:

- Collect and verify legal business name, physical address, tax or registration number, website, principal contacts and beneficial ownership information for every customer.
- Screen customers and principals against the FCC RMD removal list, FCC and FTC enforcement actions, the OFAC sanctions list and internal denial lists.
- Document the customer's intended use, expected call volumes, call purposes and calling-number sources, and require a signed acceptable use agreement prohibiting illegal robocalls, spoofing with intent to defraud, and calls to numbers on the Do Not Call Registry without consent.
- Verify that customers have the right to use the numbers they present as caller ID (e.g., numbers assigned by the Company, ported-in numbers, or documented third-party authority).
- Apply enhanced due diligence and initial call-volume limits to high-risk customers, such as outbound call centers, auto-dialer and bulk-dialing users, and customers with high short-duration call rates.

- Re-validate customer information periodically and upon significant changes in traffic patterns.

4.2 Upstream Provider Vetting

- Exchange traffic only with providers that are listed in the Robocall Mitigation Database, and verify listings before establishing, and periodically after establishing, interconnection.
- Require upstream and downstream providers by contract to maintain a robocall mitigation program, to cooperate with traceback, and to accept traffic only from RMD-listed providers.
- Obtain basic identifying information, contact details and FRN for each interconnected provider.
- Suspend or terminate relationships with providers that are removed from the RMD or that repeatedly carry illegal traffic.

4.3 Traffic Monitoring and Analytics

- Monitor originating traffic for indicators of illegal robocalls, including high call volume, low answer-seize ratio, short average call duration, sequential or rotating dialing patterns, high rates of calls to unassigned numbers, and caller ID numbers that are invalid, unallocated or unassigned.
- Third-party analytics vendor(s): 46 Labs' PeereEdge system, Class 4 switch & analytics tool
- Block or rate-limit calls that violate the Company's policy, including calls originating from invalid, unallocated or unassigned numbers and numbers on the Company's do-not-originate list.
- Retain call detail records for at least two 3 years to support investigations.

4.4 Response to Suspected Illegal Traffic

1. Investigate flagged traffic promptly, typically within 1 business day.
2. Contact the customer and request an explanation and supporting documentation, such as consent records.
3. Suspend or block traffic where there is a reasonable basis to believe it is illegal.
4. Terminate service to customers that originate illegal robocalls, and document the reason.
5. Escalate and report as appropriate to the FCC, law enforcement or the industry traceback consortium.

5.0 Traceback Cooperation

The Company commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement and the industry traceback consortium,

and to cooperate with those entities in investigating and stopping any illegal robocallers that use its service to originate calls.

- The Company is registered with the industry traceback consortium's portal: Registered.
- Traceback contacts: Abdullah, abdullah@center24.co; Backup: Ashfaq Ahmad, ashfaq@center24.co, 575-242-8855. Contacts are monitored daily, including a backup for absences.
- Each request is logged, with the date and time of receipt and response, and tracked to closure.

6.0 Roles and Responsibilities

Role	*Responsibilities*
Robocall Mitigation Officer	Owns this Policy; oversees the RMD certification and updates; serves as the designated contact; approves suspensions and terminations.
Network / Engineering	Implements STIR/SHAKEN, call signing and verification, and traffic controls; maintains call detail records.
Sales and Onboarding	Performs KYC collection, verifies customer information, and does not activate service until approved.
Traceback Response Team	Responds to traceback requests within 24 hours and logs outcomes.
Executive Management	Provides resources; approves this Policy; signs the RMD certification.

7.0 Training, Recordkeeping and Review

- **Training:** Relevant personnel receive training on this Policy at hire and at least annually.
- **Records:** KYC files, traffic-monitoring reports, blocking and termination decisions, traceback responses and attestation logs are retained for at least two three years.
- **Review:** The Policy is reviewed at least annually, and when rules change or STIR/SHAKEN status changes, and updated as needed.

8.0 Robocall Mitigation Database Certification and Filing

The Company will file its certification and this Policy (as its robocall mitigation plan) in the RMD through the FCC portal using its FRN. The certification will include:

- A statement that all calls the Company originates are subject to a robocall mitigation program, and a selection of its actual STIR/SHAKEN status (full, partial or none).
- If STIR/SHAKEN is not yet fully implemented, the extension type and basis (if any), or an explanation of why it cannot be implemented.

- A description of the specific reasonable steps in Section 4.0, including KYC procedures, upstream provider procedures, and the name(s) of any analytics vendor(s).
- The 24-hour traceback commitment in Section 5.0.
- A statement of whether, in the prior two years, the Company or any commonly owned or controlled entity has been the subject of a formal Commission, law enforcement or regulatory action or investigation concerning unlawful robocalls, and, if so, a description of it: [Yes / No — details].
- Contact information, FRN, business name(s) and addresses, and the name of the officer who signs the certification.

The Company will update its RMD filing within ten 10 business days of any change to the submitted information, and will re-certify annually as the FCC requires.

9.0 Enforcement

Violations of this Policy by employees or contractors may result in disciplinary action. Customers that originate illegal robocalls will have service suspended or terminated under the Company's acceptable use terms. The Company acknowledges that false or inaccurate RMD filings may result in removal from the database and FCC enforcement action.