

Ringflow LLC

Robocall Mitigation Program & STIR/SHAKEN Implementation

FRN 0038767364 • Non-Gateway Intermediate Provider • Dover, Delaware, USA

Ringflow LLC (“Ringflow” or “the Company”) is a United States-based telecommunications provider operating as a non-gateway intermediate provider. In accordance with Federal Communications Commission (“FCC”) requirements — including the TRACED Act, 47 C.F.R. §§ 64.6300–64.6308, and the Commission’s Sixth Report and Order (WC Docket No. 17-97) — Ringflow has implemented this Robocall Mitigation Program (“RMP”) to prevent the origination, carrying, or processing of illegal robocall traffic and to maintain the integrity of the caller ID authentication information it transmits.

1. Regulatory Status & Provider Classification

Ringflow holds an FCC Registration Number (FRN) and complies with applicable FCC regulations governing robocall mitigation and caller ID authentication. As a non-gateway intermediate provider, Ringflow carries and processes traffic exchanged between other providers; it does not originate calls from its own end-user customers, nor does it terminate calls to the called party. Its core obligations are to pass caller ID authentication information unaltered, cooperate promptly with traceback, and take reasonable steps to avoid transmitting illegal robocall traffic.

Legal entity	Ringflow LLC
FCC Registration Number (FRN)	0038767364
Provider classification	Non-gateway intermediate provider
STIR/SHAKEN status	Fully implemented (IP network)
Business address	8 The Green, Suite B, Dover, DE 19901, Kent County, Delaware, United States

2. Executive Summary & Governance

Ringflow is committed to preventing illegal traffic from traversing its network and to monitoring the traffic it exchanges with upstream and downstream providers. The Company enforces the following governance principles:

- **Zero-Tolerance Policy:** Ringflow maintains a strict policy against illegal robocalling, caller ID spoofing, fraudulent traffic origination, and abusive telecommunications practices.
- **Compliance Oversight:** A designated management-level Compliance Officer oversees RMD filings, STIR/SHAKEN compliance, customer and upstream-provider onboarding controls, and traceback coordination.
- **Documented Policies:** Policies are documented, reviewed at least annually, and updated whenever regulatory requirements or the Company’s operations change.
- **RMD Maintenance:** Ringflow recertifies its Robocall Mitigation Database filing on or before March 1 each year and updates the filing within ten (10) business days of any change to the information on file.

3. Call Authentication (STIR/SHAKEN)

Ringflow has fully implemented STIR/SHAKEN caller ID authentication across the IP portions of its network, in accordance with 47 C.F.R. §§ 64.6301 and 64.6302. Its implementation includes:

- **Preservation of Authentication:** As an intermediate provider, Ringflow passes STIR/SHAKEN authentication information (the SIP Identity header / PASSporT) unaltered to the next provider and does not strip, remove, alter, or degrade that information on calls carried over IP.
- **Attestation Integrity:** Ringflow preserves the attestation level (A, B, or C) assigned by the originating provider and does not modify the calling party number on the calls it transmits, except as expressly permitted by FCC rules.
- **Certificate Management:** Ringflow maintains the digital certificates, keys, and Service Provider Code (SPC) token credentials required to participate in the STIR/SHAKEN ecosystem through an approved STI-CA / STI-PA, with ongoing renewal, secure key storage, and credential controls.
- **Validation & Handling:** Inbound calls are validated; authentication failures and unauthenticated calls received over IP are analyzed and, where appropriate, flagged, mitigated, or blocked in accordance with this Program.

4. Robocall Mitigation & Traceback

In compliance with FCC requirements, Ringflow adheres to the following affirmative obligations to avoid transmitting illegal robocall traffic:

- **Traceback Cooperation:** Ringflow commits to responding fully and within twenty-four (24) hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (USTelecom's Industry Traceback Group).
- **Investigation Process:** Ringflow cooperates in investigating and stopping illegal robocallers whose traffic traverses its network, identifying the immediate upstream source of the traffic at issue.
- **Effective Mitigation:** Upon confirming illegal traffic, or upon notification from the Commission or the traceback consortium, Ringflow promptly mitigates the traffic — including blocking, ceasing to accept it, or requiring the responsible provider or customer to stop transmitting it.

Traceback / RMD Point of Contact:

- **Name:** Sagufta Bibi
- **Title:** President
- **Contact Details:** noc@ringflow.com

5. Advanced Network Monitoring & Traffic Controls

Ringflow uses a multi-layered approach to monitor the traffic it transmits for behavior consistent with illegal robocalling:

- **Pattern Detection:** Real-time analysis of call detail records identifies anomalies such as sudden traffic spikes, high short-duration call ratios, low answer-seizure ratios, sequential dialing, rapid caller ID rotation, and abnormal invalid-number or complaint ratios.

- **Blocking Mechanisms:** Ringflow can immediately block or refuse to accept traffic identified as illegal robocalls.
- **DNO & Cease-and-Desist Readiness:** Ringflow maintains a do-not-originate (DNO) and blocking capability for numbers that should never place outbound calls, and stands ready to conduct network-level blocking in response to FCC “cease-and-desist” notifications.
- **Anti-Fraud Controls:** Automated controls detect and block sources, lines, or accounts suspected of being compromised or of transmitting illegal traffic, and record such events to prevent recurrence and to support notification of affected parties.

6. Know Your Customer (KYC) & Upstream Provider Due Diligence

Because Ringflow exchanges traffic with other providers, disciplined due diligence on its counterparties is its first line of defense. Prior to accepting traffic, Ringflow conducts due diligence that includes:

Mandatory Requirements:

- Executed service/interconnection agreement with anti-robocall and anti-spoofing clauses;
- Verification of legal identity — business location, contact person(s), state or county of incorporation, and federal tax ID or business registration;
- Confirmation of FCC registration (FRN) and Robocall Mitigation Database status of upstream providers, where applicable;
- Traffic profile declaration (use case, call types, and estimated volumes).

Risk Classification:

- Counterparties are categorized as Low, Medium, or High risk based on their traffic profile. High-risk counterparties require management approval, enhanced due diligence, and heightened monitoring.
- **Ongoing Monitoring:** Renewing customers and upstream providers face periodic re-verification to ensure continued compliance.

7. Network Authorization & Access Controls

To prevent unauthorized origination of traffic onto its network:

- All SIP interconnections require prior authorization;
- IP authentication and credential-based access controls are enforced;
- Routing permissions are defined per customer and per upstream provider;
- Unauthorized traffic is automatically blocked;
- Access credentials are reviewed periodically.

8. Caller ID Validation & Spoofing Prevention

Ringflow enforces the following controls to preserve caller ID integrity on the traffic it transmits:

- Blocking of invalid, unallocated, or malformed caller IDs;
- Rejection of known fraudulent number ranges;

- Geographic mismatch analysis, where applicable;
- Real-time flagging of suspicious CLI patterns;
- Enforcement of attestation-level integrity under STIR/SHAKEN.

9. Blocking & Enforcement Policy

Ringflow enforces a zero-tolerance enforcement policy:

- Suspicious accounts and provider relationships are immediately reviewed;
- Traffic may be throttled or suspended during an investigation;
- Confirmed violators are permanently terminated;
- Customers and resellers are contractually obligated to monitor and block downstream offenders.

10. Traceback & Regulatory Cooperation

Ringflow fully cooperates with the U.S. Traceback Consortium (USTelecom's Industry Traceback Group), the FCC, and law enforcement authorities. Traceback requests are acknowledged and responded to within twenty-four (24) hours. In responding, Ringflow:

- Identifies upstream and downstream traffic sources;
- Suspends suspicious customers or providers during investigation;
- Permanently terminates confirmed violators;
- Maintains detailed call records to support investigations.

11. Training & Internal Controls

Relevant staff receive regular training covering STIR/SHAKEN operational procedures, FCC robocall regulations, traffic-anomaly detection, and escalation protocols.

12. Audit & Continuous Improvement

Ringflow conducts periodic audits of STIR/SHAKEN attestation handling, traffic-monitoring effectiveness, customer and upstream-provider compliance controls, and mitigation-rule performance. Findings are used to continuously improve the Program. All information Ringflow submits to the RMD is true, accurate, and complete to the best of the Company's knowledge; the Company understands that inaccurate filings or failure to update may result in monetary penalties and removal from the RMD.