

Robocall Mitigation Plan

Company Name: Exor Systems

1. Company Overview

Exor Systems is a telecommunications and technology services provider offering VoIP and SIP-based communication solutions for legitimate business use. Exor Systems is committed to preventing illegal robocalls, spoofing, and fraudulent traffic across its network and maintains strict compliance with all applicable laws and regulations.

2. Policy Against Illegal Robocalls

Exor Systems strictly prohibits the origination, termination, or facilitation of illegal robocalls, including but not limited to:

- Unsolicited robocalls
- Spoofed caller ID traffic
- Fraudulent or scam-related calling
- Calls violating TCPA, FCC regulations, or local telecom laws

All customers, vendors, and partners must comply with these policies as a condition of service.

3. Customer Due Diligence and Onboarding

Exor Systems performs reasonable and ongoing due diligence on all customers, including:

- Collection of legal business name, address, and contact details
- Verification of business registration documents
- Verification of intended use of VoIP services
- Acceptance of Exor Systems' Acceptable Use Policy (AUP)

High-risk customers or traffic profiles are subject to enhanced review and monitoring.

4. Traffic Monitoring and Network Controls

Exor Systems actively monitors network traffic to detect and mitigate illegal robocalling activity through:

- Call pattern and volume analysis
- Monitoring of short-duration, high-volume call bursts
- Detection of abnormal or suspicious calling behavior
- Blocking or throttling of suspicious traffic

Automated and manual reviews are conducted to ensure compliance.

5. STIR/SHAKEN and Caller ID Integrity

Where technically feasible, Exor Systems supports STIR/SHAKEN frameworks to authenticate caller ID information.

- Unauthorized or misleading caller ID usage is strictly prohibited
- Customers may only use caller IDs they are legally authorized to use

Any violations result in immediate corrective action.

6. Complaint Handling and Response

Exor Systems maintains a process for receiving and responding to complaints from carriers, regulators, or consumers:

- Complaints are reviewed promptly
- Traffic is investigated and traced where possible

- Corrective actions may include warnings, suspension, or termination of service

Exor Systems cooperates fully with regulators and industry traceback efforts.

7. Enforcement and Corrective Actions

If illegal robocall activity is detected, Exor Systems may take one or more of the following actions:

- Immediate suspension of traffic
- Termination of customer services
- Blocking of offending numbers or routes
- Reporting to upstream carriers or relevant authorities

These actions are taken to protect the integrity of the network and the telecommunications ecosystem.

8. Ongoing Compliance and Review

Exor Systems regularly reviews and updates its robocall mitigation practices to remain compliant with evolving regulations and industry standards. Staff and partners are informed of policy updates as required.

9. Commitment Statement

Exor Systems is committed to maintaining a lawful, secure, and responsible communications network and takes all reasonable steps to prevent illegal robocalls, spoofing, and fraudulent activity.