

Robocall Mitigation Plan and Know Your Customer Policy

Company Overview and Regulatory Compliance

Exiant communications llc is a U.S.-based telecommunications service provider committed to combating the nationwide robocalling and telecommunications fraud epidemic. We maintain full regulatory compliance with all applicable federal agencies and industry standards:

- **FCC Registration:** FRN #0026646844
- **USAC Registration:** 499a ID #832155
- **Intermediate Provider Registry (IPR):** Registered and compliant
- **Robocall Mitigation Database (RMD):** Filed and listed
- **Industry Traceback Group (ITG):** Registration submitted
- **OCN Number:** 114J, 650L (affiliate)

As an active participant in the U.S. Telecom Traceback Group community, Exiant takes an aggressive stance against fraudulent robocalling activities that harm consumers nationwide.

FCC-Required Robocall Mitigation Measures

Exiant has implemented comprehensive robocall mitigation protocols in full compliance with FCC requirements:

Customer Identity Verification and Due Diligence

We maintain rigorous Know Your Customer (KYC) protocols through comprehensive identity verification processes, including business license validation, beneficial ownership documentation, and ongoing customer relationship monitoring to prevent bad actors from accessing our network.

Contractual Anti-Robocall Provisions

All customer agreements include mandatory contractual provisions specifically prohibiting illegal robocalling activities, with clear enforcement mechanisms and immediate termination rights for violations of federal telecommunications laws and regulations.

Telephone Number Authorization Validation

We implement systematic verification processes to confirm each customer's legitimate right to use assigned telephone numbers through carrier verification, number portability validation, and ongoing authorization audits to prevent number spoofing and unauthorized usage.

Inter-Carrier Traffic Prerequisites

Before accepting traffic from other telecommunications providers, we require comprehensive vetting including RMD registration verification, regulatory compliance confirmation, and traffic quality assessments to ensure only legitimate carriers access our network infrastructure.

Do Not Originate List Implementation

Our network automatically blocks all calls originating from numbers listed on industry Do Not Originate databases, with real-time list updates and automated blocking mechanisms preventing fraudulent calls from known bad numbers.

Network Traffic Analysis and Monitoring

We continuously analyze and monitor all call traffic routing through our network using advanced analytics to identify suspicious patterns, unusual volume spikes, and potential fraud indicators through real-time monitoring systems.

Third-Party Analytics Integration

Our robocall mitigation efforts are enhanced by third-party analytics solutions provided by our switch manufacturer, offering additional layers of call pattern analysis, fraud detection algorithms, and industry intelligence integration. Our third-party analytics vendors include DenovoLabs, and Switch solutions, which combine DNO, FTC list, YouMail lookups to block calls in realtime and provide ongoing statistics.

Suspicious Call Pattern Investigation

We maintain dedicated resources for investigating suspicious calling patterns, including unusual call volumes, rapid sequential dialing, and geographic anomalies, with immediate response protocols for potential fraud identification.

Foreign Provider Compliance Oversight

We implement strict oversight protocols to ensure foreign telecommunications providers cannot utilize our network to carry or process high-volume illegal robocalls, including enhanced due diligence and traffic monitoring for international partners.

Voice Traffic Authentication Systems

All voice traffic is authenticated through our STIR/SHAKEN implementation and additional proprietary authentication protocols to verify call origin and prevent spoofing and impersonation attacks on our network infrastructure.

Violation Response Protocol

Exiant employs a progressive enforcement system for FCC Trace Act violations, including but not limited to robocalls and government impersonation schemes:

First Violation

- **Action:** Initial violation warning issued, if it is severe or clear illegal robocalling, we terminate their ability to send calls immediately
- **Documentation:** Incident recorded in customer file
- **Requirement:** Immediate cessation of violating traffic

Second Violation

- **Action:** Account suspension pending remediation
- **Duration:** Until satisfactory mitigation plan implemented
- **Review:** Comprehensive account audit required

Third Violation

- **Action:** Account termination proceedings initiated
- **Appeal Process:** Available with comprehensive mitigation plan
- **Reinstatement:** At sole discretion of Exiant management

Unlawful Activity

- **Immediate Termination:** Any account found to be engaging in unlawful use of our network will be immediately and permanently terminated without prior notice
- **No Appeal Process:** Unlawful activity terminations are final and non-reversible

Traceback Response and Compliance Management

Expedited Traceback Response and Information Sharing

Exiant will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating fully with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Exiant maintains sophisticated systems and procedures for responding to regulatory and industry traceback requests:

Response Infrastructure and Capabilities:

Regulatory Agency Coordination:

- **FCC Traceback Response:** Established procedures for responding to FCC Enforcement Bureau traceback requests including designated points of contact, information formatting requirements, and escalation procedures for complex investigations.
- **Industry Traceback Group Participation:** Active participation in US Telecom Industry Traceback Group activities including membership in working groups, participation in industry training programs, and contribution to best practice development.
- **Law Enforcement Cooperation:** Formal procedures for coordinating with federal and state law enforcement agencies including FBI, FTC, and state attorneys general offices with established information sharing protocols and legal process compliance procedures.

Regulatory Response Protocols

We maintain expedited response procedures for all Commission, law enforcement, and Industry Traceback Group (ITG) traceback requests, with dedicated personnel ensuring rapid compliance and comprehensive information sharing to support fraud investigations. We respond to all requests within 24 hours.

Designated Robocall Mitigation Officer

Exiant has designated a specific employee responsible for all robocall mitigation issues, serving as the primary point of contact for regulatory agencies, industry partners, and internal compliance coordination to ensure consistent and effective fraud prevention efforts.

Database Maintenance and Updates

We maintain current submissions to both the Robocall Mitigation Database (RMD) and Robocall Mitigation Plan (RMP) systems, with regular updates reflecting changes in our mitigation strategies, contact information, and compliance procedures.

Customer Traceback Compliance Requirements

All customers must maintain full compliance with Industry Traceback Group requirements:

Customer Response Obligations

- **Immediate Response:** All traceback requests require prompt acknowledgment and response
- **Customer Information:** Complete disclosure of originating customer data for flagged calls
- **Timeline:** Response required within industry-standard timeframes
- **Documentation:** Comprehensive records of remedial actions taken

Non-Compliance Consequences

- Failure to respond results in compliance strikes against both customer and Exiant
- Incomplete traceback forms result in customer being treated as the originating fraud source
- Account termination will result from continued non-compliance, or canceled immediately based on severity

STIR/SHAKEN Authentication Compliance

Exiant maintains full STIR/SHAKEN compliance in accordance with FCC requirements, implementing proper call authentication through our attestation framework:

Attestation Levels

- **Full Attestation (A):** Complete calling party authentication with number authorization verification
- **Partial Attestation (B):** Authenticated origination without source authorization verification
- **Gateway Attestation (C):** Source authentication for calls received through international gateways

Customer Acknowledgment and Agreement

By executing this agreement, the undersigned customer representative acknowledges and agrees to:

1. **Policy Recognition:** Full comprehension and acceptance of Exiant's Know Your Customer and Robocall Mitigation policies
2. **Regulatory Compliance:** Adherence to all FCC regulations and governing body requirements, including Industry Traceback Group and U.S. Telecom standards
3. **Traceback Participation:** Prompt and comprehensive response to all traceback requests from authorized regulatory bodies
4. **RMD Compliance:** Confirmation of registration as a Terminating Service Provider in the Robocall Mitigation Database with proper customer vetting procedures

Upstream Provider Validation and Compliance Verification

Mandatory Upstream Provider Database Verification

Exiant maintains comprehensive validation procedures for all upstream telecommunications providers to ensure traffic originates only from legitimate, compliant carriers:

Robocall Mitigation Database (RMD) Verification:

- **Current RMD Registration Confirmation:** All upstream providers must maintain current and active registration in the FCC's Robocall Mitigation Database with verified Provider ID numbers, current contact information, and filed mitigation plans reviewed and validated by Exiant personnel prior to traffic acceptance.
- **Mitigation Plan Review:** Comprehensive review of upstream provider RMD-filed mitigation plans including assessment of mitigation measure adequacy, compliance officer designation verification, and evaluation of traceback response capabilities to ensure alignment with industry standards.
- **Quarterly RMD Status Verification:** Systematic quarterly verification of upstream provider RMD registration status including confirmation of continued active status, review of any updated mitigation plans, and verification that no compliance violations or enforcement actions have affected their RMD standing.
- **RMD Contact Validation:** Regular validation of upstream provider designated contacts listed in the RMD including verification of contact information accuracy, confirmation of contact authority to respond to traceback requests, and testing of communication channels for traceback coordination.