

# FENTRIA SYSTEMS LLC

Wholesale Voice | SIP Trunking | Carrier Interconnection

## Robocall Mitigation Plan

*Prepared pursuant to the TRACED Act and 47 C.F.R. § 64.6305, in support of the Company's certification in the FCC Robocall Mitigation Database*

|                           |                                                      |                         |                                                         |
|---------------------------|------------------------------------------------------|-------------------------|---------------------------------------------------------|
| <b>Company Legal Name</b> | Fentria Systems LLC                                  | <b>OCN</b>              | 468M                                                    |
| <b>Headquarters</b>       | 3100 Smoketree Ct, Suite 640, Raleigh, NC 27604, USA | <b>FCC 499 Filer ID</b> | 839047                                                  |
| <b>FRN</b>                | 0038328142                                           | <b>RMD Filing ID</b>    | RMD0039825                                              |
| <b>Version / Status</b>   | 1.0 - Adopted                                        | <b>Effective Date</b>   | 18 June 2026                                            |
| <b>Last Reviewed</b>      | August 28, 2026                                      | <b>Website</b>          | <a href="https://fentria.com/">https://fentria.com/</a> |

### 1. Purpose and Scope

This Robocall Mitigation Plan (the “Plan”) describes the specific, reasonable steps that Fentria Systems LLC (“Fentria” or the “Company”) takes to prevent illegal robocall traffic from being originated on, transiting through, or terminating on its network. The Plan is adopted pursuant to the TRACED Act and the rules of the Federal Communications Commission (“FCC”), including 47 C.F.R. § 64.6305, and supports the Company’s certification filed in the FCC Robocall Mitigation Database (“RMD”).

The Plan applies to all voice traffic handled by the Company in any capacity – as an originating provider, an intermediate provider, or a terminating provider – and to all customers and interconnecting providers exchanging traffic with the Company’s network.

### 2. Company Overview

Fentria Systems LLC is a VoIP / Interconnected IP-Enabled Services (IPES) carrier providing wholesale voice termination, SIP Trunking, Local DIDs, Toll-Free, and ITFS services to telecommunications carriers, VoIP service providers, contact centers, and enterprise customers. The Company owns and operates its own switching and SIP infrastructure, giving it direct, real-time control over routing, traffic management, monitoring, and blocking.

The Company’s traffic is predominantly conversational business voice, with typical call durations of 60–100+ seconds. The Company does not operate automated dialing platforms, does not engage in telemarketing, and does not knowingly serve customers engaged in illegal calling campaigns.

### 3. STIR/SHAKEN Implementation – Status: Fully Implemented

The Company has fully implemented the STIR/SHAKEN caller ID authentication framework across the IP portions of its network:

- The Company holds its own Operating Company Number (OCN 468M) and is registered with the STI Policy Administrator (iconectiv), from which it has received its Service Provider Code token.
- The Company maintains its own STI certificate obtained from an approved STI Certification Authority and signs its originated traffic using its own certificate; third-party signing is not relied upon.

- All calls originated on the network are signed with the appropriate attestation level in accordance with ATIS standards: “A” attestation for fully vetted customers with a verified right to use the calling number (including Company-assigned numbers); “B” attestation for authenticated customers where the calling number cannot be verified; and “C” attestation for traffic where the origin cannot be verified.
- For traffic handled in an intermediate capacity, the Company passes SIP Identity headers unaltered and cooperates in the SHAKEN ecosystem, including certificate validation and verification processes.

#### **4. Know Your Customer (KYC) and Customer Vetting**

No customer is permitted to send traffic to the Company’s network before completing a documented onboarding and vetting process, which includes:

- Legal entity verification – confirmation of the customer’s legal name, registered address, jurisdiction of formation, ownership, and principal/controlling persons.
- Regulatory verification – confirmation of applicable U.S. registrations (FRN, FCC Form 499 Filer ID, OCN where applicable) and, for voice service providers, active listing in the FCC Robocall Mitigation Database that has not been removed or delisted; equivalent licensing checks for non-U.S. customers.
- Business validation – review of the customer’s functioning website and business model, the declared use case and nature of traffic, and expected volumes, CPS, and destinations.
- Adverse-history screening – checks for FCC enforcement actions, Industry Traceback Group “non-cooperative provider” designations, and other public indicators of prior illegal-traffic involvement.
- Contractual certifications – execution of a service agreement incorporating the Company’s Acceptable Use Policy, under which the customer certifies that it will not originate or transmit illegal robocalls; that it complies with the TCPA, the Telemarketing Sales Rule, and Do-Not-Call requirements; that prior express written consent is obtained for any prerecorded/artificial-voice or autodialed calling where required; and that it will cooperate with traceback requests.

Any material change in a customer’s traffic profile or use case requires advance notice to the Company and recertification. KYC records are retained for a minimum of two (2) years following termination of the customer relationship.

#### **5. Acceptable Use Policy and Contractual Controls**

All customer agreements incorporate the Company’s Acceptable Use Policy, which expressly prohibits illegal robocalls; caller ID spoofing with intent to defraud, cause harm, or wrongfully obtain anything of value; autodialed or prerecorded calling without required consent; violations of Do-Not-Call rules; high-volume, short-duration abuse; traffic pumping; and any unlawful use of the network. The Company’s agreements reserve the right to throttle, suspend, block, or terminate traffic or service immediately upon identification of violations, and require customers to impose equivalent obligations on their own upstream customers.

#### **6. Traffic Monitoring and Call Analytics**

The Company continuously monitors traffic at the switch level and applies call analytics designed to identify and stop suspected illegal robocall traffic, including:

- Per-customer and per-trunk monitoring of ASR, ACD/ALOC, CPS, and traffic volumes against expected baselines and defined internal thresholds.

- Detection of high-volume, short-duration calling patterns, abnormal CPS spikes, unusual concentration toward specific destinations, and excessive calling from individual originating numbers.
- Screening of originating numbers for invalid, unallocated, or unassigned NANP numbers.
- Automated alerting to the operations team, with a defined escalation path: investigation, customer notification, throttling or suspension of the affected traffic, and termination for unresolved or repeat violations.

The Company's ownership of its own switching platform enables blocking to be applied in real time at the trunk, customer, or originating-number level.

## **7. Do-Not-Originate (DNO) List**

The Company maintains a Do-Not-Originate list based on industry-recognized sources, including inbound-only government and enterprise numbers, and invalid, unallocated, and unassigned numbers. The list is updated on a regular cadence and enforced at the switch level, so that any outbound call attempt using a DNO-listed originating number is automatically blocked, consistent with FCC rules and industry best practice.

## **8. Traceback Cooperation**

The Company fully cooperates with the Industry Traceback Group (ITG), the FCC, the FTC, state attorneys general, and other law enforcement and regulatory bodies in investigating and stopping illegal robocall campaigns. Specifically, the Company commits to:

- Respond fully to all traceback requests within twenty-four (24) hours of receipt.
- Identify the customer or upstream provider from which the traffic in question was received and provide relevant call records to the extent legally permissible.
- Take timely remedial action against identified sources of illegal traffic, up to and including blocking, suspension, and termination.
- Retain records of all traceback requests, findings, and remediation actions for a minimum of two (2) years.

Designated traceback point of contact: Olivia Carter, [olivia.carter@fentria.com](mailto:olivia.carter@fentria.com), 407-610-3834.

## **9. Blocking Upon Notification and Effective Mitigation**

Upon receiving a notification of suspected illegal traffic from the FCC (including its Enforcement Bureau), the ITG, or another authorized entity, the Company will promptly investigate, block the identified traffic within the timeframe specified in the notice, and report the actions taken. The Company will not knowingly serve, and will cease serving, any originator or upstream provider determined to be a source of illegal robocalls, and will comply with all applicable FCC blocking mandates, including declining to accept traffic from voice service providers not listed in the Robocall Mitigation Database where required by the rules.

## **10. Know Your Upstream Provider (Intermediate Traffic)**

Where the Company acts as an intermediate provider, it applies vetting to upstream carriers equivalent to its customer KYC process, including verification of RMD listing, STIR/SHAKEN participation, and contractual commitments to traceback cooperation. The Company maintains current contact information for the provider immediately upstream for all interconnections so that traceback requests can be actioned without delay.

## 11. Governance, Training, and Recordkeeping

- A designated compliance function is responsible for administering this Plan, monitoring regulatory developments, and coordinating traceback and law-enforcement responses.
- Personnel involved in onboarding, NOC operations, and compliance receive training on the obligations described in this Plan.
- KYC files, monitoring and blocking logs, and traceback records are retained for a minimum of two (2) years.
- This Plan is reviewed at least annually and upon any material regulatory or operational change. The Company will update its RMD filing within ten (10) business days of any material change to the information contained therein.

## 12. Certification

The undersigned, an officer of Fentria Systems LLC authorized to legally bind the Company, certifies that the statements in this Robocall Mitigation Plan are true and correct to the best of the officer's knowledge and belief, and that the Company is committed to the ongoing implementation of the measures described herein.

Signature: Olivia Carter

Printed Name: Olivia Carter

Title: VP - Voice

Company: Fentria Systems LLC

Date: 20 July 2026