



Robocall Mitigation Plan

FortiComm LLC

Business Information

FortiComm LLC
8565 S Eastern Ave, Suite 150
Las Vegas, NV 89123

Contact Information

Liam Flatley
Director of Operations
630-621-6248
lflatley@forticomm.com

FortiComm maintains this individual as the single point of contact for all robocall mitigation, traceback, and regulatory inquiries.

Overview

FortiComm LLC (“FortiComm”) is a **non-facilities-based intermediate VoIP provider** that provides wholesale call routing services exclusively to other carriers. FortiComm does not originate retail end-user traffic.

Because FortiComm does not originate voice traffic, it is not subject to the authentication requirements applicable to originating voice service providers under **47 CFR § 64.6302**. FortiComm complies with the obligations applicable to intermediate providers under **47 CFR § 64.6305**, including preservation of STIR/SHAKEN authentication information and maintenance of a robocall mitigation program.

FortiComm has not implemented STIR/SHAKEN authentication and does not possess an SPC token or STI certificate. FortiComm does not sign calls.

This Robocall Mitigation Plan (“RMP”) describes the reasonable steps FortiComm takes to prevent illegal robocall traffic from traversing its network and to comply with applicable Commission rules.

STIR/SHAKEN Handling and Compliance

FortiComm complies with its obligations under **47 CFR § 64.6305(c)** as an intermediate provider.

Specifically:

- FortiComm does not sign calls and does not operate an authentication service.
- FortiComm preserves and transmits STIR/SHAKEN Identity header information without alteration.
- FortiComm does not remove, modify, or downgrade attestation levels.
- FortiComm does not re-sign calls.
- FortiComm blocks calls that do not contain a STIR/SHAKEN Identity header in accordance with its internal policies.
- FortiComm relies on upstream originating providers to authenticate traffic.

Know Your Customer (KYC) Procedures

FortiComm conducts due diligence prior to onboarding any customer (“subscriber”).

The following information is collected and verified:

- Legal business name
- Physical business address
- Telephone number
- Federal Registration Number (FRN), if applicable
- FCC Robocall Mitigation Database Filer ID, if applicable
- Contact person(s) and title(s)
- Nature of the subscriber’s business
- Description of intended traffic use case

FortiComm evaluates whether the subscriber’s stated use case aligns with expected traffic patterns. Subscribers are contractually prohibited from transmitting unlawful traffic and are required to comply with all applicable FCC robocall mitigation rules.

Know Your Upstream Provider Procedures

FortiComm conducts due diligence on upstream providers prior to entering into service arrangements.

FortiComm:

- Confirms upstream providers are listed in the FCC Robocall Mitigation Database where applicable
- Requires upstream providers to comply with applicable FCC robocall mitigation and STIR/SHAKEN obligations
- Cooperates with upstream providers in responding to traceback requests

- Coordinates investigations of suspicious traffic patterns

FortiComm maintains communication channels with upstream providers to facilitate rapid mitigation and response efforts.

Traffic Monitoring and Analytics

FortiComm monitors traffic patterns to identify potentially unlawful robocall activity. Monitoring includes review of:

- Anomalies in cost generated by calls from a single subscriber
- Multiple overlapping calls on a single account
- High call initiation velocity (rapid back-to-back dialing)
- Short-term volume spikes compared to historical trends
- Number of unique destination numbers within a defined time period
- Number of unique source numbers within a defined time period
- Abnormal call duration distributions

FortiComm reviews call detail records (CDRs) to benchmark traffic against expected subscriber behavior and use case.

Investigation of Suspicious Activity

When traffic monitoring identifies potential illegal robocalling behavior, FortiComm undertakes investigative procedures that may include:

- Reviewing recent and historical call detail records
- Comparing traffic patterns to stated subscriber use case
- Reviewing account activity and purchasing patterns
- Verifying call routing paths
- Coordinating with upstream providers
- Contacting the subscriber for explanation and verification

If suspicious traffic is confirmed, FortiComm may take corrective action, including:

- Immediate traffic blocking
- Suspension of service
- Termination of the subscriber agreement

Blocking and Do-Not-Originate Compliance

FortiComm:

- Implements Do Not Originate (DNO) requests received from the Industry Traceback Group (ITG)
- Blocks unauthenticated calls consistent with internal policy

- Blocks traffic identified as unlawful or suspicious following investigation
- Maintains mechanisms to prevent further transmission of confirmed illegal traffic

Traceback Cooperation

FortiComm cooperates fully with:

- The Federal Communications Commission
- Federal and state law enforcement
- The Industry Traceback Group (ITG)

FortiComm commits to responding fully and within 24 hours to all traceback requests.

FortiComm maintains records sufficient to identify call routing paths and will provide responsive documentation when requested.

Third-Party Vendors

FortiComm does not utilize third-party vendors to deploy STIR/SHAKEN authentication. Traffic monitoring and mitigation functions are conducted internally and in coordination with upstream providers.

Plan Updates

FortiComm recognizes that robocall mitigation practices must evolve to address emerging threats.

This RMP will be reviewed periodically and updated as necessary. In the event of any material change, FortiComm will update its filing in the FCC Robocall Mitigation Database within ten (10) days of such change.

Certification

I, Liam Flatley, Director of Operations of FortiComm LLC, certify under penalty of perjury that:

1. FortiComm is a non-facilities-based intermediate provider and does not originate voice traffic.
2. FortiComm has not implemented STIR/SHAKEN authentication and does not possess an SPC token or STI certificate.
3. FortiComm complies with the obligations applicable to intermediate providers under 47 CFR § 64.6305.
4. FortiComm maintains and adheres to the robocall mitigation practices described in this plan.
5. FortiComm has not been prohibited from filing in the FCC Robocall Mitigation Database.
6. FortiComm is not currently subject to a Commission enforcement action prohibiting it from filing.
7. The information contained herein is true and correct to the best of my knowledge.

Liam Flatley
Director of Operations
FortiComm LLC

Liam Flatley