FORTEL NETWORKS, INC.

ROBOCALL MITIGATION PLAN

Business Information
Fortel Networks, Inc.
P.O. Box 8
Elk Grove, CA 95759

Contact Information
Peter Priest
916 580-1900
p.priest@fortel.us

OVERVIEW

The FCC requires that, by February 26, 2024, all voice service providers ("VSPs") (re)certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan ("RMP") to ensure that they are not originating illegal robocalls.

CERTIFICATIONS

Fortel Networks, Inc. hereby certifies that:

1. It partially implements STIR/SHAKEN on the IP portions of its network by utilizing underlying carriers to sign its calls with proper attestation based on the provider's DIDs used as caller ID (ANI).
2. No prior certification has been removed by Commission action.
3. Fortel has not been prohibited from filing in the Robocall Mitigation Database.
4. Fortel commits to respond fully to all traceback requests within 24 hours from the Federal Communications Commission, law enforcement, and the industry traceback consortium.
5. Neither Fortel nor any affiliated entity has been subject to any Commission or law enforcement agency action or investigation in the prior two years due to suspected involvement with illegal robocalling or spoofing, or due to a deficiency in its RMD certification.

COMPANY STRUCTURE AND RELATIONSHIPS

1. Fortel Networks, Inc. is an independent company with no parent company, subsidiaries, or affiliates.
2. Fortel operates as a retail carrier and does not sell wholesale minutes to any customers.
3. Principal Information:

- Peter Priest, President and Director
- No other principals or directors

ROLE IN CALL CHAIN

Fortel Networks, Inc. serves as a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.

CALL ANALYTICS AND TRAFFIC MONITORING

1. Internal Analytics:
    - Monitor traffic patterns on a per-customer and per-ANI basis
    - Track call duration distributions
    - Analyze short-duration call patterns
    - Monitor for anomalous calling patterns
2. Third-Party Analytics:
    - Utilize carrier partner analytics systems for additional traffic monitoring
    - Leverage carrier blocking lists and reputation databases

KNOW YOUR CUSTOMER PROCEDURES

Customer Verification

1. Initial Screening:
    - Complete required questionnaire
    - Verify business information (name, address, nature of business)
    - Validate customer identity and business legitimacy
    - Screen for autodialing and telemarketing intentions

Upstream Provider Verification

1. Provider Assessment:
    - Collect business information including nature of business, physical location
    - Verify federal tax ID where available
    - Confirm RMD registration status
    - Document provider's role in call chain
    - Validate STIR/SHAKEN capabilities

MITIGATION MEASURES

Prevention

1. Telephone Number Authorization:
    - Verify authority to use numbers
    - Track number assignments
    - Validate Caller ID against customer inventory
    - Require authentication for call origination
2. Traffic Monitoring:
    - Monitor for suspicious patterns
    - Track short-duration calls
    - Analyze call duration distribution
    - Monitor for unusual volume patterns

Investigation and Response

1. Suspicious Activity Protocol:
    - 24/7 monitoring and alert system
    - Immediate investigation of alerts
    - Documented incident response procedures
    - Required customer cooperation
2. Enforcement Actions:
    - Service suspension capabilities
    - Account termination procedures
    - IP address blocking when necessary
    - Cooperation with law enforcement

CONTRACTUAL CONTROLS

1. Acceptable Use Policy (AUP):
    - Prohibits impersonation
    - Bans fraudulent activity
    - Requires legal compliance
    - Enables service suspension
2. Terms of Service (TOS):

- Requires cooperation with investigations
- Mandates response to illegal call allegations
- Enables call monitoring
- Requires documentation of remediation

COMPLIANCE AND UPDATES

1. Regulatory Compliance:
    - TCPA compliance
    - TRACED Act compliance
    - FCC regulations adherence
    - Industry best practices
2. Plan Maintenance:
    - Regular review and updates
    - Industry development monitoring
    - Staff training
    - Documentation of changes

This plan will be updated as needed to respond to new threats and regulatory requirements. Material changes will be filed with the FCC Robocall Mitigation Database within ten (10) days of such update.

Last updated: December 26, 2024

I declare under penalty of perjury under the laws of the United States of America that to the best of my knowledge the foregoing is true and correct.

Peter Priest
President
Fortel Networks, Inc.