



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

Robocall Mitigation Plan

Company Commitment

Fused Technology is committed to protecting consumers and the telecommunications ecosystem from illegal robocalls, spoofing, and fraudulent calling activity. We have implemented a comprehensive robocall mitigation program designed to prevent the origination, transmission, and processing of illegal voice traffic across our network.

Our robocall mitigation program incorporates customer vetting, traffic monitoring, call analytics, traceback cooperation, enforcement procedures, and industry best practices to identify and stop unlawful robocall traffic.

1. Reasonable Steps Taken to Prevent Illegal Robocall Traffic

Fused Technology has implemented the following affirmative and effective measures to prevent the origination, carrying, and processing of illegal robocall traffic:

A. Customer Verification and Due Diligence

Prior to activating service, we conduct a risk-based review of prospective customers that includes:

- Verification of legal business name and registration.
- Collection and validation of government-issued identification for individual customers when applicable.
- Verification of physical business address and contact information.
- Review of corporate formation documents and business licenses.
- Verification of tax identification numbers and business registrations.
- Screening against known fraud databases, enforcement actions, and high-risk industry indicators.
- Identification and verification of the customer's intended use of voice services.

B. Enhanced Review for High-Risk Customers

Customers identified as higher risk are subject to enhanced due diligence, including:

- Additional documentation requirements.
- Review of websites, marketing practices, and business operations.
- Verification of calling campaigns and traffic sources.
- Executive management approval prior to service activation.
- Ongoing heightened monitoring of traffic patterns.



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

C. Ongoing Traffic Monitoring

We continuously monitor traffic traversing our network for indications of unlawful robocalling activity, including:

- Excessive call volumes.
- Short-duration call patterns.
- Abnormally low answer rates.
- High complaint rates.
- Sequential dialing patterns.
- Neighbor spoofing indicators.
- Invalid, unallocated, or spoofed caller ID information.
- Traffic associated with known scam campaigns.

Traffic exhibiting suspicious characteristics is investigated promptly.

D. STIR/SHAKEN Implementation

Where required and technically feasible, Fused Technology authenticates and verifies caller identification information using the STIR/SHAKEN framework.

The company:

- Authenticates outbound calls originated by authorized customers.
- Verifies inbound call authentication information.
- Uses authentication results as part of fraud detection and mitigation efforts.
- Investigates traffic associated with failed or suspicious authentication results.

E. Traceback Participation

Fused Technology:

- Responds promptly to traceback requests from industry traceback organizations, law enforcement agencies, and regulatory authorities.
- Investigates the source of suspicious traffic identified through traceback efforts.
- Takes corrective action against customers responsible for unlawful traffic.



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

F. Enforcement Actions

When illegal robocall activity is identified, Fused Technology may:

- Issue warnings.
 - Require corrective action plans.
 - Suspend affected services.
 - Block suspicious traffic.
 - Terminate customer accounts.
 - Report unlawful activity to appropriate authorities.
-

2. Measures to Prevent New and Renewing Customers from Originating Illegal Calls

Fused Technology maintains affirmative, effective measures to prevent both new and renewing customers from originating illegal calls.

New Customer Controls

Prior to service activation, the company:

1. Conducts Know-Your-Customer (KYC) verification.
2. Confirms customer identity and legitimacy.
3. Reviews intended calling practices.
4. Evaluates customer risk factors.
5. Requires acceptance of anti-robocall contractual provisions.
6. Obtains certifications regarding compliance with applicable laws, including:
 - Telephone Consumer Protection Act (TCPA)
 - Truth in Caller ID Act
 - FCC robocall regulations



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

Contractual Safeguards

Customer agreements prohibit:

- Transmission of illegal robocalls.
- Caller ID spoofing.
- Fraudulent or deceptive calling practices.
- Use of automated dialing systems in violation of applicable laws.

Customers acknowledge that violations may result in immediate suspension or termination.

Renewing Customer Review Process

Prior to contract renewal or continued service:

- Customer traffic history is reviewed.
- Complaint records are evaluated.
- Traceback requests are reviewed.
- Any prior enforcement actions are examined.
- Customer compliance certifications may be updated.

Customers exhibiting suspicious activity may be subject to additional scrutiny, restrictions, or denial of renewal.

Ongoing Compliance Monitoring

All customers remain subject to ongoing monitoring throughout the service relationship, including:

- Automated traffic analysis.
- Complaint monitoring.
- Fraud scoring.
- Traceback review.
- Periodic account reviews.

3. Call Analytics Systems Used to Identify and Block Illegal Traffic

Fused Technology utilizes call analytics and network monitoring systems to identify potentially illegal robocall traffic.



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

Analytics Capabilities

The systems evaluate multiple risk indicators, including:

- Call velocity and volume.
- Call completion ratios.
- Answer-seizure ratios.
- Average call duration.
- Traffic spikes.
- Geographic calling patterns.
- STIR/SHAKEN attestation results.
- Invalid or spoofed caller ID information.
- Consumer complaint data.
- Known scam and fraud signatures.

Automated Detection

Call analytics systems generate alerts for:

- Suspicious traffic patterns.
- Potential spoofing activity.
- High-risk customer behavior.
- Robocall campaign indicators.
- Known fraudulent calling activity.

Blocking and Mitigation Actions

Based on analytics results, Fused Technology may:

- Block calls associated with illegal activity.
- Restrict traffic from specific customers.
- Apply additional verification controls.
- Escalate suspicious traffic for manual review.
- Suspend or terminate offending accounts.



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

Human Review

Automated analytics are supplemented by manual review conducted by trained personnel who:

- Investigate alerts.
 - Review customer records.
 - Analyze traffic patterns.
 - Determine appropriate enforcement actions.
-

4. Consumer Complaint Monitoring

Fused Technology reviews and investigates complaints received from:

- Consumers.
- Enterprise customers.
- Carriers.
- Regulatory agencies.
- Industry traceback organizations.

Complaint information is incorporated into ongoing risk assessments and mitigation efforts.

5. Employee Training and Governance

Personnel responsible for customer onboarding, compliance, fraud management, and network operations receive periodic training regarding:

- Robocall regulations.
- Traffic monitoring procedures.
- Customer due diligence requirements.
- Traceback obligations.
- Fraud detection techniques.

Senior management oversees the robocall mitigation program and reviews compliance activities regularly.



Fused Technology, Inc.
9520 Berger Road
Suite 212
Columbia, MD 21046
(410) 670-7200

6. Continuous Improvement

Fused Technology periodically evaluates and updates its robocall mitigation procedures to address evolving threats, regulatory requirements, and industry best practices. New controls, analytics capabilities, and fraud prevention measures are implemented as necessary to enhance the effectiveness of the program.

Certification

Fused Technology certifies that it has implemented the above-described robocall mitigation practices and continues to take reasonable, affirmative, and effective measures to prevent the origination, carrying, and processing of illegal robocall traffic on its network.

A handwritten signature in black ink, appearing to read 'M. Radik', is positioned above a horizontal line.

Marc Radik
President, Fused Technology, Inc.