

TELKART LLC ROBOCALL MITIGATION PLAN

Company Information

Telkart LLC

16192 Coastal Highway, Lewes, Delaware 19958, USA

4 Peddlers Row, Suite 1202, Newark, DE 19702

<https://telkartllc.com>

+1 (833) 835-5278

support@telkartllc.com

I. Background and Regulatory Framework

The Federal Communications Commission ("FCC" or "Commission") has established comprehensive requirements mandating voice service providers, including Telkart LLC ("Telkart"), to file certifications and robocall mitigation plans in the FCC's Robocall Mitigation Database ("RMD") pursuant to 47 CFR § 64.6305[1][2].

These regulations require all voice service providers to certify whether they have implemented the STIR/SHAKEN authentication framework and to demonstrate that all calls originated, carried, or processed are subject to a robocall mitigation program consistent with Commission rules[1]. The mitigation plan must include reasonable measures to prevent originating illegal robocall traffic and a commitment to respond within 24 hours to traceback requests from the Commission, law enforcement, and the Industry Traceback Group (ITG)[1].

Definition of Illegal Robocalls

The TRACED Act defines "robocall violation" as a violation of subsection (b) or (e) of section 227 of the Communications Act of 1934[1]. Telkart's mitigation program focuses on preventing two primary categories of unlawful calls:

- **47 U.S.C. § 227(b) violations** – Non-emergency calls initiated using a prerecorded or artificial voice, or an automatic telephone dialing system (ATDS) as defined by the Supreme Court in *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2021), without proper consent
- **47 U.S.C. § 227(e) violations** – Truth in Caller ID Act violations involving the knowing transmission of misleading or inaccurate caller identification information with intent to defraud, cause harm, or wrongfully obtain anything of value

The Commission has clarified that a robocall mitigation program is sufficient if it includes detailed practices reasonably expected to significantly reduce the provider's origination or carriage of illegal robocalls, provided the voice service provider complies with the practices described in its plan[1].

Annual Recertification Requirements (2026)

Effective February 5, 2026, the FCC implemented enhanced RMD compliance requirements including mandatory annual recertification by March 1st of each year, beginning March 1, 2026[3][4]. Voice service providers must verify the accuracy of all RMD information annually and update their FCC Registration Number (FRN) within 10 business days of any changes[3].

II. Telkart's Know Your Customer (KYC) Standards

Telkart operates as a voice service provider and wholesale intermediate carrier (both gateway and non-gateway) focused on business users and wholesale voice services. As part of its customer onboarding and renewal processes, Telkart implements comprehensive KYC procedures to verify customer identity, assess regulatory compliance, and mitigate risks associated with unlawful use of telecommunications services.

2.1 Customer Classification

Telkart distinguishes between two primary customer categories, applying tailored vetting practices to each:

- **Reseller Customers** – Entities purchasing telecommunications services from Telkart for resale or redistribution to downstream customers
- **End-User Customers** – Entities purchasing telecommunications services from Telkart for their own use without intent to resell

2.2 KYC Requirements for Reseller Customers

All reseller customers must complete a comprehensive KYC questionnaire and provide the following information prior to service activation or renewal:

Information Required	Details
Customer Business Name	Legal entity name and any DBA (Doing Business As) names
Entity Type	Corporate structure and state or country of incorporation
Physical Business Location	Current operational address
Previous Addresses	Any prior business locations (if applicable)
Contact Persons	Main, technical, and compliance contacts with business phone numbers and email addresses

Trade and/or Bank References	At least two verifiable references
Federal Tax ID Number	Employer Identification Number (EIN)
FCC 499 Filer ID	FCC Form 499 registration number
FCC Registration Number (FRN)	Current FCC FRN
Operating Company Number (OCN)	OCN if applicable to carrier type
Robocall Mitigation Database Filing	Proof of RMD certification indicating STIR/SHAKEN compliance or approved mitigation plan
Departmental Contacts	Contact information for Sales, Billing, NOC, Legal, and Notices departments
Trade References	Contact details for at least two business partners or suppliers
Company Website	Customer-facing online presence
Written Consent	Signed certification acknowledging responsibility for robocall mitigation, traffic monitoring, TCPA compliance, and indemnification of Telkart for unlawful service use

Table 1: Reseller customer KYC requirements

2.3 KYC Requirements for End-User Customers

End-user customers must provide the following documentation and information:

Information Required	Details
Business Registration Certificates	Certificate of Incorporation, Articles of Organization, business license, or equivalent governmental registration documents
Registered Business Name	Legal entity name and any DBA names
Entity Type	Corporate structure and jurisdiction of registration
Registered Address	Primary business address
Previous Addresses	Any prior business locations (if applicable)
Business Owner Information	Names, titles, and contact information of beneficial owners and controlling parties
Contact Persons	Main, technical, and compliance contacts

Federal Tax ID Number	EIN or Tax Identification Number
Identity Verification	Third-party identity check of responsible person and/or owner through verification application, including government-issued ID verification, address confirmation, and fraud risk assessment
Company Website	Online presence if applicable

Table 2: End-user customer KYC requirements

2.4 Verification Practices

Telkart's verification procedures include:

- Confirming carrier customers' registration status in the FCC's Form 499 Filer database
- Verifying active certification in the Commission's Robocall Mitigation Database
- Conducting internet research into the company's publicly accessible online profile
- Reviewing potential call-related complaint history and traceback records
- Performing reference checks with prospective customers' other carrier suppliers
- Analyzing new account traffic profiles for patterns relating to call duration, caller ID usage, Answer-Seizure Ratio (ASR), and other quality metrics
- Conducting third-party identity verification for end-user customers, including background checks

2.5 USF Exemption Certificate

For carrier-to-carrier wholesale traffic, Telkart collects a USF Exemption Certificate documenting the customer's status as a telecommunications carrier purchasing services for resale, ensuring proper Universal Service Fund contribution treatment.

III. Acceptable Use Policy

All Telkart customers must execute formal written contracts that include binding commitments to comply with Telkart's Acceptable Use Policy (AUP). The AUP prohibits:

- **Illegal Activities** – Using services for any illegal, abusive, false, fraudulent, deceptive, or misleading purposes, or any activity that exploits, harms, or threatens to harm children
- **TCPA Violations** – Engaging in unsolicited advertising, marketing, or other unlawful activities that violate:
 - Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.)
 - Telephone Consumer Protection Act (47 U.S.C. § 227)

- FCC TCPA regulations (47 C.F.R. § 64.1200 et seq.)
- All federal and state Do Not Call and calling-time restriction laws
- **Caller ID Spoofing** – Creating false identity, forged email addresses or headers, phone numbers, or otherwise attempting to mislead others about sender identity or message origin, including failing to comply with the Truth in Caller ID Act

Telkart's customer contracts authorize immediate suspension and/or termination of all services in the event of an AUP violation.

IV. STIR/SHAKEN Implementation and Telephone Number Authorization

4.1 Full STIR/SHAKEN Deployment

Telkart has fully implemented the STIR/SHAKEN authentication framework across its entire network in compliance with 47 C.F.R. § 64.6302-64.6305[1][5]. Telkart's network accurately signs and transmits all STIR/SHAKEN-related data received in the call path, consistent with Commission requirements.

4.2 Telephone Number Authorization and Attestation

Telkart restricts end users to making calls only from telephone numbers that Telkart has assigned to them or numbers for which they have demonstrated a right to use. Telkart applies appropriate attestation levels to such calls based on the degree of verification:

- **Full Attestation (A)** – Applied when Telkart has verified both customer identity and the customer's right to use the telephone number
- **Partial Attestation (B)** – Applied when Telkart has verified customer identity but cannot fully verify number usage rights
- **Gateway Attestation (C)** – Applied when Telkart operates as gateway provider and cannot verify call origin

4.3 Restrictions on Prerecorded Voice Calls

Telkart restricts end users from making prerecorded or artificial voice calls to ensure compliance with TCPA requirements and to prevent unlawful robocalling activity.

V. Proactive Network Monitoring and Analytics



Telkart employs multiple layers of proactive network monitoring to identify and block potentially illegal robocall traffic.

5.1 Current Monitoring Systems

ANI Scores via YouMail

Telkart utilizes ANI (Automatic Number Identification) scoring provided by YouMail, assigning reputation scores to calling numbers based on consumer complaints, feedback, and calling patterns. The system automatically rejects calls from ANIs marked as spam or scam.

Do Not Originate (DNO) Filtering

Telkart uses DNO list filtering to prevent customers from dialing phone numbers on Do-Not-Originate lists, including government agency numbers (911, IRS, Social Security Administration), unassigned number blocks, and known spoofing victim numbers.

Spoofing Filter Tool

Telkart's softswitch platform includes a built-in spoofing filter tool that blocks calls from ANIs marked as spam/scam and detects spoofed caller ID patterns. The system analyzes calling number patterns for signs of manipulation and blocks unauthorized caller ID usage.

5.2 Advanced AI Call Screening (In Testing)

Telkart is testing advanced AI-powered call screening, monitoring, and reporting systems to analyze traffic for potentially suspicious patterns associated with illegal robocalls or other unlawful usage. Upon completion of testing, Telkart plans to deploy these systems to production.

5.3 Traffic Analysis Criteria

Telkart's monitoring systems assess and flag traffic based on various criteria including:

- Matching NPA-NXXs of calling and called parties' telephone numbers (neighborhood spoofing)
- Calls purporting to originate from telephone numbers on Do-Not-Originate lists
- Call patterns sourced from fraud prevention provider robocall mitigation tools
- Abnormal call duration patterns, Answer-Seizure Ratios, and call volume spikes
- Sequential number dialing patterns typical of robocall campaigns

5.4 Response to Suspicious Activity

When Telkart detects patterns consistent with illegal robocalls or has reason to suspect illegal robocalling or spoofing on its network, Telkart takes prompt action to:

- Identify the party using Telkart's network to carry the suspicious calls
- Investigate the customer's traffic patterns and call detail records
- Implement immediate blocking or rate limiting of suspicious traffic
- Contact the customer to request explanation and remediation
- Take appropriate enforcement action including service suspension or termination

- Report violations to appropriate authorities

VI. Traceback Cooperation and 24-Hour Response Commitment

6.1 Commitment to Timely Response

Telkart commits to respond fully and in a timely manner, **within 24 hours**, to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group (ITG). Telkart will cooperate fully with such entities in investigating and stopping any illegal robocallers that use its service to originate, carry, or process illegal robocalls.

6.2 Dedicated Resources and Procedures

Telkart dedicates sufficient resources to provide timely and complete responses to traceback requests. The company will investigate suspicious activity identified by its monitoring systems or reported by appropriate parties and take appropriate action.

6.3 Contractual Traceback Requirements

Telkart includes traceback cooperation language within its carrier interconnection and service agreements, requiring parties to:

- Promptly identify the upstream provider from which a suspected illegal robocall entered their network, or the customer from which the call originated
- Respond to traceback requests within required timeframes
- Provide complete and accurate information necessary for successful traceback
- Cooperate throughout investigation and enforcement processes

6.4 Designated Points of Contact

Telkart maintains designated points of contact for traceback and compliance matters:

Contact Type	Information
General Compliance	support@telkartllc.com
Phone	+1 (833) 835-5278
Primary Address	16192 Coastal Highway, Lewes, DE 19958
Operations Address	4 Peddlers Row, Suite 1202, Newark, DE 19702
Website	https://telkartllc.com

Table 3: Telkart traceback contact information

VII. Know Your Upstream Provider Procedures

While not specifically required for non-gateway intermediate providers, Telkart has implemented "know-your-upstream-provider" procedures as follows:

- Verification of upstream providers' RMD certification status before establishing interconnection
 - Contractual requirements for upstream providers to comply with traceback requests
 - Monitoring of traffic quality and compliance patterns from each upstream provider
 - Periodic review of upstream providers' regulatory standing
 - Termination of relationships with upstream providers involved in robocall violations or non-compliance
-

VIII. Compliance Monitoring and Continuous Improvement

8.1 Ongoing Compliance Review

Telkart conducts regular reviews of its robocall mitigation program effectiveness, including:

- Quarterly audits of customer KYC documentation completeness
- Monthly statistical analysis of network traffic patterns
- Annual comprehensive review of RMD filing accuracy in advance of March 1 recertification deadline
- Review of all traceback requests and response timeliness
- Assessment of AUP enforcement consistency and effectiveness

8.2 Technology Enhancement

Telkart continuously evaluates and tests new technologies for robocall detection, prevention, and mitigation. The company monitors FCC proceedings and industry best practices to ensure its mitigation program remains effective against evolving robocall threats.

8.3 Policy Updates

This Robocall Mitigation Plan is subject to periodic review and update to reflect changes in applicable laws, regulations, FCC guidance, industry standards, and Telkart's business operations. Material changes will be communicated to customers and updated in the RMD filing as required.

IX. Enforcement and Accountability

9.1 Customer Violations

Violations of Telkart's AUP or applicable telecommunications laws result in:

- Immediate investigation and traffic review
- Service suspension pending remediation for serious violations
- Permanent service termination for egregious violations such as illegal robocalling or spoofing
- Reporting to FCC Enforcement Bureau, ITG, and law enforcement as appropriate
- Legal action to recover damages and costs

9.2 Records Retention

Telkart maintains comprehensive records to support regulatory compliance and enforcement activities:

- Customer KYC documentation for duration of relationship plus 5 years
 - Call detail records for minimum 18 months
 - Traceback requests and responses for 5 years
 - RMD certifications for duration plus 5 years
 - Traffic monitoring reports for 3 years
 - Enforcement action records for 7 years
-

X. Conclusion

Telkart LLC is committed to combating illegal robocalls and maintaining the highest standards of regulatory compliance. This Robocall Mitigation Plan demonstrates Telkart's comprehensive approach to preventing unlawful use of its network through rigorous KYC procedures, proactive network monitoring, full STIR/SHAKEN implementation, and dedicated cooperation with traceback investigations.

Telkart will continue to dedicate resources, implement advanced technologies, and maintain vigilant oversight to ensure its robocall mitigation program remains effective in protecting consumers and the telecommunications network from illegal robocall traffic.

Document Control



Effective Date: February 25, 2026

Next Review Date: February 2027

Approved By: Husain Patanwala - CEO