

Robocall Mitigation Program Description

OWS LLC

Prepared for submission to the FCC Robocall Mitigation Database (RMD)

NON-CONFIDENTIAL — REDACTED VERSION

This public version omits security-sensitive implementation details, internal thresholds, technical identifiers, customer-specific information, and other non-public operational information.

1. Purpose and Scope

OWS LLC maintains a robocall mitigation program designed to reduce the origination, carrying, and processing of illegal robocalls and unlawful caller-ID spoofing. The program applies risk-based controls throughout customer onboarding, traffic activation, ongoing traffic monitoring, complaint handling, traceback response, and termination or suspension of traffic when appropriate.

2. Customer and Traffic Onboarding Controls

OWS LLC performs customer and business-purpose review before traffic is permitted. The company evaluates intended traffic type, calling campaigns, expected calling patterns, use of telephone numbers, and available customer information to identify elevated-risk traffic. Customers are expected to provide accurate information and cooperate with compliance and traceback inquiries. Traffic may be restricted, suspended, or terminated when unlawful calling, material policy violations, misleading caller-ID practices, or unresolved compliance concerns are identified.

3. Traffic Monitoring and Detection

OWS LLC monitors traffic for abnormal or high-risk calling patterns using available network and call-detail information. Monitoring may consider call volume, answer behavior, duration patterns, caller-ID behavior, complaint information, traceback activity, and other indicators associated with potentially unlawful or abusive traffic. Elevated-risk traffic may receive additional review, enhanced monitoring, routing restrictions, or other mitigation measures.

4. Caller-ID Authentication and Spoofing Controls

Where applicable to portions of OWS LLC's network and traffic under its control, OWS LLC supports caller-ID authentication and validation practices consistent with applicable STIR/SHAKEN requirements. The company also uses reasonable controls to identify and address suspicious or unauthorized caller-ID use and may request supporting information when caller-ID ownership or use is questioned.

5. Complaint, Traceback, and Incident Response

OWS LLC investigates credible reports of illegal robocalls, spoofing, spam, or other unlawful traffic. When a traceback request is received from the FCC, law enforcement, or the industry traceback consortium, OWS LLC will cooperate with the investigation and respond within the applicable 24-hour period required by FCC rules. Available call records, customer records, routing information, and related technical data may be used to identify relevant parties. Where violations are identified, OWS LLC may block or suspend traffic, require corrective action, apply enhanced monitoring, or terminate service.

6. Blocking and Remediation

OWS LLC may block numbers, routes, campaigns, customers, or traffic patterns associated with confirmed or materially suspected unlawful activity. Mitigation actions may include traffic suspension, route restriction, caller-ID restrictions,

customer remediation requirements, enhanced verification, and termination of service. Previously identified abusive traffic patterns may be reviewed to detect materially similar activity.

7. Recordkeeping and Compliance Oversight

OWS LLC maintains appropriate records relating to customer onboarding, traffic investigations, complaints, traceback requests, mitigation actions, and material compliance incidents. Records are retained and handled in accordance with applicable legal, contractual, and internal requirements. Significant incidents and remediation actions may be reviewed by designated compliance or management personnel.

9. Program Governance and Continuous Improvement

OWS LLC periodically reviews its robocall mitigation controls in light of traceback activity, complaints, observed traffic patterns, regulatory developments, and changes in network or customer risk. Where weaknesses or new abuse patterns are identified, OWS LLC may revise its monitoring, verification, blocking, escalation, or customer-management procedures.

10. Program Commitment

OWS LLC is committed to taking reasonable steps to significantly reduce illegal robocall activity associated with traffic that it originates, carries, or processes, as applicable to its role in the call path. OWS LLC will cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocallers and will respond to applicable traceback requests within the required timeframe.

8. Public Disclosure / Redactions

This non-confidential version intentionally omits security-sensitive implementation details, internal monitoring thresholds, technical identifiers, customer-specific information, and other information not necessary for the public to understand OWS LLC's robocall mitigation program.

Filing verification note: Before submission, OWS LLC should verify that every operational statement accurately describes controls it actually maintains and that its RMD certification, STIR/SHAKEN status, role in the call path, responsible contact information, and other portal fields are consistent with current FCC records.

Reference: FCC Robocall Mitigation Database requirements and applicable FCC guidance, including 47 CFR §64.6305.