

ROBOCALL MITIGATION PRACTICES & PROCEDURES

Truck In Dispatch LLC

1. Robocall Mitigation Practices

Truck In Dispatch LLC ("the Company") implements the following robocall mitigation practices across its network to prevent the origination, transit, or termination of illegal robocall traffic.

1.1 Know Your Customer (KYC) Vetting

1. Identity verification: The Company verifies the legal identity, business registration, and physical address of all customers originating traffic on its network prior to activating service.
2. Authorized use of telephone numbers: Customers must demonstrate a right to use the calling numbers assigned to them, including for numbers used in outbound dialing campaigns.
3. Contractual compliance obligations: All customer contracts include express provisions prohibiting the use of the Company's network to originate illegal robocalls, spoofed caller ID, or traffic that violates the Telephone Consumer Protection Act (TCPA) or the Truth in Caller ID Act.
4. Risk-based due diligence: Customers engaged in high-volume outbound calling, telemarketing, or robocall-adjacent business models are subject to enhanced due diligence, including review of call scripts, consent records, and opt-out mechanisms.
5. Ongoing monitoring: Customer risk profiles are reassessed periodically and upon any material change in calling patterns or volume.

1.2 Know Your Upstream Provider (KYUP) Practices

6. The Company reviews the Robocall Mitigation Database (RMD) filing status of any upstream provider from which it accepts traffic and declines to accept traffic from providers that do not appear in the RMD, where required by rule.
7. Upstream provider contracts include representations and warranties regarding compliance with STIR/SHAKEN and robocall mitigation obligations.
8. The Company reserves the right to audit call detail records (CDRs) and traffic patterns from upstream providers to identify anomalous or high-risk traffic.

1.3 Call Traffic Monitoring and Analytics

9. Automated monitoring of call volumes, call durations, and calling patterns to detect signatures consistent with illegal robocalling (e.g., abnormally short call durations, high-volume short-burst dialing, sequential number dialing).
10. Monitoring for Do-Not-Originate (DNO) list violations and known spoofed number patterns published by industry sources.

11. Threshold-based alerting that flags customer accounts exceeding defined call volume or complaint thresholds for manual review.
12. Periodic sampling and review of outbound call traffic to confirm compliance with contractual and legal obligations.

1.4 Contractual Prohibitions and Enforcement

13. Customer agreements expressly prohibit: (a) originating calls with unauthorized or spoofed caller ID information; (b) placing calls without required prior express consent under the TCPA; (c) using autodialers or prerecorded/artificial voice messages in violation of applicable law; and (d) evading Do-Not-Call registry requirements.
14. Violations may result in graduated enforcement actions, including warning notices, suspension of outbound calling privileges, and termination of service.
15. The Company maintains the right to immediately suspend service, without prior notice, where there is credible evidence of ongoing illegal robocalling activity presenting imminent consumer harm.

1.5 Consumer Complaint Handling

16. The Company maintains a documented process for receiving and investigating consumer complaints regarding suspected illegal or unwanted robocalls originated on its network.
17. Complaints received directly, or referred from the FCC, FTC, state attorneys general, or industry traceback groups, are logged, investigated, and, where substantiated, result in corrective action against the responsible customer account.
18. The Company designates a Robocall Mitigation point of contact responsible for receiving and responding to complaints and inquiries from regulators and industry partners.

2. Call Traceback Cooperation

Truck In Dispatch LLC cooperates fully and in a timely manner with call traceback requests from:

- The USTelecom Industry Traceback Group (ITG).
- The Federal Communications Commission (FCC) Enforcement Bureau.
- The Federal Trade Commission (FTC).
- State attorneys general and other law enforcement authorities.
- Other voice service providers participating in an active traceback investigation.

The Company's standard practice is to respond to traceback requests within the timeframe requested by the initiating party, and in all cases within a commercially reasonable period not to exceed the timeframes recommended by the ITG (typically within 24–48 hours for active investigations). Traceback responses include identification of the upstream provider or customer from which the traffic was received, and relevant call detail records, to the extent permitted by law.

3. Recordkeeping

19. Customer identity verification and KYC records are retained for the duration of the customer relationship and for a minimum retention period of 24 months following termination, or longer if required by applicable law or an active investigation.
20. Call detail records (CDRs) relevant to traceback and robocall mitigation investigations are retained consistent with applicable regulatory retention requirements.
21. Complaint logs, enforcement actions, and traceback correspondence are retained and made available for regulatory review upon lawful request.
22. This document and all prior versions are retained as part of the Company's compliance record.

4. Employee Training and Governance

23. All employees involved in customer onboarding, network operations, or compliance functions receive training on the Company's robocall mitigation obligations, KYC procedures, and traceback response protocols upon hire and at least annually thereafter.
24. The Company designates a Robocall Mitigation Compliance Officer responsible for oversight of these practices, coordination of traceback responses, and maintenance of the Robocall Mitigation Database filing.