

FCC Robocall Mitigation Database Filing: Robocall Mitigation Plan (RMP)

Filing Entity: TrackDrive, LLC

1. Role in Call Processing

TrackDrive, LLC, a Colorado limited liability company (“TrackDrive”), does not originate or terminate calls directly. Instead, TrackDrive facilitates call routing and media handling through the use of Freeswitch and Plivo. TrackDrive does not operate as a gateway provider or deliver international calls into the United States directly. Based on Federal Communications Commission (“FCC”) definitions, TrackDrive operates in the following roles:

- Non-Gateway Intermediate Provider

TrackDrive partners with upstream and downstream providers to route calls but does not originate or terminate calls directly.

2. STIR/SHAKEN Compliance

TrackDrive does not sign calls with its own STIR/SHAKEN certificates. Instead, all outbound traffic is signed by terminating partners, which include:

- Commio
- Plivo
- Inteliquent
- Third Base International

These partners are responsible for inserting authenticated identity headers on behalf of TrackDrive before delivering calls to the terminating network.

3. Robocall Mitigation Practices

TrackDrive employs a comprehensive, multi-layered robocall mitigation strategy designed to proactively detect and eliminate illegal robocall traffic and telemarketing fraud on the TrackDrive Platform. Because TrackDrive operates as an Intermediate Provider, it does not rely solely on upstream carriers for mitigation; instead, it utilizes advanced identity verification (KYC) and contractual enforcement to ensure network integrity.

TrackDrive’s active robocall mitigation program consists of the following pillars:

3.1. Customer Onboarding and Identity Verification (KYC/KYB)

TrackDrive enforces a multi-layered vetting process for all prospective customers prior to

allowing full utilization of the network. No customer may actively transact or conduct bulk origination on the platform without completing the following verification protocols:

- **Identity Verification (KYC):** Every customer onboarded to TrackDrive is required to complete Stripe Identity KYC. This process mandates the submission of a valid, government-issued photo ID (passport or driver's license) alongside a real-time selfie liveness check to confirm the user's identity.
- **Payment Method Verification:** To prevent fraudulent account creation and billing abuse, every payment method added to a TrackDrive account undergoes a micro-authorization charge challenge. TrackDrive issues a reversible charge, and the user must accurately input the exact challenge amount to verify card ownership. This protocol has successfully mitigated system-wide billing and identity fraud.
- **Business Registration (KYB):** TrackDrive enforces a Business Identity verification protocol to map outbound traffic to a verified corporate or sole-proprietor entity. Customers must validate their legal status by providing their verified business identity, Employer Identification Number (EIN), and operational details directly through a secure, platform-mediated compliance interface. To satisfy this authorization gate, all customers must execute a binding legal electronic certification attesting to the accuracy of their business identity and explicitly warranting their compliance with all applicable federal and state outbound calling regulations prior to originating traffic. Additionally, TrackDrive provides an integrated platform capability allowing verified users to seamlessly register their authorized telephone numbers directly with industry registries for carrier-level trust and mitigation.

3.2. Traffic Monitoring, Call Authentication, and Incident Response

TrackDrive employs comprehensive technical and operational controls to monitor network traffic, authenticate caller identity, and immediately mitigate suspected illegal robocalling activity.

- **Caller-ID Integrity and Anti-Spoofing:** TrackDrive is structurally incapable of placing spoofed calls. The platform's codebase performs a hardcoded Caller-ID authorization check prior to every call origination.
- **Targeted Manual Compliance Review Protocol:** TrackDrive utilizes a mandatory, system-triggered manual compliance review process for newly provisioned and dually flagged accounts. The TrackDrive compliance team is automatically notified by event-driven backend triggers to conduct manual audio auditing of initial account activity. Platform-level recording is structurally mandated during these validation periods, and staff manually reviews the interactions to verify TCPA and TSR compliance before an account is cleared for unmonitored traffic permissions.
- **Continuous Behavioral Auditing:** TrackDrive utilizes automated monitoring systems to detect anomalies in traffic profiles, including spikes in volume, high short-duration call ratios, or patterns indicative of dormant account reactivation. Any account triggering these behavioral thresholds is automatically restricted and returned to the mandatory

manual compliance review queue.

3.3. Contractual Enforcement and Traceback Cooperation

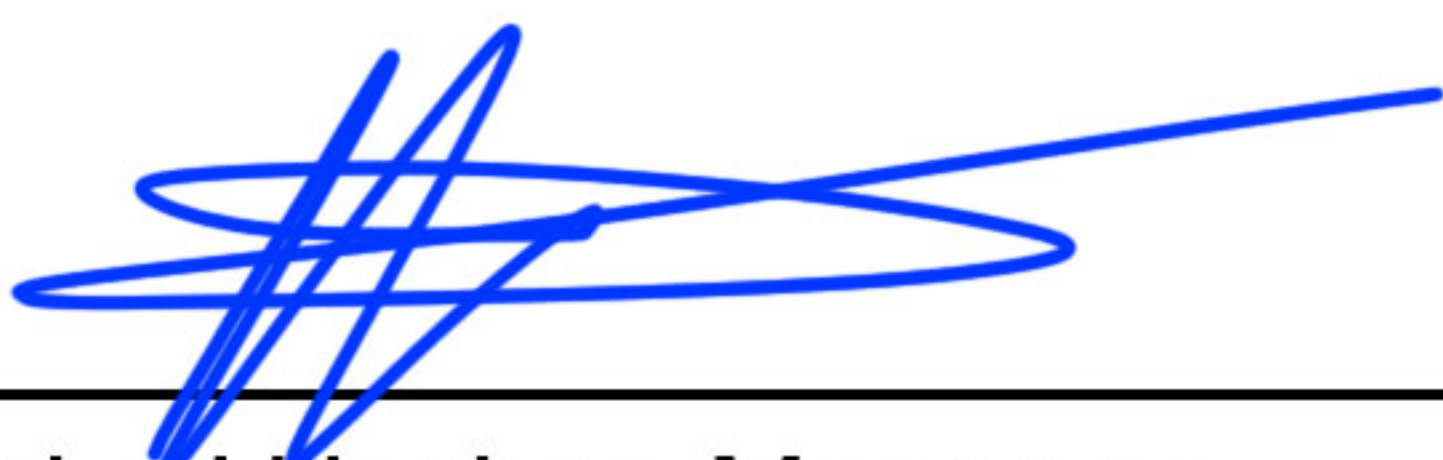
TrackDrive enforces mitigation policies through legally binding frameworks and active industry cooperation.

- **Zero-Tolerance Terms of Service:** TrackDrive's Terms of Service explicitly prohibit the origination of illegal robocalls, caller ID spoofing, and any violations of the TCPA, the FTC Telemarketing Sales Rule (TSR), and state wiretapping laws. TrackDrive reserves and exercises the contractual right to immediately suspend or terminate, without prior notice, any account suspected of originating fraudulent or illegal traffic.
- **Zero-Tolerance Suspension SOP:** TrackDrive operates under a Platform Compliance Response Standard Operating Procedure (SOP). Under this SOP, if TrackDrive receives abuse reports, ITG traceback requests, or identifies fraud through its own manual review processes, the offending customer account is automatically and immediately suspended and banned from the network. TrackDrive coordinates fully with terminating carriers, the FCC, and law enforcement in these instances.
- **Traceback & Upstream Compliance:** TrackDrive actively monitors traffic patterns and cooperates fully with the Industry Traceback Group (ITG) and law enforcement regarding suspicious call behavior. Further, TrackDrive only routes traffic through reputable upstream carriers possessing valid FCC 499 IDs, and contractually requires all partners to comply with STIR/SHAKEN frameworks and maintain active, valid registrations in the FCC's Robocall Mitigation Database.
- **STIR/SHAKEN Attestation Alignment:** Through TrackDrive's upstream verification protocols, all compliant traffic passed to terminating partners is structured to ensure it is signed at Attestation Level A by the downstream network injector.

4. Certification

The undersigned, acting solely in his official capacity as the Manager of TrackDrive, certifies on behalf of TrackDrive that the above information is accurate and complete to the best of his knowledge, information and belief, and further affirms that TrackDrive has implemented measures to mitigate illegal robocall traffic as required under the FCC's rules.

TrackDrive, LLC

By: 
Blake Hilscher, Manager