



12900 Maurer Industrial Drive, St. Louis, MO 63127

DriveCentric provides software as a service to automotive dealerships and automotive adjacent verticals. Our company is committed to preventing the origination and transmission of illegal robocalls. We have the following processes and safeguards in place to ensure compliance with FCC regulations.

Customer Onboarding and Agreements

- All new customers undergo a thorough onboarding process that includes full identity verification and business validation.
- End user license agreements explicitly prohibit the use of our software for originating illegal robocalls.

System Monitoring and Anomaly Detection

- We utilize a combination of application monitoring (Elastic.co APM) and security monitoring (CrowdStrike Falcon) to detect anomalous usage patterns that could indicate potential robocalling activity.
- Suspicious events trigger alerts that are evaluated and mitigated by our internal teams to prevent misuse of our systems.
- Our anomaly detection thresholds are continually tuned based on the evolving threat landscape to maintain the effectiveness of our monitoring capabilities.

Upstream Provider Management

- We have verified that our upstream providers are registered in the FCC's Robocall Mitigation Database and are compliant with STIR/SHAKEN caller ID authentication standards.

Incident Response

- Our incident management processes enable us to quickly address potentially abusive activities on our platform and prevent further harm.
- We conduct regular tabletop exercises to practice identifying and shutting down applications that are being used for harmful or illegal purposes, including robocalling.

DriveCentric designed our software to require manual action for initiating every call placed through our platform. This measure ensures that all calls are deliberately initiated by authorized users and cannot be automated without direct human involvement. This design deliberately prevents the platform from being used for illegal robocalling or mass-calling campaigns.

User Authentication

- Only authenticated users with valid credentials can access the platform and initiate calls.
- Two-factor authentication is required to access the software.
- Each user's activity is tracked and logged to ensure accountability.

Human Interaction Required

- A call cannot be initiated until a user manually selects a recipient.
- Calls are triggered individually, with no mechanism to support bulk or automated dialing

No Auto-Dialing Capability

- Our software does not include features for automated or sequential dialing.
- This design eliminates the possibility of using the platform for illegal robocalling operations.

We will continue to evaluate and adopt industry best practices to strengthen our robocall prevention posture. Preventing the misuse of our services for illegal robocall delivery is a company priority and we are committed to regularly enhancing our mitigation approach.