



Phone Incorporated ApS
(Phone.inc)
DK-46213564
Højbro Plads 10
1200 Copenhagen K
Denmark

Compliance Contact:
Niklas Stephenson, CEO
compliance@phone.inc

Plan Version: 1.1
Effective Date: June 2026

1. INTRODUCTION

Phone Incorporated ApS ("Phone.inc") is a Danish voice service provider routing voice traffic to the United States. Phone.inc is subject to FCC requirements under 47 CFR § 64.6305 and has certified its practices in the FCC's Robocall Mitigation Database (RMD).

Under FCC rules (47 CFR § 64.6305), all voice service providers in the call path to or within the U.S. must either implement STIR/SHAKEN caller ID authentication or maintain and certify a robocall mitigation program that includes:

- Reasonable steps to prevent the origination of illegal robocall traffic; and
- A commitment to full cooperation with law enforcement and traceback requests.

As a non-U.S. provider, Phone.inc is not eligible for STIR/SHAKEN credentials and instead maintains a mitigation-based compliance program in accordance with FCC requirements.

Phone.inc operates a mobile and desktop application for outbound voice calls, using only DID numbers purchased through the platform. The application exposes no SIP interface, API, or programmable calling mechanism to end users. As a result, automated dialing, robocalling, and caller ID spoofing are technically impossible: every call is manually initiated by an authenticated user, with their assigned DID presented as the caller ID.

2. CONTRACTUAL REQUIREMENTS AND PROHIBITIONS



Phone.inc's Terms of Service, which all users must accept prior to account activation, explicitly prohibit any use of the platform for automated calls, robocalling, spam calling, or any other activity that violates U.S. federal or state law, including the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, and relevant FCC regulations (47 CFR § 64.1200, § 64.6305).

Prohibited activities under Phone.inc's Terms of Service include:

- Any use of the platform to originate automated or prerecorded voice calls without the prior express consent of the called party, as required under the TCPA;
- Any attempt to manipulate, falsify, or circumvent caller ID presentation;
- Any use of the platform in a manner inconsistent with the manual, person-to-person calling model for which it is designed.

Because the Phone.inc application is closed and does not provide programmatic calling access, caller ID is always set to the user's purchased DID and cannot be altered by the user. These technical constraints serve as a built-in enforcement mechanism for the contractual prohibitions above.

Phone.inc reserves the right to suspend or terminate any account immediately and without prior notice upon evidence of non-compliant, suspicious, or unlawful activity, at its sole discretion.

3. CUSTOMER ONBOARDING AND ACCOUNT CONTROLS

Phone.inc implements a **Tiered, Risk-Based Verification Program** to ensure the legitimacy of its business customers and prevent the origination of illegal traffic.

3.1. Tier 1 (Automatic/Baseline)

Applied to every account at signup, these affirmative measures make mass or automated calling technically impossible:

- **Closed Architecture:** No SIP or API access; manual dialing only via authenticated apps.
- **DID-Locked CLI:** Outbound caller ID is strictly limited to the user's assigned DID.



- **Onboarding Requirements:** Mandatory ToS acceptance, a valid credit card, and a business address.
- **Fraud Screening:** Integration with Stripe Radar for identity and payment fraud detection.
- **Continuous Monitoring:** Automated traffic analysis to detect anomalous calling patterns.

3.2. Tier 2 (Risk-Triggered)

Invoked by traffic anomalies, customer complaints, traceback involvement, Stripe Radar flags, or high-risk signup indicators. Requires full KYC verification as a condition of continued service.

3.3. Tier 3 (Enforcement)

Immediate suspension or termination of service upon confirmed violation of terms or failure to complete requested Tier 2 verification.

These controls, combined with the application's inherent technical limitations, ensure that only legitimate, manually initiated calls are originated through the Phone.inc platform.

4. TRAFFIC MONITORING AND TRACEBACK RESPONSE

Phone.inc implements comprehensive internal monitoring alongside Stripe Radar and other tools to identify and mitigate potentially unlawful calling activity. Phone.inc performs its own independent controls to ensure network integrity.

Monitoring covers:

- Unusually high call volumes from individual accounts over short periods;
- Unusually short or anomalous average call durations;
- Any traffic patterns inconsistent with manual, person-to-person calling behavior;
- Complaints received from called parties or downstream carriers.

All outbound calls are presented with the caller's assigned DID as the caller ID. CLI values are validated against E.164 formatting requirements. No mechanism exists within the Phone.inc platform for users to alter or spoof their assigned DID.



If suspicious activity is identified, Phone.inc's compliance function initiates a review. The account holder may be contacted and required to explain the traffic in question. Phone.inc may suspend or terminate the account pending or following such review, at its sole discretion.

Phone.inc cooperates fully with all traceback requests received from the FCC, the ITG, or other authorized enforcement entities. Upon receipt of a traceback request, Phone.inc commits to:

- Responding within 24 hours, as mandated by the FCC under 47 CFR § 64.1200(n)(2);
- Identifying the source of the call within its network;
- Notifying the relevant account holder and requesting information regarding the traffic in question, where appropriate;
- Enforcing immediate corrective action, including account suspension or termination, where a violation is confirmed.

Niklas Stephenson, CEO, serves as the designated compliance contact for all traceback-related matters and can be reached at compliance@phone.inc. All investigations and actions taken are logged to ensure full auditability and regulatory defensibility.

5. ROBOCALL MITIGATION DATABASE COMPLIANCE

Phone.inc maintains an active RMD registration as required under 47 CFR § 64.6305 and updates it promptly upon any material change to this Plan.

6. POLICY GOVERNANCE AND COMPLIANCE RESPONSIBILITIES

Phone.inc maintains a structured governance approach to ensure ongoing compliance with FCC obligations.

6.1. Policy Review and Updates

This Robocall Mitigation Plan is reviewed at least annually, or sooner if required by:



- New or updated FCC rules, enforcement guidance, or declaratory rulings;
- Emerging robocall threats, technologies, or changes in industry mitigation standards.

Material changes to this Plan will be promptly reflected in Phone.inc's RMD certification. Phone.inc explicitly commits to completing RMD recertification annually between February 1 and March 1. Furthermore, Phone.inc will update its RMD filing within 10 business days of any material change, including changes to name, contact information, ownership, or STIR/SHAKEN implementation status.

6.2. Internal Compliance Responsibilities

Niklas Stephenson, CEO (compliance@phone.inc), is responsible for:

- Overseeing implementation of this Plan and all associated procedures;
- Monitoring developments in FCC robocall enforcement and updating procedures accordingly;
- Coordinating all investigations, traceback responses, and regulatory communications;
- Conducting periodic internal reviews to assess the effectiveness of mitigation controls.

6.3. Enforcement Action Disclosure

Phone.inc certifies that it has not been subject to any FCC or law-enforcement action or investigation for robocalling, spoofing, or RMD deficiency in the prior two years.

7. CORPORATE OWNERSHIP AND AFFILIATIONS

Phone Incorporated ApS is a standalone legal entity. Niklas Stephenson is the principal owner and exercises management control. Phone.inc has no affiliated voice service entities or DBA designations.



8. CONCLUSION

This Robocall Mitigation Plan outlines our company's formal commitment to preventing the origination of unlawful robocall traffic and maintaining full compliance with applicable U.S. FCC regulations. We implement a multi-faceted mitigation strategy that includes:

- Risk-based customer onboarding and fraud screening
- Binding contractual prohibitions against illegal robocalling and spoofing;
- Real-time traffic monitoring, anomaly detection, and caller ID validation;
- Full cooperation with traceback efforts initiated by the FCC, Industry Traceback Group (ITG), or authorized enforcement bodies;
- Immediate enforcement actions, including blocking or suspension of traffic deemed unlawful or non-compliant;

We are committed to the ongoing execution, periodic review, and continuous improvement of this Plan in response to evolving threats and regulatory developments. Our compliance team maintains accountability for implementation and regulatory communication.

By adhering to this framework, we protect the integrity of our network, uphold our responsibilities as an international voice service provider, and contribute to the global effort to combat illegal robocalls. Our active registration with the FCC's RMD affirms our good standing and operational commitment to delivering lawful voice traffic.