

Robocall Mitigation Plan – Updated Plan (2026)

The Masser Group Inc. dba Masser Technologies

Effective Date: 02/20/2026 (Updated for 2026 RMD Annual Recertification)

Supersedes/Updates: **Robocall Mitigation Plan effective 12/17/2024**

1. Purpose and Scope

This **Robocall Mitigation Plan** outlines the policies, practices, and procedures implemented by **The Masser Group Inc. dba Masser Technologies** (“we,” “us,” or “the company”) to combat unlawful and fraudulent robocalls. This plan adheres to the requirements set forth by the **Federal Communications Commission (FCC)** under the **TRACED Act**.

This plan applies to:

- Calls originating on our network.
- Traffic transiting through our network.

The goal is to **identify, mitigate, and prevent** unlawful robocalls while maintaining compliance with FCC rules for robocall prevention and consumer protection.

2. Company Contact Information

Company Name:	The Masser Group Inc. dba Masser Technologies
Contact Person:	Roger Curtis
Title:	Robocall Mitigation Officer
Email:	rcurtis@massertechnologies.com
Phone:	(915) 613-1211 ext. 102
Address:	5862 Cromo Dr, Suite 145, El Paso, TX 79912

3. Voice Ecosystem

Masser Technologies is a reseller of voice services provided by our upstream voice services provider (“VSP”), **PayG, LLC dba SkySwitch** (FRN 0027004217, RMD0002940). All calls that originate or terminate with our end customers are handled by our VSP.

4. Robocall Prevention Measures

We have implemented the following measures to prevent unlawful robocalls:

4.1. STIR/SHAKEN Implementation

- Our VSP has implemented the **STIR/SHAKEN** framework on IP-based voice networks to authenticate caller ID information.
- All calls originating from our network are verified and signed using our VSP's STIR/SHAKEN protocols to ensure legitimacy.

4.2. Robocall Traffic Monitoring

- **Real-time Monitoring:** Our VSP monitors outbound and inbound call traffic patterns for irregularities such as high call volumes, short call durations, or repetitive dialing.
- **Traffic Analytics:** Our VSP's system employs AI-based analytics tools to detect and flag suspicious robocall traffic.
- **Network Audits:** Regular audits are performed to identify potential sources of illegal robocalls.

4.3. Caller ID Validation

- Caller ID information is validated before calls are allowed to originate on our network.
- Only customer-assigned caller IDs are allowed to originate calls.
- Customers must register legitimate business phone numbers, and unregistered or spoofed caller IDs are blocked.

5. Know Your Customer

We utilize the mitigation technique of "Know Your Customer." We maintain close relationships with our end-customers who are all small and medium businesses (SMBs). We do not offer our voice services to residential customers.

5.1. Customer Registration

- All new customers must undergo a thorough vetting process before they are permitted to place calls on our network.
- Customers are either assigned Direct Inward Dial (DID) numbers as new customers or we will port in DID(s) from the customer's losing provider which requires a losing provider invoice for verification.

5.2. Terms of Service Compliance

- Our Terms of Service strictly prohibit the use of our services for unlawful robocalls, caller ID spoofing, or fraudulent activity.
- Violation of these terms will result in immediate suspension or termination of services.

5.3. Customer Monitoring

- We continuously monitor customer call behavior to identify any abnormal activity indicative of illegal robocall campaigns.
- Any flagged customers are investigated, and appropriate action is taken, including termination of service if necessary.

6. Mitigation of Identified Robocalls

We take the following actions when unlawful robocall activity is detected:

- **Immediate Blocking:** Calls identified as unlawful or suspicious are immediately blocked.
- **Customer Notification:** Affected customers are notified and required to cease unlawful activity.
- **Traffic Investigation:** Detailed investigations are conducted to identify the source and nature of illegal calls.
- **Escalation to Authorities:** Information regarding unlawful robocall activity is escalated to the FCC, FTC, or law enforcement agencies as required.

We affirm we will respond to requests from law enforcement, the FCC, and the Industry Traceback Group to trace suspect calls for mitigation efforts and will cooperate in investigating and stopping any illegal robocallers.

6.1 Traceback Cooperation – Response Timing (2026 Clarification)

For purposes of RMD recertification and in alignment with common industry practice reflected in provider certifications, we commit to responding to valid traceback requests **as soon as practicable and generally within 24 hours** of receipt.

7. RMD Accuracy, Annual Recertification, and Update Obligation (2026 Clarification)

We acknowledge the FCC's annual RMD recertification obligation due **March 1, 2026**, and we will verify that our RMD filing remains accurate and truthful as part of that recertification.

We also acknowledge the requirement that any changes to our RMD registration information be submitted **within 10 business days** of the change (including contact information, underlying providers, and related required RMD fields), and that failure to update or submitting inaccurate information may lead to enforcement consequences (including base forfeitures described in industry compliance notices).

8. Conclusion

The Masser Group Inc. dba Masser Technologies is committed to preventing unlawful robocalls and ensuring full compliance with FCC requirements. By using a VSP that has implemented STIR/SHAKEN, robust monitoring systems, and consumer protection measures, we aim to minimize the impact of illegal robocalls on our customers and network.

For questions regarding this Robocall Mitigation Plan, please contact: **Roger Curtis, Robocall Mitigation Officer.**