

# Robocall Mitigation Plan

Sharp Media Group, LLC

RMD Filing No.: **RMD0002939**

FRN: **0029065711** | OCN: **716L**

Effective date: **2025-08-28**

Version: **1.0**

This document describes Sharp Media Group, LLC's robocall mitigation program and the reasonable steps taken to prevent the origination of illegal robocall traffic.

## Document control

|                                    |                                  |
|------------------------------------|----------------------------------|
| <b>Document title</b>              | Robocall Mitigation Plan         |
| <b>Company</b>                     | Sharp Media Group, LLC           |
| <b>RMD Filing No.</b>              | RMD0002939                       |
| <b>FRN / OCN</b>                   | 0029065711 / 716L                |
| <b>Effective date</b>              | 2025-08-28                       |
| <b>Version</b>                     | 1.0                              |
| <b>Prepared by</b>                 | Chase Williams                   |
| <b>Robocall mitigation contact</b> | Chase Williams (Member, Support) |
| <b>Contact phone</b>               | 816-355-4500                     |
| <b>Contact email</b>               | chase@sharpmediallc.com          |

**Disclaimer:** This plan is intended to describe operational and technical measures implemented by Sharp Media Group, LLC. It is provided for robocall mitigation transparency and does not constitute legal advice.

## Table of contents

- 1. Program overview and objectives
- 2. Network description and call chain role
- 3. STIR/SHAKEN implementation
- 4. Know Your Customer (KYC) and customer eligibility controls
- 5. Analytic systems and mitigation / blocking controls
- 6. Complaint handling and internal investigations
- 7. Traceback response procedures (24-hour commitment)
- 8. Upstream provider management (know your upstream providers)
- 9. Recordkeeping, training, and program maintenance
- Appendix A. Robocall mitigation contact information

## 1. Program overview and objectives

Sharp Media Group, LLC maintains a robocall mitigation program designed to prevent the origination of illegal robocall traffic and to support rapid investigation and mitigation when suspicious activity is identified. The program combines (i) strict customer eligibility and Know Your Customer (KYC) procedures, (ii) technical access controls that limit who can originate traffic, (iii) analytic monitoring and escalation, and (iv) timely cooperation with traceback efforts.

Key program objectives include:

- Prevent unauthorized origination of calls by enforcing customer-specific, whitelisted origination IP addresses and blocking all other IP addresses.
- Limit service to known, vetted business customers and prohibit call centers and high-volume outbound calling use cases.
- Use upstream-carrier analytics (Bandwidth) and internal monitoring signals (complaints, traceback requests, abnormal volumes, and tracked abuse indicators) to identify suspicious or illegal traffic.
- Respond fully to traceback requests within 24 hours and take prompt mitigation action when warranted.

## 2. Network description and call chain role

Sharp Media Group, LLC operates as a voice service provider serving end users. The company originates VoIP calls for its customers and connects to the public switched telephone network (PSTN) through an upstream voice carrier.

**Upstream voice carrier:** Bandwidth.

Sharp Media Group restricts call origination at the network edge using customer-specific IP allow-listing. Only designated IP addresses for each customer are permitted to originate voice traffic; all other source IP addresses are blocked from origination.

## 3. STIR/SHAKEN implementation

Sharp Media Group, LLC certifies complete STIR/SHAKEN implementation for the calls it originates on its IP network. All calls originated by Sharp Media Group are signed prior to entering the PSTN.

Sharp Media Group's upstream voice carrier, Bandwidth, signs calls on Sharp Media Group's behalf. Sharp Media Group maintains an operational relationship with its upstream carrier to support call authentication and to address any call authentication-related issues.

## 4. Know Your Customer (KYC) and customer eligibility controls

Sharp Media Group limits VoIP service to customers that have an established relationship with the company for services other than VoIP. The company does not offer anonymous or self-service VoIP onboarding.

### Customer eligibility restrictions

- Only known customers with an existing, non-VoIP business relationship are eligible for VoIP service.

- Call centers and high-volume outbound calling use cases are not permitted.
- Any indication that a prospective customer intends to engage in mass outbound dialing, robocalling, or caller ID spoofing results in denial of service.

### **KYC controls at onboarding**

At onboarding (and as needed thereafter), Sharp Media Group performs risk-based identity and legitimacy checks, which include:

- Secretary of State (SOS) business registration verification for the customer's legal entity.
- Collection and validation of the customer's EIN.
- Collection of customer legal name, service address, and authorized point(s) of contact.
- Validation of publicly available indicators where available (for example, company website) to confirm consistency with the stated business identity and intended use.

### **Acceptable use and enforcement**

Customers are prohibited from originating illegal robocalls, using spoofed caller ID, or otherwise violating applicable law or FCC rules. Sharp Media Group enforces these requirements through monitoring and escalation actions described in Sections 5 and 6, including traffic blocking, suspension, and termination when warranted.

## **5. Analytic systems and mitigation / blocking controls**

Sharp Media Group uses layered technical and operational controls to identify and mitigate potentially illegal or abusive traffic.

### **5.1 Network access controls (customer IP allow-listing)**

- Each customer is assigned specific whitelisted IP address(es) authorized to originate voice/SIP traffic.
- All non-whitelisted IP addresses are blocked from originating voice traffic.
- IP allow-listing is reviewed and updated when customer origination environments change and as part of incident response.

### **5.2 Upstream-carrier analytics**

Sharp Media Group uses upstream-carrier analytics provided by Bandwidth to identify potentially illegal, suspicious, or abusive calling patterns and to support mitigation actions when such traffic is indicated.

### **5.3 Monitoring signals and triggers**

The following signals may trigger investigation or mitigation action:

- Customer or consumer complaints indicating unwanted, unlawful, or suspicious calling behavior.
- Traceback requests or inquiries from the FCC, law enforcement, or the industry traceback consortium.

- Abnormal calling volumes or calling pattern anomalies inconsistent with the customer's approved use case.
- Any tracked abuse indicators or evidence of system misuse.

### **5.4 Mitigation actions**

When suspicious or potentially illegal traffic is identified, Sharp Media Group may take one or more of the following actions, as appropriate to the circumstances:

- Block originating traffic (including immediate blocking of unauthorized origination IP addresses).
- Suspend service while investigating and requiring corrective action.
- Terminate service for confirmed or repeated abuse, or where the customer cannot provide a satisfactory explanation and remediation.
- Coordinate with the upstream carrier (Bandwidth) to support additional network-level mitigation if needed.

## **6. Complaint handling and internal investigations**

Sharp Media Group investigates reports of suspected illegal robocalling, spoofing, or other abusive calling behavior associated with its network. Complaints and inquiries are triaged and investigated promptly based on severity and available information.

### **6.1 Complaint intake channels**

- Email to the robocall mitigation contact: chase@sharpmediallc.com
- Telephone to the robocall mitigation contact: 816-355-4500
- Upstream carrier (Bandwidth) notices, analytics alerts, or abuse reports
- FCC, law enforcement, or traceback consortium inquiries

### **6.2 Investigation workflow**

- Confirm the call(s) or traffic pattern at issue using available call detail records (CDRs) and technical logs.
- Identify the associated customer account and the authorized origination source (including whitelisted IP address(es)).
- Determine whether activity is consistent with the customer's approved use case and acceptable use restrictions.
- Apply mitigation actions described in Section 5.4 as warranted (block, suspend, terminate).
- Document investigation findings and actions taken.

## **7. Traceback response procedures (24-hour commitment)**

Sharp Media Group will respond fully to traceback requests within 24 hours from the FCC, law enforcement, and the industry traceback consortium.

### **7.1 Traceback response steps**

- Acknowledge receipt of the traceback request and assign an internal owner.
- Review available call records and logs to identify the originating customer and source.
- Provide responsive information to the requesting entity, consistent with applicable law and privacy obligations.
- Take prompt mitigation action if the traffic appears illegal or abusive, including blocking/suspension/termination as appropriate.
- Coordinate with Bandwidth when escalation to upstream mitigation is needed.

## **8. Upstream provider management (know your upstream providers)**

Sharp Media Group maintains and monitors its upstream provider relationship with Bandwidth. This includes maintaining current points of contact for network operations and abuse issues, complying with upstream policies and requirements, and coordinating on mitigation actions when suspicious traffic is identified.

Upstream provider controls include:

- Maintain current upstream provider account and abuse/NOC contacts.
- Coordinate promptly with the upstream provider regarding analytics alerts, abuse reports, and mitigation actions.
- Support upstream requests for information needed to investigate suspected illegal robocalls, including traceback support within required timeframes.

## **9. Recordkeeping, training, and program maintenance**

### **9.1 Recordkeeping**

Sharp Media Group retains records sufficient to support its robocall mitigation obligations, including customer onboarding/KYC documentation, customer IP allow-list assignments, and call detail records/logs needed to investigate complaints and respond to traceback requests. Records are retained for a period consistent with operational needs and applicable legal requirements.

### **9.2 Training and awareness**

Personnel responsible for provisioning, network operations, and abuse response are expected to understand this plan and to escalate suspicious activity promptly to the robocall mitigation contact.

### **9.3 Review and updates**

Sharp Media Group reviews this plan periodically and updates it as its network, vendors, or mitigation controls change. RMD filings are updated within 10 business days.

## **Appendix A. Robocall mitigation contact information**

**Company:** Sharp Media Group, LLC

**Business address:** 5943 NE Antioch Rd, Gladstone, MO 64119

**Robocall mitigation contact:** Chase Williams (Member, Support)

**Contact business address:** 6000 N State Route 9, Suite A, Parkville, MO 64152

**Phone:** 816-355-4500

**Email:** chase@sharpmediallc.com

**Upstream voice carrier:** Bandwidth