

Responsive IP – Robocall Mitigation Plan

Responsive IP has implemented a robocall mitigation program designed to prevent the origination and transmission of illegal robocalls over our network. This program applies to **all voice traffic originating from, or transiting through, our network**.

1. Traceback Cooperation

Responsive IP commits to **fully and promptly cooperating** with the FCC, law enforcement agencies, and the Industry Traceback Group (ITG).

We will:

- Respond to traceback requests **as soon as possible, and no later than 24 hours** when feasible
 - Provide complete and accurate call detail records (CDRs) and related account information as permitted by law
 - Take **immediate mitigation action** when illegal traffic is identified, including blocking, suspension, or termination of service
-

2. Know-Your-Customer (KYC) Procedures

Responsive IP uses a **risk-based customer vetting process** before activating voice services. This includes:

- Identity verification of the individual and business entity
- Verification of authority to act on behalf of the business
- Collection of business formation documents where applicable
- Review of the customer's intended use of service
- Screening for high-risk industries commonly associated with illegal robocalling

New accounts are subject to **usage limitations and monitoring** until trust is established.

3. Contractual Compliance Requirements

All customers must agree to terms prohibiting the use of our services for illegal robocalling or unlawful telemarketing.

Our agreements explicitly allow Responsive IP to:

- **Immediately block traffic**
- **Suspend service**
- **Terminate accounts without notice**

if we detect or reasonably suspect illegal robocalling, spoofing, or traffic related to scams or fraud.

4. Traffic Monitoring & Analytics

Responsive IP employs **ongoing traffic monitoring** to identify suspicious patterns consistent with illegal robocalling or fraud. This includes monitoring for:

- Abnormally high call volumes
- Short-duration or high-velocity calling patterns
- Invalid, unallocated, or spoofed caller ID
- Neighbor spoofing patterns
- Traffic pumping and artificial traffic inflation
- International toll fraud indicators

We use automated and manual review processes. When suspicious traffic is detected, we investigate and take **rapid mitigation action**, which may include blocking calls or terminating the customer.

5. Upstream & Downstream Provider Controls

Responsive IP only exchanges traffic with voice service providers that are **listed in the FCC Robocall Mitigation Database at the time traffic is exchanged**, as required by FCC rules.

We periodically verify the RMD status of upstream providers and reserve the right to block traffic from providers that fall out of compliance.

6. STIR/SHAKEN Implementation

Responsive IP has implemented **STIR/SHAKEN call authentication** across our IP network as required by the FCC.

We:

- Authenticate calls using the STIR/SHAKEN framework
 - Assign attestation levels (A, B, or C) based on our relationship with and knowledge of the customer
 - Ensure accurate caller ID information is used in call signaling
 - Investigate and act on calls that fail authentication or appear to use spoofed caller ID
-

7. Mitigation of Illegal Robocalls

If Responsive IP identifies traffic that is illegal or highly likely to be illegal, we will:

1. **Immediately investigate** the source
2. **Block the traffic** where appropriate
3. **Notify the customer** (unless prohibited by law enforcement guidance)
4. **Suspend or terminate service** for confirmed violations

We maintain internal records of mitigation actions and traceback responses.

8. Ongoing Compliance Commitment

Responsive IP continuously reviews and updates its robocall mitigation practices to remain aligned with FCC rules, industry standards, and emerging robocall threat patterns.