

# Robocall Mitigation

This document details the preventative measures and commitments to mitigate illegal robocall traffic originating from customers we resell to.

## Preventative Measures

We employ a multi-layered approach to prevent and detect illegal robocalls:

- **Real-time Traffic Monitoring:** By using tools provided by the carriers we resell for, we use call detail record tools to analyze call volume, duration, and patterns to detect anomalies indicative of illegal robocall campaigns. We also cap the duration of calls and the value of calls beyond which the customer must contact us requesting changes which we reserve the right to deny.
- **Customer Vetting:** New customers undergo a vetting process and must satisfy our requirements before we establish service. This can include submitting identification documents and a meeting to validate intended use.
- **Block List Management:** We update the databases of the carriers we resell for with numbers that should be blocked or we input them ourselves where appropriate..
- **Abuse Reporting Mechanisms:** We provide channels to our end users for reporting suspected illegal robocall activity.

## Know Your Customer/Upstream Provider (KYC/KYUP)

Our commitment to responsible telecommunications includes stringent processes for both customers. We work with our upstream providers on a continuous basis to ensure that we meet the necessary requirements.

### Customer Vetting

We ensure all customers have a legitimate need for telecommunication services and are aware of all legal and regulatory obligations.

| Vetting Requirement   | Description                                               |
|-----------------------|-----------------------------------------------------------|
| Business Registration | Verification of official business registration documents. |

| Vetting Requirement      | Description                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Compliance Agreement     | Customer signs an agreement to establish service. This can be in the form of an email.                                                                                                                            |
| Traffic Profile Analysis | Review of expected traffic volume, call patterns, and typical dialing destinations. First time calls are always emailed to us.                                                                                    |
| Customer Contact Info    | Verification of primary contact and escalation details.                                                                                                                                                           |
| Residential Contact      | Customers are registered in our database and CDR records monitored. We are notified of excessive calling patterns and calling rates are set to a threshold beyond which a request for increase must be submitted. |

## Upstream Provider Vetting

We maintain strong relationships with compliant upstream providers and regularly collaborate to ensure compliancy.

| Vetting Requirement    | Description                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| Traceback Cooperation  | We learn the provider's methods for traceback.                                                                       |
| STIR/SHAKEN Compliance | Providers share their commitment to implementing and maintaining STIR/SHAKEN or comparable anti-spoofing technology. |
| Regulatory Status      | Verification of the provider's legal and regulatory standing.                                                        |

## 24-Hour Traceback Commitment

We are committed to responding to all legitimate industry traceback requests, including those initiated by the Federal Communications Commission (FCC) and the Industry Traceback Group (ITG), within a 24-hour window.

Our designated designated point of contact is responsible for:

1. Immediate acknowledgment of the traceback request.
2. Rapid investigation and analysis of the identified call path.
3. Providing comprehensive and accurate data to the requesting entity within 24 hours of receipt.
4. Taking necessary actions (e.g., blocking or suspension) against confirmed sources of illegal traffic.

## Call Analytics and Monitoring

We leverage our provider's call analytics platforms for continuous, in-depth monitoring of network traffic.

- **Provider's Behavioral Analysis:** Algorithms monitor call attempts per hour, successful connection rates, and call duration to identify atypical, high-volume, short-duration call patterns consistent with robocalling.
- **Provider's ID Spoofing Detection:** We monitor for non-assigned or invalid Caller ID numbers, as well as repetitive, sequential dialing.
- **Provider's Reporting:** Key metrics and suspicious activity are automatically reported by our provider for immediate investigation.
- **Provider's Automated Mitigation:** Our provider's systems are configured to automatically trigger alarms and institute pre-defined mitigation actions (e.g., rate limiting) upon detection of severe, confirmed illegal traffic.