



1 Marina Park Dr.
Suite 1410
Boston, MA 02210

Robocall Mitigation Plan

Date: 12-19-2024

Introduction

Abine, Inc, DBA DeleteMe provides phone masking services using Bandwidth as our upstream communications service provider. These services are designed to protect the privacy of users while facilitating legitimate communications. Our robocall mitigation plan ensures compliance with FCC regulations and mitigates the risk of illegal robocalls originating from our network.

Know Your Customer (KYC)

Overview:

We implement robust KYC procedures to ensure that customers using our phone masking services are legitimate and comply with legal and regulatory requirements.

KYC Policies and Processes:

- 1. Customer Onboarding:**
 - All customers undergo identity verification during the onboarding process, including validation of business registration, contact information, and use-case justification.
 - Contracts include clauses prohibiting the use of services for illegal purposes, including robocalls.
 - 2. Ongoing Monitoring:**
 - Call traffic is continuously monitored to identify suspicious patterns indicative of robocall activity.
 - Customers flagged for irregular behavior are subject to investigation, and services may be suspended or terminated if violations are confirmed.
 - 3. Customer Accountability:**
 - Customers must provide valid, accurate Caller ID information.
 - Customers are required to agree to terms of service prohibiting spoofing or fraudulent practices.
-

Know Your Upstream Provider



1 Marina Park Dr.
Suite 1410
Boston, MA 02210

Overview:

We rely on Bandwidth as our trusted upstream provider for phone masking services. Bandwidth has implemented industry-leading practices for call authentication and robocall mitigation, including the STIR/SHAKEN framework.

Due Diligence on Bandwidth:

1. **STIR/SHAKEN Compliance:**
 - Bandwidth ensures compliance with STIR/SHAKEN protocols to authenticate and validate caller identities, minimizing the risk of illegal robocall origination.
 2. **Service-Level Agreements (SLAs):**
 - Our agreements with Bandwidth include commitments to prevent the origination of illegal robocalls and to cooperate in traceback investigations.
 3. **Ongoing Collaboration:**
 - We maintain regular communication with Bandwidth to stay informed about changes in regulations, best practices, and technical updates for call authentication and mitigation.
-

Traceback

Overview:

Abine Inc. DBA DeleteMe responds to all traceback requests from the FCC, law enforcement, and the registered traceback consortium and will cooperate with such entities in investigating and stopping illegal robocalls that use our service to originate calls.

Traceback Procedures:

1. **Incident Response:**
 - When notified of suspicious or illegal robocall traffic, we immediately investigate the source by analyzing call records and patterns.
 - We work closely with Bandwidth to trace the call to its origin.
 2. **Timely Reporting:**
 - We respond promptly to traceback requests from the ITG, law enforcement, or other authorized entities.
 - Relevant data, including call logs and customer account details, is shared to support investigations.
 3. **Corrective Actions:**
 - If a customer is found responsible for illegal robocalls, their account is suspended or terminated.
 - Preventive measures, such as enhanced monitoring or stricter KYC requirements, are implemented to avoid recurrence.
-



1 Marina Park Dr.
Suite 1410
Boston, MA 02210

Robocall Mitigation Program

Overview:

Our robocall mitigation program incorporates industry best practices to prevent, detect, and address illegal robocall traffic on our platform.

Core Components:

1. Call Authentication:

- Bandwidth applies STIR/SHAKEN protocols to authenticate calls and prevent spoofing.
- We ensure all calls originating from our platform carry accurate and validated caller identity information.

2. Traffic Monitoring:

- Real-time monitoring of call volumes and patterns is conducted to detect anomalies or potential robocall activity.
- Automated tools flag high-volume or repetitive calling patterns for review.

3. Enforcement Actions:

- Customers found violating our policies are subject to warnings, suspensions, or permanent account termination.
- Any suspicious traffic is reported to the ITG and relevant authorities.