

## **ReliaSys Technologies – Robocall Mitigation Program**

### **Program Overview**

ReliaSys Technologies maintains a Robocall Mitigation Program designed to prevent, detect, and mitigate the use of its voice services for illegal robocalls, fraudulent calling activity, and unlawful caller ID spoofing.

ReliaSys Technologies provides business VoIP services utilizing an underlying wholesale voice provider and network infrastructure. ReliaSys works with its underlying service provider to implement industry-standard call authentication, monitoring, and mitigation practices, including applicable STIR/SHAKEN requirements.

### **Customer Verification**

ReliaSys Technologies takes reasonable steps to verify the identity and legitimacy of customers before providing voice services. Customer information is maintained as part of the normal account onboarding and service provisioning process.

Customers are expected to provide accurate information and to use ReliaSys voice services in compliance with applicable federal and state laws, FCC regulations, and the terms of their service agreement.

### **Caller ID and Number Usage**

ReliaSys Technologies prohibits customers from using its voice services to unlawfully spoof telephone numbers or misrepresent the originating identity of a call.

Customers are expected to use telephone numbers assigned to them or otherwise authorized for their use. ReliaSys may investigate reported instances of suspected unlawful caller ID spoofing or misuse of telephone numbers.

### **STIR/SHAKEN**

Where applicable, ReliaSys Technologies utilizes the STIR/SHAKEN framework through its underlying voice service provider to authenticate caller ID information and support the identification of legitimate originating calls.

The appropriate level of caller ID attestation is determined based on the information available to the originating service provider and the customer's authorization to use the telephone number presented on the call.

ReliaSys Technologies works with its underlying voice provider to support compliance with applicable STIR/SHAKEN requirements.

## **Call Traffic Monitoring and Detection**

ReliaSys Technologies may monitor voice traffic and customer usage for activity that appears inconsistent with normal business calling patterns or that may indicate fraudulent, abusive, or unlawful use of the service.

Potential indicators may include, but are not limited to:

- Unusually high outbound call volumes
- Rapid increases in call activity
- Large numbers of short-duration calls
- Repeated calls to large numbers of unrelated destinations
- Suspected caller ID spoofing
- Customer complaints or reports of abusive calling activity
- Other activity identified as potentially fraudulent or unlawful

Where suspicious activity is identified, ReliaSys may investigate the activity and take appropriate action.

## **Mitigation and Enforcement**

When ReliaSys Technologies identifies suspected illegal robocalling, spoofing, fraud, or other abusive use of its voice services, it may take appropriate mitigation measures, including:

- Contacting the customer for additional information
- Requesting verification of calling activity
- Temporarily restricting or suspending calling activity
- Blocking specific traffic or telephone numbers
- Suspending or terminating the customer's service
- Escalating the matter to the underlying voice service provider
- Cooperating with appropriate regulatory authorities or law enforcement when required

The specific action taken will depend on the nature and severity of the activity.

## **Customer Responsibilities**

ReliaSys Technologies requires customers to use its voice services in accordance with applicable laws, regulations, and service agreements.

Customers are responsible for ensuring that their calling practices are lawful and that any automated calling, prerecorded messaging, caller ID information, and telephone numbers used by the customer comply with applicable requirements.

ReliaSys Technologies may take action when a customer is determined to be using its services for unlawful or abusive calling activity.

### **Cooperation With Underlying Voice Provider**

Because ReliaSys Technologies utilizes an underlying wholesale voice provider for portions of its VoIP infrastructure, ReliaSys works with that provider regarding applicable call authentication, traceback, robocall mitigation, and related regulatory requirements.

Where appropriate, ReliaSys will cooperate with its underlying provider and authorized regulatory or law-enforcement entities in investigating suspected illegal robocalling or spoofing activity.

### **Program Maintenance**

ReliaSys Technologies will periodically review and update its Robocall Mitigation Program as necessary to reflect changes in its services, network architecture, regulatory requirements, and industry practices.

ReliaSys Technologies is committed to maintaining reasonable procedures to reduce the risk that its voice services are used to originate or facilitate illegal robocalls and unlawful caller ID spoofing.

### **ReliaSys Technologies**

**Program:** Robocall Mitigation Program

**Effective Date:** August 17, 2026

**Last Reviewed:** August 17, 2026