

RYSTEC

Robocall Mitigation Plan



Pursuant to 47 C.F.R. § 64.6305 Rystec Inc submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Rystec Inc hereinafter also referred to as “Rystec” or “the company”) has in place to mitigate illegal robocalls. The company may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, its capabilities and its needs.

Rystec has enforceable terms of use and/or an acceptable use policy noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. The policy states that at any time for any reason without notice, we can suspend or terminate any Service(s) for the following reason(s) that warrant such action:

- (1) if you violate or breach or abuse the Company Terms and Conditions;
- (2) if a law enforcement request or other government order is in effect and you reject or fail to respond;
- (3) if you harass, offend, or threaten our employees;
- (4) if you use Services to violate any state or federal laws or laws of any other competent jurisdiction in any manner;
- (5) failure to pay for Service(s), submission of insufficient funds or the dispute of credit card charges;
- (6) you provide false or inaccurate information upon the activation of your account;
- (7) you violate our Acceptable Use Policy ("AUP");
- (8) "Spoofing" or falsely (or deceptively) displaying outbound Caller ID (CID) to any payment numbers, utility company numbers, police numbers, government agency numbers, or any other emergency service number. We may terminate any or all of the Services at any time for any reason upon notice to you. The action we take upon any of these matters is done to protect our interests, the interests of our customers, and other parties.

Rystec confirms that the upstream providers have a certification in the Robocall Mitigation Database. The company will not accept voice traffic from an unregistered provider. The Company has been

informed of the upstream providers “Know-Your-Customer” guidelines and have provided them with the necessary KYC documentation they’ve requested that the company completes.

Rystec follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that the company has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

Rystec also validates, when possible, that the entity has a legitimate right to use its asserted calling numbers. The Company uses this information to support the attestation level it assigns to calls that it originates for that customer.

Rystec contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service.

Rystec requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.

Prior to installing services for new customers, the company takes the following measures to weed out end users that could potentially generate robocall traffic:

The Company uses a KYCs to confirm the following information for its customers:

- Customer’s identity
- Customer’s right to use the telephone number presented on calls
- Service Address
- Credit History

When the customer is a business, Rystec also requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

Rystec uses proprietary call analytics software to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. The Company will immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If the Company determines that the traffic was likely unlawful, then the

company will warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then the company will terminate their service.

Rystec will comply fully with all conditions set forth in the FCC'S 2024 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

Rystec has designated an individual as a dedicated point of contact for addressing traceback requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>. The Company will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.

If a pattern of questionable activity is detected Rystec Inc will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Requests from the ITG must be submitted in writing and include the following information:

Phone Number in Question:

Phone Number Dialed:

Date / Time Stamp:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

Rystec will provide valid law enforcement and regulatory agencies with the relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated Robocall Mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. The company will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. The company will cooperate fully with such entities in investigating and stopping any illegal robocallers that use the Company's service to originate, carry, or process illegal robocalls.

Requests from the valid agency must be submitted in writing and include the following information:

Law Enforcement Agency Name:

Agency Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

Rystec performs the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. The Company has not had any agency action or investigation due to suspected unlawful robocalling or investigations.

Rystec is not subject to any Commission, Law Enforcement, or Regulatory Agency Action or investigation due to suspected unlawful robocalling or spoofing. Rystec has not had any complaints or tracebacks.

Rystec does not wish to publicize any private and/or classified information that has the potential to expose the Company to fraud and/or anti-competitive actions. Therefore, the Company will submit a redacted version for the public site and requests that the FCC keep the unredacted version CONFIDENTIAL.