

ROBOCALL MITIGATION PROGRAM

Bigly Sales, Inc. & affiliates (“Bigly Sales”)

This Robocall Mitigation Program (RMP) describes with particularity the steps Bigly Sales takes to avoid the origination, carrying, or processing of illegal robocall traffic. Bigly Sales is a United States-based company offering a suite of next-generation communications services powered by Artificial Intelligence (AI). The company will be offering voice services soon. Bigly Sales does *not* originate wholesale or international traffic, and is *not* an intermediate provider or gateway provider. Bigly Sales does *not* originate high-volume, short-duration, or auto-dialer traffic. Bigly Sales does *not* receive intermediate traffic from upstream providers. Bigly Sales has *not* been prohibited from filing in the Robocall Mitigation Database pursuant to law enforcement action. This RMP will be updated as regulations and business practices evolve.

Tracebacks/Law Enforcement Inquiries

Bigly Sales commits to respond within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. Bigly Sales’s contact for tracebacks/law enforcement inquiries (and employee responsible for addressing robocall mitigation issues) is:

- Contact Name: Thomsas Ryan
- Phone: (561) 254-4007
- Email: tom@biglysales.com cc: pphipps@qsiconsulting.com
- Address: 11197 Blackhawk Blvd. Davie, FL 33328

Call Analytics

Bigly Sales monitors and analyzes voice traffic originated on its network, and utilizes call analytics systems to identify and block illegal traffic. Traffic is analyzed to identify high-volume, short-duration, or other traffic patterns indicative of robocalling campaigns.

Bigly Sales intends to use a third-party vendor TransNexus for its STIR/SHAKEN caller ID authentication solution. This deployment will allow the company to comply with STIR/SHAKEN implementation requirements, and also offers a portfolio of tools enabling analytics, telecom fraud prevention, and robocall prevention.

Bigly Sales investigates suspicious call patterns. If a pattern consistent with illegal robocalls or other fraudulent traffic is identified, Bigly Sales will identify the party that is using its network in such manner and take appropriate action to stop processing the traffic. Appropriate action may include suspension of service, blocking, or notifying law enforcement.

Acceptable Use Policy

Bigly Sales voice service customers must adhere to the company’s Acceptable Use Policy (AUP). Bigly Sales’s AUP identifies illegal and fraudulent activity as a prohibited use of the company’s service, and authorizes the company to take immediate action including service suspension and termination (with or without written notice) to address such traffic.

STIR/SHAKEN Implementation

Bigly Sales will implement STIR/SHAKEN (S/S) caller ID authentication and verification via third-party vendor. Calls originated by Bigly Sales will be signed with a S/S token reflecting Bigly Sales's credentials.

Know-Your-Customer

Bigly Sales performs due diligence to know its customers and takes affirmative measures to prevent new and renewing customers from originating illegal calls.

During customer onboarding, Bigly Sales collects specific information about its customers to ensure their legitimacy via a service application process. That information includes: Contact Person, Address details, Contact email, telephone number, and Credit Card. Bigly Sales checks this information as part of our Customer Verification Process.