

Robocall Mitigation Program Description

Filer: Brabo BV

FRN: 0038256319

Provider Type: Voice Service Provider / VoIP Provider

The filer has implemented a robocall mitigation program consistent with 47 CFR § 64.6305(a). All calls originated by the filer on its network are subject to this robocall mitigation program. The filer has taken reasonable steps to avoid originating illegal robocall traffic and commits to respond fully and 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 illegal robocallers that use its service to originate calls.

The filer does not control the network infrastructure necessary to implement STIR/SHAKEN. Specifically, the filer does not control the softswitch and session border controller (SBC) layer used to authenticate outbound calls and therefore does not control the underlying network elements on which STIR/SHAKEN authentication would need to be deployed. The filer relies on third-party underlying network providers for call-processing and outbound call authentication functionality. Because the filer does not operate or control the softswitch/SBC layer required to authenticate outbound calls, the filer is unable to implement STIR/SHAKEN on any portion of its network at this time. This basis is consistent with the Commission's recognition that some providers lack control over the network infrastructure necessary to implement STIR/SHAKEN, and this explanation is provided consistent with 47 CFR § 64.6305(d)(2)(i).

To mitigate illegal robocall traffic, the filer uses reasonable procedures to review and monitor originating traffic for suspicious patterns, unusual volumes, invalid or unverifiable caller identification information, short-duration/high-volume traffic, and other indicia of potentially unlawful robocalling. When suspicious activity is identified, the filer investigates the traffic, may request supporting information from the customer or upstream service relationship, and may restrict, suspend, or terminate service where warranted.

The filer maintains know-your-customer procedures designed to understand who its customers are and the nature of their expected use of service. Before or during onboarding, the filer collects and reviews identifying information such as customer name, business identity, contact information, billing information, and the expected use case for the service. The filer may also request additional documentation when warranted by the nature of the customer, traffic profile, or service requested. The filer reviews customer activity for consistency with the stated use of service and investigates discrepancies or suspicious conduct. The filer also maintains procedures to know its underlying or upstream provider relationships as applicable to its operations. The filer describes these procedures to

comply with the FCC's robocall mitigation plan requirements regarding customer and provider due diligence.

The filer does not currently use a separate data analytics system as part of its robocall mitigation program. The filer instead relies on operational monitoring, customer due diligence, traffic review, traceback response procedures, and enforcement actions where warranted.

The filer maintains records sufficient to support investigations of suspicious traffic and to respond to traceback requests. The filer will cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocall traffic and will update this robocall mitigation description as required if material information changes.

Contact for Robocall Mitigation Issues:

Name: R Schick

Title: Director

Business Address: Boomgaardstr 229 2018 Antwerpen Belgium

Telephone: 32-3-547-0765

Email: twirl-kitty-jersey@duck.com