

Our company provides hosted voice services to business customers as a reseller and does not control the underlying network infrastructure used to originate calls. We maintain a robocall mitigation program consistent with 47 CFR § 64.6305(a) and take reasonable steps to avoid originating or carrying illegal robocall traffic.

As part of our mitigation program, we perform customer vetting prior to service activation, including verification of customer identity, business information, and billing details. Customers are required to agree to acceptable use policies that expressly prohibit illegal robocalling, spoofing, and abusive calling practices.

We monitor customer traffic patterns in coordination with our upstream provider, Viirtue, and promptly investigate complaints, alerts, or reports of suspected illegal robocall activity. When potential violations are identified, we take appropriate enforcement actions, which may include warning notices, service suspension, or termination.

STIR/SHAKEN authentication and call signing are implemented by our upstream provider, Viirtue, which controls the underlying network infrastructure. While we do not implement STIR/SHAKEN directly, we rely on Viirtue's network-level implementation and incorporate those protections into our overall robocall mitigation efforts.

We commit to responding fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium, and to cooperate fully in investigations to identify and stop illegal robocall traffic.