VOIP Essential Robocall Mitigation Review Policies and Procedures

Effective: July 17, 2023

VoIP Essential, in connection with its provision of Telephony Services, maintains these written policies, practices, and procedures to monitor, review, and analyze call traffic, and to use commercially reasonably efforts to identify, mitigate, and block unlawful Robocalls, or investigate patterns consistent therewith, including, without limitation, the consideration of call duration, call volume, calls per second, and, if available to VoIP Essential, the location of the calls' origination or U.S. point of entry.

In furtherance of this commitment, VoIP Essential undertakes the following actions:

Before onboarding a new end user or carrier customer, VoIP Essential will comply with applicable federal law, including 47 C.F.R. § 64.1200(n)(3), and the company's Consent Decree with the State of Indiana, to know its originating end user customers and wholesale customers. To implement that so-called "KYC," or Know Your Customer, duty, VoIP Essential requires all new and renewing wholesale customers to complete the KYC form attached as **Exhibit A**. End users are required to fill out the data solicited on the VoIP Essential website: https://dashboard.voipessential.com/customer/register.

Responsible company personnel then review each prospective customer's KYC submission, and if and as necessary, consult commercially reasonable and available sources to corroborate the information provided by the prospective customer and to follow-up with the customer to address any questions or concerns raised by the KYC process.

Prospective carrier customers' FCC 499 Filer ID and Robocall Mitigation Database status will be checked at these or any successor URLs established by the Federal Communications Commission for such verification purposes:

https://apps.fcc.gov/cgb/form499/499a.cfm

https://fccprod.servicenowservices.com/rmd?id=rmd_listings

Further, a prospective carrier customer's status as an authorized voice service provider will be verified via the then-current Policy Administrator's website, which is currently located at:

https://authenticate.iconectiv.com/authorized-service-providers-authenticate

VoIP Essential will likewise maintain in good standing its STIR-SHAKEN compliance with the Policy Administrator and Certificate Authority and authenticate calls in accordance with applicable law and ATIS standards.

VoIP Essential further commits to timely responding to all tracebacks from the ITG or any successor authority as designated by the FTC, as well as all lawful requests from state and federal law enforcement agencies. Once these inquiries put VoIP Essential on notice of traffic that is highly likely to be illegal, VoIP Essential takes appropriate action, such as suspending and/or terminating a VoIP Essential end user's account for the end user responsible for such traffic, absent significant mitigating circumstances revealed during the investigation; and, in the case of carrier customers, securing ample assurances that the responsible source of the traffic has been terminated from their network availability and thus no such further traffic should ingress onto VoIP Essential's network or, failing such assurances, full termination of that wholesale customer's account.

In addition to the foregoing KYC and robocall mitigation practices, VoIP Essential also undertakes various commercially reasonable efforts to identify and mitigate unlawful Robocalls, as defined in the Consent Decree and applicable law. For instance, VoIP Essential:

- Blocks traffic from numbers identified on a commercially available DNO (Do Not Originate) list, currently provided via SOMOS;
- Uses an innovative robocall-mitigation tool, RoboGuard, that employs Media IP-based blocking analytics rather than the traditional, inferior ANI-based blocking provided by other commercially available sources to block all calls from Media IP addresses that the service provider has deemed to be highly likely to be scam, fraudulent, already the subject of tracebacks or FCC cease-and-desist published notices, as well as the target of CLEC complaints.
- Tracks and analyzes periodic (monthly, and/or on an as-needed basis) reports that identify various call criteria, including, without limitation, total minutes of use, calls per second, average call duration, answer seizure ratio (in and out), call-completion ratio, blocked CID and Media IP counts, and SIP code-related data, and then analyzes those reports to identify anomalous traffic patterns that warrant further investigation.

VoIP Essential Personnel who support these business and compliance objectives are an integral part of the company's compliance success. They are expected to read and implement these Policies and Procedures, and to bring any questions or concerns they may have about them to their superiors.