

SIP VoIP, LLC

Robocall Mitigation Program

Pursuant to the rules of the Federal Communications Commission, including 47 CFR Section 64.6305 (Robocall Mitigation and Certification), SIP VoIP, LLC has implemented the following Robocall Mitigation Program.

Role in the Call Path

SIP VoIP, LLC operates as a Non-Gateway Intermediate Provider with a STIR/SHAKEN implementation obligation. SIP VoIP, LLC provides wholesale voice transit services, carrying and processing voice traffic between originating and terminating providers. SIP VoIP, LLC neither originates nor terminates calls to end users.

Operating Company Number (OCN): 923K

Business Address: 200 Continental Drive, Suite 401, Newark, DE 19713

Preventing Illegal Traffic

SIP VoIP, LLC is committed to compliance with the Telephone Consumer Protection Act (TCPA), the TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence) and the rules of the Federal Communications Commission pertaining to the prevention of illegal robocalling, fraudulent calling and other illegal use of its network. To that end, SIP VoIP, LLC requires each customer to provide information that enables SIP VoIP, LLC to “know its customers” and properly conduct the necessary due diligence to comply with the law and protect its network.

Due Diligence

SIP VoIP, LLC conducts due diligence with respect to each customer, both those existing prior to the date of this Robocall Mitigation Program and new customers, that is designed to ensure the customer will not originate illegal robocall traffic, or other illegal traffic, and includes:

- The proper formation and good standing of the customer entity, including whether it is foreign or domestic
- A description of the customer’s business, including whether the customer uses any auto-dialing technology
- The physical location of the customer’s business
- A review of the customer’s website
- Obtaining the customer’s current and prior IP addresses for review, including whether they are foreign
- Determining the customer’s ownership and management, and
- Ascertaining whether there is any litigation pertaining to the customer or its principals.

Wholesale Customers and Know-Your-Upstream-Provider Procedures

SIP VoIP, LLC will only accept traffic for termination from carrier customers that have an active registration in the Robocall Mitigation Database. SIP VoIP, LLC verifies each upstream provider's FRN, RMD registration status, and 499 Filer ID against public FCC databases before activating any account. SIP VoIP, LLC will review the customer's Robocall Mitigation Program on file with the FCC.

For any wholesale customers, SIP VoIP, LLC also investigates:

- Whether the customer has been determined by US Telecom's Industry Traceback Group to be a "Non-Cooperative Voice Service Provider"
- Whether the customer has been blocked from another voice service provider's network after being determined to have violated laws or regulations pertaining to illegal robocalling, fraudulent calling, illegal telemarketing practices or otherwise has been determined to be a "bad-actor upstream voice service provider"
- Whether the customer has implemented the STIR/SHAKEN Authentication Framework
- Obtaining assurance that the wholesale customer will promptly provide the identity of its customer or end user that was the source of reportedly illegal call traffic that the customer routed to SIP VoIP, LLC
- Whether the customer is registered with the Universal Service Administrative Company and has obtained a Form 499 Filer ID.
- Whether the customer or any controlling person has been subject to an adverse judgment or government enforcement action involving telecom services.

Contractual Provisions

SIP VoIP, LLC requires all customers to agree to terms and conditions at onboarding that include the following:

- A certification that the customer does not generate or knowingly pass illegal or unwanted call traffic.
- A prohibition against removing, altering, or otherwise manipulating ANI, CPN, or other originating party information, consistent with the Truth in Caller ID Act.
- A commitment to respond promptly to all traceback requests and to act on any illegal traffic on its network.
- A requirement that the customer holds its own customers to the same compliance standards.
- A commitment to notify \${co} of any material change to the information provided at onboarding within 30 days, and consent to annual re-verification of FCC credentials.

SIP VoIP, LLC reserves the right to suspend or terminate service immediately, without prior notice, if any customer is found to be in violation of these terms. Illegal robocalling and the knowing transmission of illegal traffic constitute a material breach of the customer agreement.

Autodialed Call Traffic

For any customer that SIP VoIP, LLC determines will transit autodialed call traffic, SIP VoIP, LLC will not receive any call traffic from such customer until the customer assures SIP VoIP, LLC it has taken reasonable steps to screen the legitimacy of the proposed autodialed call

traffic, including, without limitation, obtaining, verifying and providing to SIP VoIP, LLC the following:

- the name, point of contact and contact information for the entity on whose behalf the originating caller is proposing to make the autodialed calls
- a description and sample recording or transcript (in English) of the proposed autodialed calls
- a list of the proposed ANIs to be autodialed
- the originating caller's subscription number to the Federal Do-Not-Call Database and any applicable state Do-Not-Call Databases
- a statement as to whether the originating caller would be undertaking the proposed calls with the consent of the proposed autodialed call recipients and, if so, a description and sample evidence of how such consent was obtained
- the proposed calls per second for the relevant autodialed call campaign
- the proposed dates of the relevant autodialed call campaign.

STIR/SHAKEN Implementation

SIP VoIP, LLC has fully implemented the STIR/SHAKEN authentication framework across its network consistent with 47 C.F.R. § 64.6302. As a Non-Gateway Intermediate Provider:

- SIP VoIP, LLC passes authenticated caller identification information it receives with a SIP call unaltered to the next provider in the call path, in accordance with 47 C.F.R. § 64.6302(a).
- SIP VoIP, LLC authenticates caller identification information for all SIP calls it receives directly from an originating provider for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, in accordance with 47 C.F.R. § 64.6302(d).

SIP VoIP, LLC has obtained its own SPC token from the STIR/SHAKEN Policy Administrator and uses that token to generate a certificate with an approved Certificate Authority. Where authentication is required, calls are signed using SIP VoIP, LLC's own digital certificate.

Call Blocking and Analytics

SIP VoIP, LLC will block services to a customer if it determines that the customer is using the services for illegal robocalling.

SIP VoIP, LLC uses Fraud Central software to identify and block illegal robocall traffic. Fraud Central provides traffic monitoring capabilities that assist SIP VoIP, LLC in detecting suspicious calling patterns and anomalous traffic behavior on its network.

Do-Not-Originate List

All customers bear full responsibility for ensuring that traffic sent to SIP VoIP, LLC does not include calls originating from numbers on the Do-Not-Originate (DNO) list, including numbers that are invalid, unallocated, or otherwise designated as inbound-only. Upon customer request and with the customer's consent, SIP VoIP, LLC may enable SOMOS DNO list filtering on its softswitch on the customer's behalf as a courtesy. This filtering is provided on a best-efforts basis and SIP VoIP, LLC shall not be liable if any DNO-listed calls still pass through the

network. Regardless of whether SIP VoIP, LLC applies DNO filtering, the customer remains solely responsible for ensuring that no DNO-listed numbers are originated on traffic sent to SIP VoIP, LLC.

Do-Not-Call Compliance

All customers bear full responsibility for Do-Not-Call compliance on all traffic sent to SIP VoIP, LLC. Upon customer request and with the customer's consent, SIP VoIP, LLC may apply DNC filtering at the network level on the customer's behalf as a courtesy. This filtering is provided on a best-efforts basis and SIP VoIP, LLC shall not be liable if any DNC-listed calls still pass through the network. Regardless of whether SIP VoIP, LLC applies DNC filtering, the customer remains solely responsible for ensuring compliance with all applicable federal and state Do-Not-Call laws and regulations.

Enforcement Actions

When suspected illegal robocall activity is identified, SIP VoIP, LLC may take one or more of the following actions:

- Immediate investigation of the traffic source.
- Temporary suspension or permanent termination of service without prior notice.
- Blocking of specific calling numbers, prefixes, or customers.
- Notification to upstream or downstream providers.
- Cooperation with the FCC, law enforcement, or industry traceback groups.

Enforcement actions are documented and retained in accordance with internal compliance procedures.

Traceback Requests

SIP VoIP, LLC 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 from using its services to carry or process calls.

Updating RMD Submission

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5), and (f)(5), SIP VoIP, LLC will update its submission in the Robocall Mitigation Database within 10 business days of any change to the applicable information it must provide. SIP VoIP, LLC certifies annually, on or before March 1, that any information submitted to the Robocall Mitigation Database is true and correct, in accordance with 47 C.F.R. § 64.6305(h).