

Robocall Mitigation Plan

Company Name: TeleVoip ESC

Company Address The Corporation Trust Center
1209 Orang
Wilmington, DE 19801

Company Phone #: 561-922-9585

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires voice service providers to implement STIR/SHAKEN authentication on Session Initiation Protocol (“SIP”) traffic on carrier networks as well as to implement a Robocall Mitigation Plan (“RMP”) covering non-SIP Time Division Multiplexing (“TDM”) traffic.

TeleVoip ESC operates as a provider of “voice service” as set forth in Section 64.6300(l) of the Federal Communications Commission’s (“Commission”) rules, 47 C.F.R. §64.6300(l). TeleVoip ESC has a mix of TDM and SIP traffic on its network. TeleVoip ESC certifies that all SIP voice traffic originating on its network is authenticated under the STIR/SHAKEN authentication framework, pursuant to 47 CFR § 64.6301(a). For all voice traffic, including traffic originating on underlying networks over which TeleVoip ESC lacks control of the network infrastructure necessary to implement the STIR/SHAKEN authentication framework, TeleVoip ESC internally performs subscriber vetting, telephone number validation, and network traffic monitoring, analysis, and investigation as set forth below, and adopts the North America Numbering Council Call Authentication Trust Anchor Working Group’s *Best Practices for the Implementation of Call Authentication Frameworks* into this RMP.

The Commission grants TeleVoip ESC a continuing extension for implementing STIR/SHAKEN authentication for TDM traffic provided TeleVoip ESC comply with Commission rules applicable to such portions of the TeleVoip ESC network subject to extension. To this end,

TeleVoip ESC hereby submits this RMP to the Robocall Mitigation Database describing and confirming practices, policies, and procedures to mitigate unlawful robocalling, which include the following:

- (1) TeleVoip ESC specific reasonable steps to avoid originating illegal robocall traffic as part of this RMP;
- (2) TeleVoip ESC's commitment to respond fully and timely to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers using TeleVoip ESC's service to originate calls; and,
- (3) TeleVoip ESC's intent to participate in industry tradeshow, groups, or consortiums, working to strengthen efforts to combat unlawful robocalling, and additional call verification and authentication solutions.

EFFORTS TO AVOID ORIGINATING ILLEGAL

ROBOCALLS AS PART OF THE RMP

TeleVoip ESC offers a digital, cloud-based, high-performance network SIP solution for customers. TeleVoip ESC's meaningful investments in the digital network includes software technology, equipment and resources to combat illegal robocalls as part of this RMP consistent the most rigorous regulatory and compliance requirements.

As part of TeleVoip ESC's RMP, TeleVoip ESC provides the following affirmative, effective measures to help minimize the impact of illegal or unwanted robocalls, and prevent new and renewing customers from using TeleVoip ESC to originate illegal calls:

- **Customer Vetting** TeleVoip ESC maintains a comprehensive customer vetting process to meet "Know Your Customer" ("KYC") obligations. This KYC vetting process provides an understanding of the nature of activities for any new

and existing customers. Prior to installing services for new customers, in an effort to screen out end users potentially generating robocall traffic, TeleVoip ESC confirms the following information:

- Customer's identity
- Customer's right to use the telephone number presented on calls
- Service Address
- Credit History

When dealing with a business end user customer, TeleVoip ESC also requires business organizational/incorporation documents. Moreover, TeleVoip ESC conducts reputational verification in addition confirming the validity of customer business compliance with the law. Identifying and understanding customers through this KYC vetting process diminishes the opportunity to use TeleVoip ESC's network for spoofed or illegal traffic.

- **Customer Contracts/General Terms and Conditions.** TeleVoip ESC maintains enforceable terms of use within end user customer contracts. The terms and conditions define the circumstances by which TeleVoip ESC will deny, suspend, or terminate service to a customer. TeleVoip ESC prohibits customers from originating fraudulent calling using any fraudulent means, devices, or technologies. TeleVoip ESC's end user customer Terms and Conditions permit TeleVoip ESC, without notice, to discontinue, block or suspend services if necessary to prevent fraud, scams, tampering, schemes, false or invalid numbers. As stated further below, TeleVoip ESC shall block or suspend the service of any customers originating unlawful robocalls through TeleVoip ESC. TeleVoip's RMP includes an increasing investment in resources over time to further strengthen adherence to compliance to all such

requirements by customers.

- **Acceptable Use Policy.** In addition to Terms and Conditions of contract, TeleVoip ESC also obligates end user customers through the Acceptable Use Policy (“AUP”). The AUP prohibits customers from utilizing the service for any illegal, fraudulent, objectionable and/or unauthorized manner, reserving the sole and absolute right to deny, restrict or immediately suspend or terminate service if the use of the service by the customer, or anyone having access to or using the service, either violates the AUP or includes unlawful conduct.
- **Automatic Number Identification Management:** TeleVoip ESC shall block originating telephone numbers if identified based upon patterns of activity.
- **Proactive Blocking.** TeleVoip ESC requests underlying carriers to block calls from phone numbers on Do-Not-Originate lists published by US Telecom and Neustar.
- **Underlying Network Provider.** TeleVoip ESC works with underlying providers and supports the benefit of deploying systems to detect potential robocall activity relying upon statistics such as average call duration, ASR, and call count carrier/consumer reports.
- **Traffic Reports and Industry Information.** TeleVoip ESC established methods and procedures to monitor its network and detect / prevent fraudulent activity. TeleVoip ESC uses call authentication, call labeling, and call blocking services to protect its networks and consumers from harmful calls. As stated above, TeleVoip ESC also uses software to monitor its network’s daily usage and has established methods and procedures in place to address issues immediately once identified. Reports generated by Call Detail Record and pattern trends, fraud information sharing through industry organizations, and

third-party notifications and complaints, may identify potential unlawful robocalling. Although no evidence exists suggesting TeleVoip ESC in any way originates illegal robocall campaigns, in any instance where unlawful calling is identified, TeleVoip ESC maintains contractual ability to take any action it deems necessary to eliminate the fraudulent activity.

ONGOING COMPLIANCE

TeleVoip ESC will continue to fully comply with all conditions set forth in the Commission's Orders mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

Should TeleVoip ESC detect a pattern of questionable activity, TeleVoip ESC will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated. Requests from the Industry Traceback Group (ITG) must be submitted in writing and include the following information:

Company Name:

Company Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

TeleVoip ESC will cooperate with state and federal regulators to prevent any and all illegal robocalls. Requests from the valid agency must be submitted in writing and include the following information:

Law Enforcement Agency Name:

Agency Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

TeleVoip ESC will provide valid law enforcement and regulatory agencies with the relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities and implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

COMPANY INFORMATION AND POINT OF CONTACT

TeleVoip ESC designates the following individual as a dedicated point of contact for addressing traceback requests:

Name: Inam Haq

Title: Director

Department: Executive

Business Address: The Corporation Trust Centre, 1209 Orang, Wilmington,
DE 19801

Telephone Number: (561) 922-9585

Email Address: inam@televoip.us

TeleVoip ESC provided ITG with the contact information and business hours for those individuals. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>.
TeleVoip ESC will respond promptly to inquiries from the Industry ITG.

ONGOING ROBOCALL MITIGATION

TeleVoip ESC anticipates that this RMP will evolve as TeleVoip ESC and underlying carriers enhance practices and procedures, and as the Trust Anchor and industry generally gain experience in caller ID authentication protocols.

CERTIFICATION

I, Inam Haq, Director of TeleVoip ESC, do hereby certify, under penalty of perjury, the following:

- a. TeleVoip ESC lacks control of the network infrastructure necessary to implement the STIR/SHAKEN authentication framework on TDM and SIP calling.
- b. TeleVoip ESC business name and primary address follows:

TeleVoip ESC

The Corporation Trust Center

1209 Orang

Wilmington, DE 19801
- c. Entities owning 10% or more of TeleVoip ESC include: none. TeleVoip ESC has no subsidiaries or affiliates.
- d. TeleVoip ESC has had no licenses revoked by the Commission and has not been subject to enforcement action by the Commission.
- e. TeleVoip ESC does not operate under any other business name.
- f. TeleVoip ESC has not previously used or operated under any other business name.
- g. The name, title, department, business address, telephone number and email address of the individual responsible for addressing robocall-related issues for the Robocall Mitigation Plan follows:

Name: Inam Haq

Title: Director

Department: Executive

Business Address: The Corporation Trust Center, 1209 Orang, Wilmington, DE
190801

Telephone Number: (561) 922-9585

Email Address: inam@televoip.us

- h. TeleVoip ESC's role in the call chain is that of a voice service provider without a STIR/SHAKEN implementation obligation to serve end users.
- i. TeleVoip ESC has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. TeleVoip ESC is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. TeleVoip ESC OCN is 438K



Inam Haq, Director