

S-NET INC. ROBOCALL MITIGATION PLAN

Pursuant to 47 C.F.R. § 64.6305, S-Net Communications, Inc. (“S-Net”, “the Company”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls.

This report describes the practices and procedures which S-Net has in place to protect its business customers and to mitigate illegal robocalls. S-Net may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

S-Net has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, and none of its prior certifications have been removed from the Database by the Commission.

S-Net has not been, at any time in the prior two years, the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with the Company’s findings of actual or suspected wrongdoing due to it transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

S-Net, Inc. is a Managed Service Provider “MSP” focused on supporting businesses. As an MSP the Company provides multiple IT products and services to its business customers along with adjunct telecommunications products and services.

S-Net Communications, Inc. is registered with the Federal Communications Commission (“FCC”) and holds the 499 Filer ID number of 828599. The Company’s FRN/CORESID Number is 0020419545.

THE COMPANIES PRIMARY PLACE OF BUSINESS

1100 E Woodfield Road, Suite 101, Schaumburg, IL 60173

Phone: 847-321-1500

Website: www.snetconnect.com

General Email: support@snetconnect.com

Mailing Address:

1100 E Woodfield Road

Suite 101

Schaumburg, IL 60173

LEADERS OF THE COMPANY ARE:

CEO

Name: Alex Fayn

Address: 1100 E Woodfield Road, Suite 101

City, State, Zip: Schaumburg, IL 60173

Direct Dial: 773-321-1515
Email: afayn@snetconnect.com

CTO

Name: Eugene Likhovid
Address: 1100 E Woodfield Road, Suite 101
City, State, Zip: Schaumburg, IL 60173
Direct Dial: 847-687-2318
Email: elikhovid@snetconnect.com

DESIGNATED RMD CONTACT

Name: Kim Zacharkiewicz
Address: 1100 E Woodfield Road, Suite 101
City, State, Zip: Schaumburg, IL 60173
Direct Dial: 773-321-1528
Email: kzacharkiewicz@snetconnect.com

STIRSHAKEN COMPLIANCE

S-NET Communications Inc. (S-NET) has fully implemented the STIR/SHAKEN authentication framework across its entire network, and all calls it originates are compliant with § 64.6301(a)(1) and: S-Net Utilizes Neustar/TransUnion for its STI-AS and STI-VS services. S-NET has implemented a robocall mitigation program by sending valid CallerID in the SIP From Header and/or the P-Asserted Identity header of every SIP INVITE message that originates from its network.

S-NET is in full control of all CallerID assignments and does not allow a call to originate without a valid CallerID.

These messages are sent to S-NET's upstream trunk carriers: Telnyx, LLC, Bandwidth Inc., Inteliquent Inc., and VoIP Innovations Inc.

S-NET also utilizes Neustar's/TransUnion robocall mitigation services. This service scans all TNs coming in, labels them appropriately, and blocks the ones that have a known history of fraudulent activity.

KNOW YOUR CUSTOMER

S-Net has a rigorous KYC policy for the in order to support the Business Customers that it resells services to. S-Net has an in-depth presales process where representatives work with the prospect or customer to understand all the unique factors of the Customer's business. The objective of this is two fold: a. to get to know the customer; and b. to provide the best possible service to the customer by fully understanding all facets of their business.

S-Net performs a thorough reputation check and credit check on each of its customers and verifies the following information: legal business name, legal form of business, federal tax ID, nature of the business, primary contact person, and service address.

Not only does S-Net have a rigorous intake and Onboarding process where it secures extensive information for Customers but all relationships between S-Net and customers are governed by an MSA. The MSA specifically states the business customer is not able to resell any services that are sold to the customer by S-Net.

S-Net conducts due diligence on new and renewing customers, confirming the customer's identity and the customer's service address for all customers.

- S-Net verifies customer's business reputation prior to providing service.
- S-Net verifies customer information when contracts are renewed or services are added.
- S-Net verifies the customer's identity and their right to use the telephone number presented on calls.
- S-Net has a specific Acceptable Use Policy ("AUP") which defines all Company policies regarding the circumstances by which S-Net will deny, suspend or terminate service to a customer.

Additionally, as mentioned above all Company customers are required to agree to, and; are contractually bound by S-Net strict policies, contractual terms and conditions and a Company Acceptable Use Policy ("AUP") prohibiting the act of fraudulent voice activity as a condition of doing business with S-Net.

If any customer is found to be in possible and/or or actual violation of any Company policy as it relates to suspicious traffic and/or possible fraud, the Company has the right to immediately halt, cease and/or suspend the customers account or associated telephone numbers.

MEASURES TO PREVENT OR AVOID ILLEGAL ROBOCALLS

- S-Net has in place an enforceable terms of use and/or an acceptable use policy. S-Net also has in place policies designed to detect and prevent fraudulent traffic on its network.
- S-Net uses analytics technologies and services provided by its upstream provider and third parties to monitor traffic on its network and identify potentially unlawful call origination activity. If S-Net has a reasonable basis to believe that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, S-Net can suspend and/or terminate service to the customer by the use of the underlying platform which is provided by the underlying carrier.
- S-Net has a protocol to work with the Company's upstream provider to block various types of calls by default by using the tools provided to the Company by the underlying provider who supports the platform.

TRACEBACK

The company is committed to cooperating with the Federal Communications Commission (FCC), law enforcement, and the industry traceback consortium in investigating and stopping any illegal robo-callers that it learns are using our service to originate calls or transit calls into the United States and territories.

The Company commits to fully responding within 24 hours to all traceback requests from the ITG, the TPTG, the FCC, and law enforcement. The Company shall cooperate with these groups to investigate and stop any illegal robo-callers from using the Company's service to carry or process illegal calls.

When notified by the FCC's Enforcement Bureau, Company shall block and report identified illegal traffic, and any substantially similar traffic, on an ongoing basis when Company receives actual written notice of such traffic from the Enforcement Bureau. If Company determines that the identified traffic is not illegal, Company shall provide the Enforcement Bureau with an explanation as to why Company reasonably concluded that the identified traffic is not illegal, and what steps it took to reach that conclusion.

The Company utilizes a combination of tools provided by its underlying carriers and platform providers along with third-party solutions to check for Do Not Originate (DNO) numbers. In addition, the Company utilizes a combination of internal tools and third-party solutions to detect invalid phone number formats, area codes and unassigned number blocks. The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns and to check originating number use against customer profiles.

UPSTREAM PROVIDERS

S-Net has relationships with a number of upstream providers. The key primary upstream providers listed below provide the services to S-Net.

Telnyx, LLC
Bandwidth Inc.
Inteliquent Inc.
VoIP Innovations Inc.

The company has the ability through this platform and with the interaction of the upstream provider, to reserve the right to refuse traffic from any party at any time where robocalling or use of originating numbers that are not valid.

The Company is able to block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number transiting the Company's networks.

ONGOING ROBOCALL MITIGATION

The company monitors and examines call detail records (CDRs) on a repeating basis to detect suspicious call activity and/or calling patterns. When the company, or its underlying provider detects network usage patterns consistent with illegal robocalls or suspects illegal robocalling is taking place, the company will immediately seek to identify the party that is originating, terminating, or routing these calls and take appropriate action.

The actions taken may include, but are not limited to, initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate and/or d/b/a name; blocking the party's ability to originate, terminate, or route calls on the network; and/or providing notice to law enforcement authorities.

As part of Company plan to mitigate and prevent any originating robocalls, the company is committed to early identification and investigation of possible robocalling conditions. Among other things, with the tools and resources provided to the Company by its underlying carrier, the company watches for higher-than-normal subscriber traffic volume, including large bursts of traffic in small timeframes or spikes in usage.

With the tools provided to the Company by its underlying provider, the company also monitors for originating calls classified as high volume short duration ("HVSD"), tracks for low call completion percentages, and/or originating calls with sequential called-to-number dialing patterns.

COMPANY DECLARATION

The Company certifies that it has never been under investigation or committed any violations within the last two years with any local, state, or Federal agency or equivalent related to telemarketing or robocalling. Additionally, the Company is not currently subject to a formal action or investigation due to suspected unlawful robocalling or spoofing.

If or when the Company business changes, designated Company representatives will update this RMP as appropriate.