

DYOPATH, LLC VOIP Robocall Mitigation Plan

DYOPATH, LLC VOIP hereby submit this Robocall Mitigation Plan (the "RMP") to the Federal Communications Commission ("FCC") pursuant to the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.

- (1) **DYOPATH, LLC VOIP** is a Cooperative Voice Service Provider as defined by the USTelecom Industry Traceback Group ("ITG") and takes all necessary steps to prevent illegal robocalling activities to reduce the number of illegal robocalls and removes those CSPs that are considered uncooperative, or generate Tracebacks in order to protect the Public Switched Telephone Network from abusive and/or unlawful robocalls. **DYOPATH, LLC VOIP** takes steps beyond the ITG to move more rapidly, including directly communicating with originating providers that have provided Direct Inward Dial ("DID") numbers to parties using those numbers to generate such illegal, abusive and/or unlawful robocalls as well as directly contacting affected agencies or third parties.
- (2) **DYOPATH, LLC VOIP** is implementing STIR/SHAKEN in partnership with Sansay Systems as the STI-Certificate Authority (STI-CA) service provider for Company. Sansay will interact with the STI-Policy Administrator (STI-PA) on **DYOPATH, LLC VOIP** behalf.
- (3) **DYOPATH, LLC VOIP** monitors its network for fraud and fraudulent activity. We have active monitors that continuously run to detect suspicious traffic patterns, fraud and hack attempts. Our network operations center acts on the information provided by our monitoring systems as well as information provided by other upstream and downstream operators to reduce fraudulent and/or illegal robocall traffic. **DYOPATH, LLC VOIP** acts as quickly as possible to reject such traffic through blocks and if appropriate shuts down the CSP. In some cases **DYOPATH, LLC VOIP** will notify the DID provider of the fraud directly by contacting their support department.

(“ANIs”) based on data in the LERG, numbers that are known government agencies using lists compiled by the industry as well as blocking by the Originating Carrier Number (“OCN”) inclusive of mobile numbers.

- (4) **DYOPATH,LLC VOIP** notifies the customer of such traffic and asks for remediation as well as cooperation under the TRACED act to identify repeated originators of such traffic.
- (5) **DYOPATH,LLC VOIP** has a “Know Your Customer” policy that includes a manual check of whether or not a customer has a US address, a US based representative, an FRN, a USAC Filer ID, a record in the Robocall Mitigation Database and participates in traceback events. Interoperability tests are conducted with each client through an automated system designed to avoid any manual error. CSPs and gateway operators are required to comply with the STIR/SHAKEN framework. Non-gateway operators sign an addendum certifying that they are not providing wholesale access to the PSTN prior to attestation under STIR/SHAKEN.

Acceptable Use Policy

You must not use our Services for illegal, fraudulent, or abusive purposes. If we find improper use, we may terminate your Service and charge applicable fees. Prohibited Uses of **DYOPATH,LLC VOIP**

1. Illegal or Harmful Behavior:

Do not engage in behavior that is illegal, obscene, threatening, harassing, defamatory, or invasive of another’s privacy.

Avoid deceptive, fraudulent, or malicious actions.

2. Unsolicited Messages (Spam):

Sending unsolicited messages (spam) via email, voicemail, SMS, or faxes is strictly prohibited.

Do not collect information about others without their consent.

3. Malicious Software:

Negligently transmitting harmful software (viruses, trojan horses, etc.) is forbidden.

4. Caller ID Integrity:

Creating false Caller ID identities or misleading others about the origin of your calls is not allowed.

5. Intellectual Property Rights:

Do not transmit material that infringes on intellectual property rights of third parties.

6. Excessive Usage:

Use the Services within expected business norms.

Avoid excessive usage that disrupts other customers experience.

7. Interference and Exploitation:

Do not interfere with other customers' use of the Services.

Avoid methods or devices designed to exploit or bypass this policy.

By adhering to these guidelines, you contribute to a positive and secure communication environment.