

## Endstream Communications Robocall Mitigation Plan

Endstream Communications, LLC (“Endstream”) 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) Endstream 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. Endstream 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) Endstream 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 Endstream’s behalf.
- (3) Endstream 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. Endstream acts as quickly as possible to reject such traffic through blocks and if appropriate shuts down the CSP. In some cases Endstream will notify the DID provider of the fraud directly by contacting their support department.

- (4) Endstream has systems that can automatically block and blacklist certain traffic, inclusive of non-confirming originating numbers (“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.
- (5) Endstream 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.
- (6) Endstream 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.