

ACM Communications

Robocall Mitigation Compliance with TRACED Act

ACM Communications. (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 robocallers that it learns are using our service to originate calls or transit calls into the United States and territories.

The Company has partially implemented STIR/SHAKEN internally and fully with its external providers.

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 robocallers from using 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 (unless Company’s investigation determines that the traffic is not illegal) 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 does not allow ANY automated dialers on its network.

The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles. The Company uses data systems for analytics and reviews to identify illegal robocalling in addition to a Know Your Customer (KYC) requirement to access the Company’s networks. The process includes:

- Monitoring its network to identify suspicious traffic/calling patterns.
- Limiting users capacity via call per second and/or concurrent session limits.
- Regularly checking call patterns for possible abusive traffic.
- All new customers are verified with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. First time users are generally meet in person to as equipment is installed for them at their location. The Company severely limits the capabilities of all accounts and may require additional authorization not limited to pin codes and second factor authentication for certain types of calls.

ACM Communications has three upstream providers from which is receives and/or sends voice traffic: The Company reserves the right to refuse traffic from any party at any time where robocalling or use of originating numbers that are not valid or they are not authorized to use has occurred or is suspected. The Company directly controls the specific

equipment that is connected to its network with each user residing on their own Company controlled system. This allows us to easily stop ALL calls from an offending user location if needed. 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 network.