

BCM One Robocall Mitigation Compliance with TRACED Act

BCM One, Inc. and its affiliated entities (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 following entities are all subject to the robocall mitigation policies and procedures described in this document:

- BCM One, Inc.
- Arena One, LLC
- Coredial, LLC
- BCM One Cloud Communications, LLC
- nexVortex, LLC
- PayG, LLC
- SIP.US LLC
- Wholesale Carrier Services, Inc.
- Pure IP California LLC

The Company has fully implemented STIR/SHAKEN for all of its affiliated entities.

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 utilizes a combination of internal tools and 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, originating number use against customer profiles.

The Company has an Upstream Provider Policy required to access the Company’s networks to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. If the customer is a Voice Service Provider, The Company confirms that the provider is appropriately listed in the FCC’s RMD and has not been delisted pursuant to an enforcement action before accepting traffic from the provider.

The Company uses data systems for analytics and reviews to identify illegal robocalling in addition to a Know Your Customer (KYC) requirements. The process includes:

- Monitoring the network to identify suspicious traffic patterns.
- Limiting customers' 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. The Company severely limits the capabilities of new accounts until these appropriate processes are complete.

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 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.