

CMH Solutions LLC
1421 Commonwealth Ave
Cleveland, OH 44124

Robocall Mitigation Compliance with TRACED Act

Introduction

CMH Solutions LLC ("*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. CMH Solutions takes a multi-layer approach to mitigating robocalls using multiple methods as outlined below.

STIR/SHAKEN Implementation

The Company has fully implemented STIR/SHAKEN.

Traceback Requests

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 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.

Know Your Customer

The Company adheres to all Know Your Customer (*KYC*) requirements prior to granting new clients access to the Company's networks. Our vetting 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.

During the onboarding phase, we conduct detailed assessments to determine each provider's position within the broader telecommunications ecosystem. This classification process helps us understand their operational role - whether as originators of voice services, international intermediaries, or domestic relay operators. This understanding enables us to properly manage authentication requirements for unsigned traffic streams.

Our contractual framework explicitly prohibits the transmission of unauthorized automated calls. In cases where suspicious patterns are detected, we initiate immediate corrective action through a structured response protocol:

- Issuing formal warnings requiring immediate cessation of problematic traffic.
- Implementing progressive enforcement measures if violations persist.
- Initiating service termination proceedings for repeat offenders.

This multi-layered approach ensures consistent compliance with industry standards while maintaining the integrity of our telecommunications infrastructure.

Know Your Provider

Our organization implements a rigorous evaluation system for all upstream telecommunications partners who route voice communications through our network. This systematic approach ensures compliance with regulatory requirements and industry standards for traffic termination and transit operations.

As part of our initial verification protocol, we mandate that all prospective upstream providers maintain active registration status within the Robocall Mitigation Database. No voice traffic is accepted from unverified entities, establishing a fundamental security baseline for our network integrity.

Our partnership criteria include several essential components:

- Implementation of a robust anti-robocall strategy.
- Establishment of thorough customer screening procedures.
- Deployment of sophisticated call pattern analysis systems.
- Maintenance of comprehensive monitoring protocols for suspicious activity detection.