



ROBOCALL MITIGATION PLAN

PUBLIC

CMS Internet LLC

131 S Main St
Mount Pleasant, MI 48858



Robocall Mitigation Plan

CMS Internet ("CMS") is committed to preventing illegal calls originating from or transiting its network and to complying fully with the Federal Communications Commission's (FCC) robocall mitigation requirements under the TRACED Act, 47 CFR Part 64 (Subpart HH), and related orders. This Robocall Mitigation Plan (RMP) describes the specific reasonable steps CMS takes to avoid originating, transmitting, or facilitating illegal robocalls or spoofed traffic. CMS has fully implemented STIR/SHAKEN caller ID authentication and supplements this with additional proactive measures across fraud detection, traffic screening, customer vetting, provider due diligence, traceback cooperation, and other practices.

STIR/SHAKEN

CMS has fully implemented STIR/SHAKEN caller ID authentication as of July 15, 2021. All calls originated by CMS customers are authenticated and signed in accordance with the STIR/SHAKEN framework.

Attestation levels are assigned consistent with industry best practices and ATIS standards (full "A" attestation where CMS has verified both the customer's identity and authorization to use the calling number; partial "B" or gateway "C" as appropriate based on verification). The assigned attestation level and Origination Identifier (ORIGID) are recorded in call detail records (CDRs) for every call to support investigations, traceback requests, and robocall mitigation efforts.

Know Your Customer

CMS adheres to best practices recommended by the NANC Call Authentication Trust Anchor Working Group and implements a robust Know Your Customer (KYC) policy and procedures.

CMS collects the following information from customers before provisioning service:

- Validated identifying information;
- Business ownership details;
- Employer Identification Number (EIN);
- Authorized contacts list;
- Description of the customer's business and intended service use;
- Publicly available business records;
- Proof of physical location of service; and
- Additional enhanced due diligence measures for high-risk customers.

All interactions with customers are authenticated to confirm the right to access accounts or request modifications.



131 S Main Street
Mount Pleasant, MI 48858

(800) 962-7022

Know Your Provider

CMS only accepts traffic from and delivers traffic to registered providers in the Robocall Mitigation Database (RMD).

Prior to onboarding any upstream provider, CMS conducts a review to confirm their registration in the RMD, their STIR/SHAKEN implementation status, and the robocall mitigation measures they have implemented on their network. This information is periodically reviewed to monitor any changes in registration status or compliance. CMS also verifies expected provider behavior, including the preservation of identity headers sent or received, before authorizing production traffic.

Telephone Number Authorization

Customers using telephone numbers not directly managed by CMS must register those numbers and provide a valid Letter of Authorization (LOA) confirming they are the authorized subscriber or user of the numbers. When a customer attempts to originate calls from an unregistered number, CMS notifies them and offers the option to register with a valid LOA or have the number blocked from origination.

Exceptions may be granted for business telephone systems performing legitimate call forwarding. In such cases, CMS collaborates with the customer to ensure proper signaling and compliance where feasible.

Residential customers are not permitted to originate calls using numbers outside of those directly managed by CMS and assigned to the applicable account.

Traceback Requests

CMS will respond within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and will cooperate fully with these entities to investigate and halt illegal robocalls using its network for origination or transit. CMS will collaborate with customers to immediately address and remediate any unauthorized or unlawful calling, including potential suspension or termination of service.

Traceback requests can be sent to: **noc@cmsinter.net**

Network operations center is available 24x7: **(989) 400-4888**



Fraud Monitoring Practices

CMS employs internal fraud monitoring to identify and prevent potential illegal robocall activity on its network. This involves analyzing call detail records for indicators such as unusual call volumes, spikes in international calls, short-duration calls, and sequential dialing patterns.

The system establishes a baseline of typical calling behavior over a recent period for each account and compares current activity against it within defined time windows. When deviations exceed set thresholds, real-time notifications are sent to the CMS network operations center. All alerts are logged for review.

Ongoing efforts include exploring advanced detection techniques to improve speed and accuracy, as well as internal testing of fraudulent patterns using simulation tools in an isolated lab environment.

Do Not Originate (DNO) Practices

CMS utilizes a comprehensive Do Not Originate (DNO) list containing numbers identified as invalid, unallocated, inactive, or specifically designated by responsible organizations and service providers as unsuitable for origination. This includes numbers vetted by industry groups as having been used to spoof illegal, fraudulent, or malicious traffic. All calls are screened against this dataset in real time, and any matching prefix or number results in immediate blocking to prevent the transmission or delivery of potentially unlawful traffic.

Enforcement

CMS immediately investigates any suspicious activity detected or reported for calls originated by a customer or received from a provider. Customers originating invalid or suspicious calls are immediately notified. If action cannot be immediately taken, the entire account or the affected number will be immediately disabled or blocked. Invalid or suspicious calls received from an upstream provider are immediately investigated. In this case the applicable provider is notified, engaged for further investigation, and the numbers are blocked if necessary.

CMS Terms of Service prevent the use of its services for illegal purposes.

Eligibility

Neither CMS nor any entity with which it shares common ownership, management, directors, or control has been subject to any formal FCC, law enforcement, regulatory action or investigation in the prior two years due to involvement with illegal robocalls or spoofing, or due to a deficient RMD certification or mitigation plan.