

ROBOCALL MITIGATION PLAN

Filed pursuant to 47 CFR § 64.6305 — Foreign Voice Service Provider Certification

1. Filer Identification

This Robocall Mitigation Plan (the “Plan”) is submitted to the United States Federal Communications Commission (“FCC”) Robocall Mitigation Database (“RMD”) by the filer identified below (the “Company”), a Canadian voice service provider.

Legal entity name	MMD Data Corporation
Business address	66 West Avenue, St. Thomas, ON N5R 5H7 Canada
Jurisdiction of formation	Ontario, Canada
FCC Registration Number (FRN)	0038554861
Provider classification	Voice Service Provider without a STIR/SHAKEN obligation (foreign)
Primary contact	Daniel Pfingstgraef
Traceback / enforcement contact	Daniel Pfingstgraef, Partner rmd@mmddata.com , 226-400-4011
Date of certification	June 17, 2026

2. Nature of Operations and Basis for Filing

The Company is a reseller of voice telecommunications services to business and community customers located in Canada. The Company does not own carrier-grade network facilities; it provides voice service to its end users using underlying transport and termination supplied by its upstream carrier.

The Company’s U.S.-bound traffic is originated by Canadian end users and handed to its upstream provider, FOURTEEN IP INC. (“Upstream Carrier”), which carries and terminates that traffic into the United States. As a condition of carriage, the Upstream Carrier requires the Company to maintain a valid certification in the RMD. The Company files this Plan on that basis and certifies the matters below under penalty of perjury.

Caller identification profile. The Company’s end users present **Canadian** North American Numbering Plan (NANP) telephone numbers in the caller identification field. The Company does not assign, and its end users do not present, United States NANP numbers.

STIR/SHAKEN status. As a Canadian entity, the Company is not eligible to obtain a United States Service Provider Code (SPC) token and has no U.S. STIR/SHAKEN implementation obligation. The Company does not authenticate or sign calls under the U.S. STIR/SHAKEN framework, and does not sign calls under the Canadian STIR/SHAKEN regime. Accordingly, the Company relies entirely on the robocall mitigation program described in this Plan, as contemplated by 47 CFR § 64.6305(b).

3. Reasonable Steps to Avoid Originating Illegal Robocall Traffic

The Company has implemented the following practices, reasonably designed to prevent the origination of illegal robocalls and unlawfully spoofed traffic on its network:

3.1 Know Your Customer (KYC)

- Every customer is onboarded under a written service agreement that expressly prohibits illegal robocalling, unlawful caller-ID spoofing, and any use of the service that violates applicable Canadian or United States law.
- Before a customer is activated, the Company verifies the customer's identity and legitimacy, including its registered business name, a billing and operational contact, and the specific telephone numbers the customer is authorized to use as caller identification.
- A record of each customer's verification and authorized number list is retained as part of the customer file.

3.2 Caller-ID Integrity

- Outbound caller identification is constrained, on a per-customer basis, to telephone numbers that have been assigned to the customer by the Company or verified as belonging to the customer. The Company's session border / trunking configuration rejects or overrides any caller-ID value outside a customer's authorized list.
- Customers are not permitted to present arbitrary, unverified, or third-party telephone numbers, and the platform is configured to prevent them from doing so.

3.3 Traffic Monitoring

- The Company reviews call detail records (CDRs) on a recurring basis for indicators of abuse, including abnormal call volumes, short-duration call spikes, elevated invalid- or unallocated-number ratios, and other patterns consistent with autodialed or fraudulent campaigns.
- Anomalies identified through this review are investigated and, where warranted, result in mitigation action under Section 3.4.

3.4 Enforcement Against Offending Customers

- The Company's service agreement reserves the right to throttle, suspend, or terminate any customer found to be originating illegal robocall traffic, and the Company exercises that right promptly upon confirmation of such activity.
- Confirmed abuse and the action taken in response are documented and retained as described in Section 6.

4. Commitment to Respond to Traceback Requests

The Company commits to respond fully and **within 24 hours** to all traceback requests it receives from the FCC, from law enforcement, and from the industry traceback consortium (the Industry Traceback Group), consistent with 47 CFR § 64.6305(b).

- The traceback contact identified in Section 1 is responsible for receiving and actioning traceback requests and is reachable within the required timeframe.

- Upon receiving a traceback, the Company identifies the relevant source of the implicated call within its records and provides the requesting party with the information needed to continue the trace, including the originating customer and the immediate upstream path.
- Where a traceback identifies one of the Company's own customers as the originator of illegal traffic, the Company takes prompt mitigation action under Section 3.4.

5. Cooperation with the FCC, Law Enforcement, and Industry

- The Company will respond to lawful inquiries from the FCC and law enforcement regarding suspected illegal traffic on or transiting its network.
- The Company will cooperate with its Upstream Carrier and with downstream United States providers in investigating and mitigating suspected illegal robocall campaigns.
- The Company will keep its RMD filing accurate and current, updating the filing within ten (10) days of any change to the information it contains, and recertifying annually by March 1 as required by 47 CFR § 64.6305(h).

6. Know-Your-Upstream and Recordkeeping

- The Company's sole upstream provider for United States-bound voice is FOURTEEN IP INC.. The Company has confirmed that its Upstream Carrier maintains its own robocall-mitigation and RMD obligations.
- The Company maintains records sufficient to support traceback responses and to demonstrate compliance with this Plan, including customer onboarding and verification records, each customer's authorized caller-ID list, and call detail records.
- Call detail records are retained for at least 12 months. Records relevant to a specific traceback or investigation are preserved for the duration of that matter.

7. Certification

The undersigned, a duly authorized representative of the Company, certifies under penalty of perjury that the Company has implemented the robocall mitigation program described in this Plan; that all calls originated, carried, or processed on the Company's network are subject to that program; and that the information contained in this Plan and in the associated RMD filing is true, accurate, and complete.



Daniel Pfingstgraef, Partner

MMD Data Corporation

Date: **June 17, 2026**