

ROBOCALL MITIGATION PLAN

Filer: IsoFusion, Inc. d/b/a TrueRing

Date of Filing: October 14, 2026

1. SECTION 1: REGULATORY COMPLIANCE AND ENFORCEMENT HISTORY

IsoFusion, Inc. ("the Company") and its operating brand, TrueRing, certify that they have not been prohibited from filing a certification in the FCC Robocall Mitigation Database (RMD). Neither IsoFusion, Inc., its subsidiaries, nor any of its current executives or principals have any history of enforcement actions, official citations, or formal warnings from the Federal Communications Commission (FCC), Federal Trade Commission (FTC), or state authorities regarding illegal robocalls, Telephone Consumer Protection Act (TCPA) violations, or Telemarketing Sales Rule (TSR) violations.

2. SECTION 2: STIR/SHAKEN STATUS AND INFRASTRUCTURE EXEMPTION

The Company operates primarily as an internet service provider and interconnected VoIP reseller.

- **Upstream Architecture:** The Company utilizes the carrier-grade network infrastructure of [Alianza, Inc.](#) (RMD0006320) to process and terminate outbound residential voice traffic. Alianza, Inc. has fully implemented STIR/SHAKEN protocols on its IP voice networks. For our business customers the Company relies on our upstream wholesale carrier, Sangoma U.S., Inc. (Filer ID: 831033) to execute cryptographic call token signing (STIR/SHAKEN) at the transmission gateway layer before traffic is handed off to intermediate or terminating carriers.
- **Exemption Claim:** Because the Company operates without direct control over the physical underlying network switches necessary to execute cryptographic signatures via an STI-PA token, the Company claims an **Infrastructure Exemption** under **47 CFR § 64.6305(d)(2)(i)**.
- **Hosted PBX Guardrails:** On the Company's proprietary hosted-PBX solution, strict system configurations ensure customers are limited to utilizing only pre-assigned, dedicated phone numbers. The software architecture prevents end-users from altering, spoofing, or overriding the outgoing Caller ID parameter.

3. SECTION 3: KNOW YOUR CUSTOMER (KYC) AND VETTING PROCEDURES

To ensure no illegal traffic originates on its platform, the Company enforces strict "Know Your Customer" protocols prior to service activation:

- **Geographic Boundaries:** The Company exclusively sells corporate services to entities legally registered and physically based within the United States.
- **Identity Verification:** Before executing a service agreement, all prospective business accounts are subject to identity verification, company purpose and intended phone use.
- **Contractual Enforcement:** All customers must execute a Master Services Agreement (MSA) that includes explicit restrictions prohibiting the utilization of the Company's services for high-volume automated dialers, telemarketing, or any form of unlawful or deceptive activity. Violation of these policies triggers immediate, unconditional termination of service.

4. SECTION 4: TRAFFIC MONITORING AND FRAUD DETECTION

The Company deploys internal monitoring and fraud detection systems to observe traffic anomalies in real-time:

- **Anomaly Triggers:** The platform continuously monitors outbound call volumes, short-duration call ratios, and simultaneous call-concurrency thresholds.
- **Mitigation:** If an enterprise customer accounts for an unexpected spike in traffic patterns consistent with illegal robocalling, the fraud detection engine flags the account and suspends outward calling privileges pending an administrative review.

5. SECTION 5: CARRIER COMPLAINTS AND INVESTIGATION TRIAGE

The Company treats downstream carrier alerts with high severity. Upon receipt of a complaint, abuse notice, or warning from a peer or upstream carrier, the Company:

1. Immediately initiates an internal audit of Call Detail Records (CDRs) to isolate the exact source customer.
2. Temporarily suspends or throttles the suspect traffic channel to mitigate immediate harm to the public telephone network.
3. Demands immediate verification of compliance from the end-user. Failure to prove authorization or a legitimate business purpose results in permanent account closure.

6. SECTION 6: MANDATORY 24-HOUR TRACEBACK COMMITMENT

Pursuant to FCC regulations, IsoFusion, Inc. dba TrueRing affirms its absolute commitment to cooperate with all authorized investigative bodies. The Company will respond **fully and within 24 hours** to all formal traceback requests received from the Federal

Communications Commission, federal or state law enforcement agencies, and the official industry traceback consortium (the Industry Traceback Group / ITG). The Company will actively assist these entities in tracking, isolating, and stopping any bad actors attempting to exploit its platforms.