

ROBOCALL MITIGATION PLAN (RMP)

Company: AUTHENCORE USER LLC **Effective Date:** April 16, 2026

I. Introduction and Statement of Principles

AUTHENCORE USER LLC maintains an unwavering commitment to consumer protection and the integrity of the global telecommunications network. We have established a rigorous Robocall Mitigation Program designed under high-security standards to proactively prevent, detect, and block illegal calling traffic, caller ID spoofing, and any form of unauthorized automated telemarketing.

II.

Network Architecture and Origination Control

Our technological infrastructure prioritizes security and traceability at every level:

- **Management Platform:** We implement PBX as our core routing and call management system, ensuring a controlled and auditable operational environment.
- **Signaling Security:** All voice traffic and SIP signaling are protected using industry-standard encryption protocols (TLS/SRTP) to prevent data manipulation or interception.
- **Origination Restriction:** Traffic on our network is strictly limited to originating exclusively from known, authenticated, and previously authorized endpoints and extensions.
- **Traffic Filtering:** We categorically reject traffic originating from unknown sources or unverified third-party networks.

III.

"Know Your Customer" (KYC) Policy

To mitigate risks and prevent access by malicious actors, we enforce a strict KYC policy for all new and existing clients:

- **Identity Verification:** We require valid business documentation, identity verification of legal representatives, and verifiable physical and tax contact information prior to activating any services.
- **Use Case Evaluation:** We comprehensively review the nature of the client's business model and their intended telecommunications use case to ensure alignment with our policies.
- **Mass Traffic Restrictions:** Our Terms of Service explicitly prohibit the use of our network for unauthenticated broadcast traffic, illegal robocalls, unregulated predictive dialers, or any automated telemarketing activity without prior express consent (strict TCPA compliance).

IV.

Continuous Traffic Monitoring and Analysis

AUTHENCORE USER LLC actively monitors call patterns traversing our network to identify anomalies that suggest illegal activity:

- **Real-Time Alert Metrics:** We monitor traffic in real-time to detect unusually high call volumes and traffic bursts (high Calls Per Second - CPS rates).
- **Performance Analysis:** Our systems are configured to flag and audit accounts displaying patterns of short-duration traffic, a low Answer Seizure Ratio (ASR), or an abnormally low Average Length of Call (ALOC), which are classic indicators of robocalling campaigns.
- **Periodic Audits:** We conduct periodic reviews of Call Detail Records (CDRs) to ensure continuous compliance with our internal policies and federal regulations.

V. Response, Mitigation, and Traceback Protocols

Upon detecting suspicious activity or receiving notifications from upstream providers or regulatory agencies regarding illicit traffic:

- **Immediate Action:** We will immediately suspend, block, or terminate any accounts or extensions found to be originating illegal traffic.
- **Traceback Cooperation:** We are fully committed to cooperating with the FCC's Industry Traceback Group (ITG), the Traceback Consortium, and law enforcement agencies to identify the source of any suspicious call passing through our network within a 24-hour timeframe.

VI.

STIR/SHAKEN Implementation Status

In compliance with current Federal Communications Commission (FCC) regulations:

- **Extension Certification:** AUTHENCORE USER LLC certifies that it currently qualifies for the extension of the STIR/SHAKEN caller ID authentication framework implementation deadline applicable to small voice service providers, pursuant to 47 C.F.R. § 64.6304.