
Robocall Mitigation Plan for Telecom Audit Solutions, LLC

1. Introduction and Commitment

Telecom Audit Solutions, LLC ("TELECOM AUDIT SOLUTIONS"), an interconnected VoIP provider specializing in international gateway traffic collection for wholesale, enterprise, and call center clients, is committed to preventing the origination, carrying, and termination of illegal robocalls on its network.

Pursuant to the Federal Communications Commission's (FCC) rules under 47 C.F.R. § 64.6300 et seq., this Robocall Mitigation Plan (RMP) outlines TELECOM AUDIT SOLUTIONS's comprehensive practices and procedures. These measures include the implementation of the STIR/SHAKEN call authentication framework where feasible and robust mitigation strategies to combat illegal robocall traffic.

2. STIR/SHAKEN Implementation

TELECOM AUDIT SOLUTIONS is classified as a small provider and is working diligently toward full implementation of the STIR/SHAKEN protocol within its IP network.

Notwithstanding this extension, TELECOM AUDIT SOLUTIONS is committed to employing alternative and effective measures, as detailed in this plan, to mitigate illegal robocalls.

3. Robocall Mitigation Practices and Procedures

3.1. Customer Compliance and Agreements

All TELECOM AUDIT SOLUTIONS customers are contractually obligated to adhere to all applicable federal and state laws and regulations, including the Telephone Consumer Protection Act (TCPA), FCC robocall rules, and Federal Trade Commission (FTC) regulations. Customer agreements explicitly grant TELECOM AUDIT SOLUTIONS the right to immediately block traffic or terminate service for any violation of these prohibitions against illegal robocalling and spoofing.

3.2. Know Your Customer (KYC) and Customer Onboarding

TELECOM AUDIT SOLUTIONS employs a rigorous Know Your Customer (KYC) process for all new clients. This commercially reasonable due diligence includes, but is not limited to:

- Verification of business identity and legal status (e.g., state/country of incorporation).

- Collection of a physical business address, primary contact information, and Federal Tax ID/EIN.
- Validation of business nature and intended use of services.
- Collection of USAC Filer ID and banking/payment information.

3.3. Network Monitoring and Anomaly Detection

TELECOM AUDIT SOLUTIONS continuously monitors calling patterns and traffic volumes across its network to identify and investigate anomalies indicative of fraudulent activity, such as illegal robocalling, traffic pumping, and international toll fraud. Upon identifying suspicious activity, TELECOM AUDIT SOLUTIONS will take immediate action, which may include blocking specific traffic patterns or terminating customer agreements, particularly if a violation is determined to be intentional.

3.4. Robocall Mitigation Database (RMD) Compliance

TELECOM AUDIT SOLUTIONS is registered in the FCC's Robocall Mitigation Database. In accordance with FCC mandates, TELECOM AUDIT SOLUTIONS will only accept voice traffic for termination from other providers that are also duly registered in the Robocall Mitigation Database and have filed their own RMPs.

3.5. Cooperation with Traceback Requests

TELECOM AUDIT SOLUTIONS commits to fully and promptly cooperating with all lawful traceback investigations initiated by the FCC, law enforcement agencies, and the industry traceback consortium (e.g., USTelecom's Industry Traceback Group). This cooperation is essential to investigating and stopping illegal robocallers who attempt to misuse our network.

4. Continuous Improvement

TELECOM AUDIT SOLUTIONS is committed to the continuous review and enhancement of this Robocall Mitigation Plan. We will actively monitor industry "best practices" and technological advancements to strengthen our internal processes and adapt our systems to the evolving threat of illegal robocalls.

5. Certification and Filing

TELECOM AUDIT SOLUTIONS certifies that the information provided in this plan is true and accurate to the best of its knowledge. This plan will be updated and re-filed in the FCC's Robocall Mitigation Database as required by law or whenever significant changes to our mitigation practices occur.