



FRN: 0003737640

OCN: 5447

Robocall Mitigation Plan

Updated: April 24, 2024

I. Robocall Mitigation Program Introduction

This Robocall Mitigation Plan is submitted by Access One, Inc. ("Access One") pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission ("Commission") which require all voice service providers to establish a robocall mitigation plan ("RMP"). This document sets forth Access One's current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. Access One views these policies and procedures as constituting reasonable steps to avoid the origination of illegal robocalls on its network and in addition to following these steps, Access One commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

A. Company Summary

Access One is a facilities-based CLEC and interconnected Voice over Internet Protocol ("VoIP") provider located in Chicago, Illinois and provides domestic originating and terminating services to a broad range of business customers.

Access One has no affiliated companies. Access One has never been subject to a formal action or investigation due to suspected unlawful robocalling or spoofing.

B. Filing of RMP and Implementation of STIR/SHAKEN

Access One has fully implemented STIR/SHAKEN and has submitted its certification that all voice traffic that originates on its network is authenticated with STIR/SHAKEN consistent with those regulations adopted by the Commission. In addition, Access One has uploaded this RMP into the RMD because it details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic and has included a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

II. Robocall Mitigation Program

This RMP applies to Access One's calling platforms and provides information on Access One's policies and procedures on the following topics that are discussed in turn below which details the specific reasonable steps Access One has taken to avoid carrying or processing illegal robocall traffic:

- (1) Knowing Your Customer Procedures
- (2) Knowing Your Upstream Provider Procedures
- (3) Requiring Contractual Provisions to Mitigate Illegal Robocalls
- (4) Only Accepting Traffic from Providers in the RMD
- (5) Blocking Calls on a Do-Not-Originate List
- (6) Analyzing and Monitoring Network Traffic Routing Through Access One's Network
- (7) Authenticating Voice Traffic Originated by Access One
- (8) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (9) Designating an Employee Responsible for Addressing Robocall Mitigation Related Issues
- (10) Updating Access One's RMD Submission and RMP

A. Knowing Your Customer Procedures

Consistent with the Commission's Caller ID Authentication Best Practices, Access One vets the identity of its subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources. In so doing, Access One takes affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.

In this regard, Access One has implemented appropriate Know Your Customer ("KYC") protocols when onboarding new or renewing customers. As part of its KYC protocols, Access One requires any customer to provide sufficient information to ensure its legitimacy. Among other things, Access One generally requires its customers to provide the full legal name of the company, state or country of incorporation, the physical address of its operations, the billing name and address (when different), and the customer contact name and telephone number, and nature of the customer's business.

B. Knowing Your Upstream Provider Procedures

Access One's upstream providers (Sinch and Peerless) are both STIR/SHAKEN compliant and have filed their submissions in the RMD. Access One has longstanding relationships with these upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, Access One, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking steps necessary to ensure monitoring and preventing their use for the transmission of illegal robocalls.

C. Requiring Contractual Provisions to Mitigate Illegal Robocalls

Voice service customers of Access One are subject to robust terms and conditions that (1) obligate customers not to use Access One's services for unlawful purposes; and (2) preserve Access One's right to terminate customers for violations of the law. Access One's contracts include terms that forbid the customer from using Access One's services to originate and/or otherwise transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act ("TCPA") and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ("TRACED Act") and/or the rules promulgated pursuant to these statutes. Access One's contract terms provide that if any calls originated or otherwise transmitted by the customer to Access One violate these statutes, then Access One may, at its sole discretion, suspend or terminate the customer's service immediately, among other remedies.

D. Only Accepting Traffic from Providers in the RMD

Voice Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R. § 64.6305(e)(1), Access One accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers and Foreign Intermediate Providers. In accordance with 47 C.F.R. § 64.6305(e)(2), Access One accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Gateway Providers. In accordance with 47 C.F.R. § 64.6305(e)(3), Access One accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD showing that the Gateway Provider has affirmatively submitted its filing and RMP, and (b) has not been de-listed pursuant to an enforcement action.

E. Blocking Calls on a Do-Not-Originate List

In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), Access One blocks calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan numbers. Access One has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number. Access One is utilizing the DNO list offered by US Telecom.

F. Analyzing and Monitoring Network Traffic Routing Through Access One's Network

Upon receiving call traffic, Access One also analyzes and monitors the call traffic that originates on, terminates to, or routes through Access One's voice network. Consistent with the Commission's Caller ID Authentication Best Practices, Access One monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling.

In this regard, Access One has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, atypical call activity, and subscriber information), receive automatic alerts, investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis. When analyzing and monitoring call traffic, if Access One discovers call patterns that are consistent with illegal robocalling, Access One, after further investigation, takes appropriate action to address such behaviors, which may include working with the originating customer to resolve problematic traffic, blocking the problematic calls and/or terminating the customer's service.

G. Authenticating Voice Traffic

Access One : (1) authenticates and verifies caller identification information for all SIP calls that exclusively transit its own network; (2) authenticates caller identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider, and to the extent technically feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path; and (3) verifies caller identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.

H. Responding to Commission, Law Enforcement and ITG Traceback Requests

Access One is committed to ensuring that its network is not utilized for the origination, termination or routing of unwanted and illegal robocalls. In accordance with the Commission's regulations, Access One will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium ("ITG") within 24 hours and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use Access One's network to carry or process calls. As part of this commitment, Access One will take the necessary steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable rules.

I. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Access One's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, Access One provides the following name, title, department, business address, telephone number, and email address of the individual within Access One that leads Access One's team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: John Scarpa

Contact Title: Director / Engineering

Contact Address: 820 W. Jackson Blvd; Suite 650, Chicago, Illinois 60607

Contact Telephone Number: (312) 441-9213

Contact Email: jscarpa@accessoneinc.com,

J. Updating Access One's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), Access One will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.