

MIDCONTINENT COMMUNICATIONS (MIDCO) ROBOCALLING MITIGATION PROGRAM AND POLICY

Introduction

This document sets forth the analyses that are performed and actions taken by Midcontinent Communications (“Midco”) in its role as an end-user voice service provider to identify service providers, subscribers, and phone numbers that are likely to be associated with illegal robocalls or other fraudulent voice activity; to pre-qualify prospective customers who are unlikely to generate or pass illegal and fraudulent calls; to monitor existing subscribers and upstream providers for traffic patterns and other information indicative of the potential for transmitting fraudulent robocalls; and to mitigate the acceptance and transport of fraudulent robocall traffic on the Midco network.

Robocall Mitigation Program

Midco, through its trade groups such as ATIS, NCTA, CableLabs, SCTE, etc., is participating in the development of a call authentication standard for non-IP calls and working with its various vendors on the same. In addition, we monitor the efforts of the Federal Trade Commission & the Federal Communications Commission in regard to robocall mitigation efforts, identification of industry trends, provision of consumer education materials, and other related information and alerts.

Midco is also working with its vendors to implement a robocall mitigation program for the non-IP portions of its networks. Specifically, Midco partnered with Neustar for a robocalling solution on non-IP portions of the network. Assuming that the customer has caller ID (the vast majority), the system completes the analytics for robocalling. Midco is compliant with STIR/SHAKEN with all SIP carriers that have implemented STIR/SHAKEN.

More specifically, Midco uses software provided by Neustar to monitor terminating voice traffic in real time to warn our customers of potential robocalls by overwriting the caller id field with “Potential Spam”. The software provides detailed reporting identifying suspected illegal robocalls and allows Midco to identify high volume attempts that are potential robocall traffic. Midco also uses internal analytics to identify unusual increases in voice network utilization which will be investigated to identify the customer generating the traffic.

Midco prohibits illegal activity on its network and informs customers of this illegal activity prohibitions. As stated in Ongoing Mitigation Practice, Midco has reporting in place to mitigate illegal robocalling traffic.

Know Your Customers

Customer Validation conducted on potential as well as existing customers and upstream providers, and their affiliates is designed to identify any that are known to or likely to be engaged in fraudulent activities. Potential prospects or current customers and upstream providers who have been known to act improperly or otherwise be involved in fraudulent robocalling will cause the companies to be rejected by Midco and existing customer relationships may be severed. Midco does research and documents the qualification or disqualification of current and potential customers or upstream providers as follows:

Subscribers

- Midco collects identifiable information of new or existing customers in connection with the provision of services and includes:
 - Contact information such as name, billing address, business and mobile telephone numbers, as well as email and text messaging addresses;
 - Physical service address;
 - State or country of incorporation;
 - Federal tax ID;
 - Nature of customer's business including if/how they will employ auto-dialers or robocall style tools in the conduct of their business

Upstream Providers

- The registration of potential upstream providers in the FCC's Robocall Mitigation Database ("RMD") and Intermediate Provider Registry ("IPR") is checked, and those without current registrations are disqualified from doing business with Midco.

Contractual Obligations imposed by Midco include prohibitions on transmitting fraudulent traffic, and short-duration and auto-dialed calls.

- The Acceptable User Policy (AUP) stipulates the consequences for originating such traffic including suspension of service and termination of network services.
- Traceback and prohibited traffic language is included in any contractual agreements that Midco may directly have with any upstream provider. Any upstream carrier found in violation must take corrective action or face suspension or termination of contract.

Ongoing Mitigation Practices

Monitoring Traffic of existing customers and upstream providers is continuous. Midco initiates mitigation measures if data suggests improper call activity is occurring. Measures include suspension or termination of service. Midco deploys network analytics to collect voice network data that can identify behaviors which might indicate fraudulent robocalling activity. The following data is collected and analyzed daily:

- Call traffic trends including call volume, average call duration, answer seizure ratio, and

- maximum distinct daily called telephone number in a 24-hour period;
- Collection of suspicious telephone numbers that include the originating telephone number, terminating telephone number, total calls, total connected minutes, short duration amounts, average call duration, and answer seizure ratio;
- Terminating traffic trends that include callback rates, answer seizure rates, and call durations to establish historical calling patterns;
- Phone number identification information on customer-originating calls to possibly identify telephone numbers that have been manipulated and not associated with Midco-assigned telephone numbers. Data include originating NPA-NXX, originating OCN, originating OCN territory, total calls, total connected minutes, average call duration, answer seizure ratio, and maximum distinct daily called telephone numbers in a 24-hour period.

Traceback Cooperation

- Midco is committed to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group (ITG), and to cooperating with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
- If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, Midco notifies and removes the offending customer.
- Midco has identified a single internal point of contact for all traceback inquiries:
Contact Name:

Patrick Miller
 Directory of Voice & Mobility
Patrick.Miller@Midco.com
 (605) 274-2970
 Normal Business Hours: 8:00 a.m. to 5 p.m. CST

Principals, Affiliates, Subsidiaries, and Parent Companies

There are no principals, affiliates, subsidiaries, or parent companies that exercise management or control of Midcontinent Communications.

Certification

Midcontinent Communications (OCNs 7076, 3065, 429A and 995H) certifies it has not been prohibited from filing in the Robocalling Database pursuant to law enforcement action.