

Randolph TMC Robocall Mitigation & STIR/Shaken Plan

RTMC has implemented the following Robocall Mitigation & STIR/Shaken Plan to detect and prevent unlawful robocalls from originating on its network. All calls that originate on RTMC's network are subject to the described robocall mitigation program.

RTMC has upgraded its Session Border Controllers to the latest version of software and has implemented STIR/Shaken on the IP portions of its network.

RTMC has also implemented the Ribbon Call Trust Reputation Scoring service to mitigate originating and terminating robocalls on its network.

Originating Robocall Mitigation

To prevent robocalls from originating on a voice service provider's network, a query is made to the Reputation Scoring service for every call attempt to determine the likelihood that a call is illegitimate and should be blocked. The query is done using SIP messaging.

A call will be considered illegitimate for two reasons:

- If the originating number is being spoofed using a telephone number that shows up on a Do-Not-Originate list or is an unallocated, unused, or invalid number.
- If reasonable analytics indicate the call is highly likely to be illegitimate and malicious in intent.

If the call is determined to be illegitimate, the response back to the originating call controller/switch will be to block the call; the originating call controller/switch will be instructed to route the call based on normal routing.

Terminating Robocall Mitigation

To prevent robocalls from terminating on a voice service provider's network, a query will be made to the Reputation Scoring service for every call, prior to final call disposition, to determine the likelihood that a call is illegitimate and should be blocked or is likely legitimate and should be allowed to proceed normally. Unfortunately, many calls may have reputation scores that fall somewhere between these two outcomes and should be given special call validation treatment options. Some examples of call validation treatment options are:

- Route to an announcement indicating the call cannot be completed at this time
- Divert to a voice mail system

- Route to a "CAPTCHA" system that will play an announcement asking the calling party to respond to instructions, such as entering a specific set of digits, if they want the call to proceed.
- Alter the Calling NAME (CNAM) display to "Potential SPAM" to let the terminating party know so they can decide to answer or not answer a call

RTMC has contracted with Ribbon Communications and Cordell/Nex-Tech to provide robocall analytics of its network's outbound traffic. The vendor's analytics identify patterns of suspected illegal robocalls based on their behavior and/or their status as suspected robocalls as reported to the Federal Communications Commission (FCC), Federal Trade Commission (FTC), and as reported by other carriers. The Cordell/Nex-Tech software is integrated with RTMC's Ribbon Call History server that collects the incoming and outgoing call data. RTMC receives daily email reports about telephone numbers originating from suspected illegal robocalls on its network, including from unassigned, inactive, and do-not-originate TNs. RTMC also receives email notifications if any of its numbers experience a change in reputation, such as suspicious traffic patterns or other detected anomalies outside the normal behaviour of its company's traffic. RTMC will examine the reports, investigate, and identify the source of the calls as unlawful or legitimate.

RTMC monitors all originating network traffic using the Cordell/Nex-Tech software for suspicious or abnormal call volume or activity. Calls that meet the following qualifying factors are investigated internally to determine if the calls are legitimate or unlawful:

- High-volume voice network traffic
- Large bursts of calls in a short timeframe
- Short-duration calls
- Low average call duration
- Low call completion ratios
- Sequential dialing patterns
- Neighbor spoofing patterns

Traceback

RTMC is committed to cooperating and responding within 24 hours to the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls.

Customer Vetting

RTMC has procedures in place to prevent new & renewing customers from using its network to originate illegal robocalls. RTMC thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Enforcement

If it is determined that a RTMC customer is originating prohibited, unlawful robocalls on our network, RTMC will notify the customer of the unlawful robocalls and work with them to resolve the issue.

RTMC has also implemented Innovative Systems Terminating Call Manager service for incoming calls on its SIP trunk groups to block known fraudulent telemarketer calls. The majority of these fraudulent calls originate from the 876 area code. These calls are challenged and are able to press 1 to state they are not a telemarketer, which adds them to the allowed list.

RTMC has implemented the Ribbon Call Trust Reputation Scoring service on all TDM trunks to mitigate any robocalls originating and terminating on it's network.