GET THE FACTS

FCC ROBOCALL MITIGATION DATABASE MYTHS

The Federal Communications Commission (FCC) is very serious about stopping illegal robocalls. As of September 28, 2021, Communications Service Providers (CSPs) must refuse to accept traffic from voice service providers not listed in the Robocall Mitigation Database (RMDB).

Despite the mandate for CSPs to certify what actions they've taken regarding STIR/SHAKEN and robocall mitigation in the RMDB, the ability to identify and block calls from carriers who have not registered in the database will be very difficult.

While carriers receiving the call must validate, in real-time, that the carrier that sent them the call is registered in the RMDB, the proper routing identifiers (i.e., Operating Company Number (OCN)) are not actually listed in the database.

Below are some RMDB myths we've debunked, and actions you can take to ensure compliance despite the limitations.

> "To succeed, we not only need an all hands-on-deck response from government, but we need industry commitment and focus. Our message to providers is clear: certify under penalty of perjury the steps you are taking to stop illegal robocalls, or we will block your calls."
>
> *- Federal Communications Commission (FCC)*

MYTH	FACT
A carrier should block all traffic from other carriers that have not fully implemented STIR/SHAKEN.	The FCC mandate states all intermediate providers and terminating voice service providers must refuse to accept traffic from carriers that not listed in the Robocall Mitigation Database. Carriers may choose to apply call treatment to traffic not signed with STIR/SHAKEN, but not required due to this regulation. In addition, many carriers received an extension to implement STIR/SHAKEN. They instead implemented a robocall mitigation program and registered in the database. **Bottom line: If a carrier is registered in the RMDB, other carriers do not need to block their traffic, regardless of what they have implemented.** Read the eBook: STIR/SHAKEN FAQs for CSPs.

neustar

MYTH	FACT
If a carrier is registered in the RMDB, their calls can be trusted.	Calls from carriers listed in the RMDB can still be illegal robocalls or spoofed. The database ensures there is a way to track participation and what robocall mitigation measures each carrier has implemented. **Bottom line: The robocall mitigation analytics policies of the terminating carriers (or in some cases contact centers or enterprises) will ultimately determine final call treatment based upon a multitude of factors.** Learn about Neustar's Robocall Mitigation solutions.
RMDB data is static – download the information once and I'm done?	There are over 5,000 carriers, and their status is changing frequently, so it's best to use real-time data service to ensure it remains current. Not doing so can result in your customers' traffic inadvertently being blocked. **Bottom line: Regulations keep changing, and it's important to keep up with the latest FCC reports and orders, so you stay compliant.** Read the eBook: Robocall Mitigation FAQs for CSPs.
Can a carrier just look at the interconnects where they receive traffic?	Yes, but the carrier receiving the call must first validate that the service provider from whom they received the call is registered in the database. Then, be sure to perform a thorough review of interconnects that are often overlooked. Matching these names to the RMDB is challenging because the consolidation in the industry has resulted in name changes. **Bottom line: To ensure carriers are accounting for all traffic, review all wholesale and enterprise customers (including contact centers, international carriers) interconnects.** Read the eBook: Crossing the Finish Line: Four Steps to STIR/SHAKEN Robocall Compliance for Small- to Mid- Sized Carriers.

Neustar is a pioneer in call authentication. As the co-author of STIR standards and early contributor to the SHAKEN framework, we play an ongoing leadership role in defining industry standards with ATIS, IETF, and CRTC. We provide the industry's reference implementation of STIR/SHAKEN as the exclusive operator of the ATIS Robocalling Testbed, where real world STIR/SHAKEN implementations are being tested for interoperability, and Neustar leads the industry in commercial call authentication deployments. Visit our STIR/SHAKEN Resource Hub to learn about insights, resources, and solutions. And learn how you can implement robocall mitigation solutions today.

Contact us at callerid@team.neustar

neustar