FCC Removes Non-Compliant Providers from the Robocall Mitigation Database

Action Immediately Prevents Providers with Certification Deficiencies from Connecting with U.S. Networks

WASHINGTON, August 6, 2025—Today, as part of the agency's efforts to safeguard Americans from illegal robocalls, the Federal Communications Commission's Enforcement Bureau removed 185 non-compliant voice service providers from the Robocall Mitigation Database. This will prevent those providers from connecting to U.S. networks until they comply with FCC regulations. All removed providers violated Commission rules by maintaining deficient certifications after repeated warnings and apparently participating in illegal robocall campaigns or failing to support official efforts to investigate such campaigns. The agency also reminded all providers of the importance of complete and accurate Robocall Mitigation Database certifications, which are essential to ensuring transparency and accountability in the fight against illegal robocalls.

Chairman Brendan Carr issued the following statement:

"The FCC is engaged in a comprehensive effort to combat the scourge of illegal robocalls. That includes preventing providers from connecting to our networks if they fail to meet their regulatory obligations. The FCC expects every provider to do its part to protect Americans from these scammers."

Additional Background:

In December 2024, the Commission ordered 2,411 providers to cure their deficient filings or provide a reason why they should not be removed from the Robocall Mitigation Database. Today's action removes 185 of these providers from the Robocall Mitigation Database. Removed providers will only be permitted to refile in the database with express approval from the FCC's Enforcement and Wireline Competition Bureaus.

The FCC's Robocall Mitigation Database was established to promote transparency and effective robocall mitigation. Providers are required to certify that all the calls that they originate on their networks are subject to a robocall mitigation program. Further, they must certify that they have implemented the STIR/SHAKEN framework of caller ID authentication on all IP-based portions of their networks. In addition to implementing STIR/SHAKEN, all providers must submit robocall mitigation plans. Failure to meet these obligations may result in removal from the database and blocking of the provider's traffic.

###

Media Contact: MediaRelations@fcc.gov / (202) 418-0500
@FCC / www.fcc.gov