

Contents of the Robocall Mitigation Program Description

A. Role in Call Chain & STIR/SHAKEN Status

Voice Service Providers must specify if they have:

- Fully implemented STIR/SHAKEN across the entire network,
- Partially implemented it on a portion of their network,
- Not implemented it at all.

They must also include the type of extension(s) received under § 64.6304 or explain why implementation isn't feasible due to lack of control over the necessary infrastructure. [eCFR Federal Register](#)

Gateway and **non-gateway intermediate providers** must similarly state their STIR/SHAKEN implementation status in the applicable context of calls carried or processed. [eCFR Federal Register](#)

B. Reasonable Steps to Avoid Illegal Robocall Traffic

All provider types must describe the **reasonable steps** they take to avoid originating, carrying, or processing illegal robocall traffic. This includes:

- **Know-Your-Customer / Know-Your-Upstream-Provider Procedures**
 - Voice service providers must comply with § 64.1200(n)(4).
 - Gateway and intermediate providers must comply with § 64.1200(n)(5).
[eCFR Federal Register](#)
- **Analytics Systems**
 - Describe any call analytics or monitoring systems used to detect suspicious or illegal calls, including whether any third-party vendor is used, and if so, provide the vendor's name(s). [eCFR TransNexus Federal Register](#)

C. Traceback Commitments

All providers must explicitly commit to:

- Respond **fully and within 24 hours** to any traceback requests from the FCC, law enforcement, or the Industry Traceback Consortium.
- Cooperate with these entities in investigating and stopping illegal robocallers.
[eCFR GovInfo](#)

D. Enforcement History / Ongoing Investigations

Providers must state whether, in the **past two years**, they—or any entity under shared ownership or control—have been subject to a formal Commission, law enforcement, or regulatory action or investigation involving illegal robocalls or spoofing, or regarding a deficient RMD certification or mitigation plan. If yes, they must provide:

- Name(s) of the agencies,
- Date action/investigation commenced,
- Current status,
- Summary of findings,
- Whether any final determinations were issued. [eCFR Federal Register](#)

E. Supporting Administrative & Identity Information

When uploading the RMPD (PDF) and certification in the RMD portal, providers must also supply (per DA 24-73 and § 64.6305):

- Legal business name(s), current and previously used names.
- Whether the provider is a foreign voice service provider (if applicable).
- Role(s) in the call chain (voice service, gateway, intermediate).
- Whether they are eligible for extensions or exemptions from STIR/SHAKEN.
- Company principal, affiliates, parent companies (as applicable). [Federal Register+1TransNexus](#)

Also required in the portal:

- Name, title, department, business address, phone, and email of the designated robocall mitigation point of contact.
- Operating Company Number (OCN), if applicable. [Federal Register+1](#)

F. Confidential and Redacted Submission Options

If certain parts of the mitigation plan are sensitive, the provider may submit both **unredacted (confidential)** and **redacted (public)** versions under the protective order guidelines adopted for RMD filings.