

Overview

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. In the previous order, the FCC required voice service providers to implement STIR/SHAKEN within the IP portions of their network prior to June 30, 2023 as required by 47 CFR 64.6304(a)(1).

Those not yet compliant must implement and certify the implementation of a Robocall Mitigation Plan to ensure that this illegal traffic does not originate on their networks as they work within the industry to become fully compliant.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that:

- Details the reasonable steps taken to avoid originating illegal robocalls;
- Demonstrates a commitment to respond to traceback requests.
- To cooperate with investigating and stopping illegal robocalls; and
- Is filed in the Robocall Mitigation Database.

In the *Sixth Caller ID Authentication Report and Order*, The FCC expanded the robocall mitigation database (RMD) filing requirements to include:

- Non-gateway intermediate providers and voice services providers to meet the same reasonable steps – general mitigation requirements outlined above.
- Providers' programs must also commit to respond fully, within 24 hours, to all traceback requests.
- The role the provider is playing in the call path.
- Detailed information supporting any extension or exemptions.
- Information regarding their principals, affiliates, subsidiaries, and parent companies.
- A statement whether they are subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing and provide information concerning any such actions or investigations.
- Voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls.
- non-gateway intermediate providers and voice service providers must, like gateway providers, describe any "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls.
- Providers must describe any call analytics systems they use to identify and block illegal traffic.

I. Description of Robocall Mitigation Program

As part of our company's and affiliates submission to the Robocall Mitigation Database, this document describes (1) the specific reasonable steps the provider has taken to avoid originating illegal robocall traffic as part of its Robocall Mitigation Plan, and (2) its commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

II. Entities Covered By Certification

The following entities are all subject to the robocall mitigation policies and procedures described in this document. As part of the expanded requirements, each's OCN and role is provided in the table below:

Company	OCN	Role
Cross Telephone Company, L.L.C.	1985	Voice Service Provider (VSP)
Cimarron Telephone Company, L.L.C.	1982	Voice Service Provider (VSP)
The Pottawatomie Telephone Co., L.L.C.	2020	Voice Service Provider (VSP)
Cross Cable Television, L.L.C.	809H	Voice Service Provider (VSP)
Cross Wireless, L.L.C. d/b/a Bravado Wireless	148G	Voice Service Provider (VSP)
Cross Valliant Cellular Partnership	387E	Voice Service Provider (VSP)
Cim Tel Cable, L.L.C.	N/A	Affiliate – Non-Voice Service Provider (Included for Ownership Disclosure Only)
MBO Video, LLC d/b/a MBO Networks	N/A	Affiliate – Non-Voice Service Provider (Included for Ownership Disclosure Only)
OpticTel Long Distance, L.L.C.	N/A	Non-Gateway Intermediate Provider

The providers are directly or indirectly owned by Cross Telephone Company, L.L.C. ("Cross") and / or MBO, L.L.C. ("MBO") and, when aggregated together, have fewer than 100,000 voice service subscriber lines. Both Cross and MBO and affiliated providers are subject to the same Robocall Mitigation Plan. For the purpose of this document, these entities are collectively referred to as "provider".

III. Efforts to Avoid Originating Illegal Robocalls as Part of the Robocall Mitigation Program

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

IV. Non-Gateway Intermediate Provider

[REDACTED]
[REDACTED]. The provider utilizes common equipment described within this mitigation plan. The intermediate carriers' customers are customers within the providers networks who select the intermediate carrier as their long-distance carrier. Our intermediate carriers' upstream customers are the voice service providers and their end user.

V. Traceback and Enforcement Cooperation

Provider will actively cooperate with the traceback community, the Industry Traceback Group ("ITG"), law enforcement requests, and the Commission to investigate and stop illegal robocalls. Provider will dedicate sufficient resources to provide prompt and complete responses to traceback requests within 24 hours of receiving the request.

VI. Stir/Shaken Development and Implementation

Provider has purchased the necessary hardware and applications for implementing a centralized policy and routing solution to interoperate with our Border Gate Control Function (BGCF), Session Border Controllers (SBCs), and Gateways. Our providers originate traffic using traditional telephony methods where services are installed and originate from a physical location. Calls are converted to "IP transport" for outbound terminations to intermediate carriers (toll providers); and are signed using [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] These products allow calls originating from within our network to be signed as they egress towards the IP enabled intermediate carriers.

The policy routing solution acts as a broker and is part of our call trust and validation network, which utilizes reputation scoring from third party identity and resource hubs. [REDACTED]

VII. Regulatory Action Affirmation

No providers or affiliates listed in this plan are subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing and provide information concerning any such actions or investigations.

VIII. Annual Certification and CORES Compliance

The provider hereby **annually recertifies** that the information contained in this Robocall Mitigation Plan and its associated Robocall Mitigation Database filing is **true, accurate, and complete** as of the date of submission. The provider certifies that all calls originated, carried, or processed on its network are subject to a robocall mitigation program that meets the requirements of **47 C.F.R. § 64.6305**, and that no prior certification has been removed by Commission action nor has the provider been prohibited from filing in the Robocall Mitigation Database.

The provider certifies that all information associated with its **Commission Registration System (CORES)** record is **accurate and current**. The provider further commits to updating any changes to its CORES information, including but not limited to ownership, contact information, or corporate relationships, **within ten (10) business days** of such change, in accordance with applicable Commission rules.