



Robocall Mitigation Plan



Pursuant to 47 C.F.R. § 64.6305 Flyp Marketing LLC submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. As of April 1, 2024 Flyp Marketing LLC is fully stir shaken certified, this report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Flyp Marketing LLC has in place to mitigate illegal robocalls as of September 1, 2024. Flyp Marketing LLC may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

Flyp Marketing LLC has fewer than 100,000 subscribers and is therefore eligible for the STIR/SHAKEN implementation exemption for small carriers under 47 CFR § 64.6304. The company requires this extension to complete the implementation of the STIR/SHAKEN technology. Flyp Marketing LLC is judiciously working to prevent unlawful robocalls from originating on its network while in the process of installing the new STIR/SHAKEN authentication architecture. In the meantime, Flyp Marketing LLC has implemented the following robocall mitigation plan to address unlawful robocall traffic:

Flyp Marketing LLC has enforceable terms of use and/or an acceptable use policies noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. Prior to installing services for new customers, the company takes the following measures to weed out end users that could potentially generate robocall traffic:

The Company confirms the following information for its customers:

Customer's identity

Customer's right to use the telephone number presented on calls

Service Address

Credit History

When the customer is a business, Flyp Marketing LLC also requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

Flyp Marketing LLC has established methods and procedures to monitor its network and detect / prevent fraudulent activity. The company uses call authentication, call labeling, and call blocking services to protect its networks and consumers from harmful calls. It also uses software to monitor its network's daily usage and has established methods and procedures in place to address issues as soon as they are identified.

Flyp Marketing LLC will comply fully with all conditions set forth in the FCC'S 2024 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

Flyp Marketing LLC has designated an individual as a dedicated point of contact for addressing traceback requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See

<https://www.ustelecom.org/the-industry-rollback-group-itg/for-providers/>.

Flyp Marketing LLC will respond promptly to inquiries from the Industry Rollback Group (ITG). If a pattern of questionable activity is detected Flyp Marketing LLC will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated. Requests from the ITG must be submitted in writing and include the following information:

Company Name:

Company Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

Flyp Marketing LLC will cooperate with state and federal regulators to prevent any and all illegal robocalls. Requests from the valid agency must be submitted in writing and include the following information:

Law Enforcement Agency Name:

Agency Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

Flyp Marketing LLC will provide valid law enforcement and regulatory agencies with the relevant nonproprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.