

ROBOCALL MITIGATION PROGRAM

IFR Technologies LLC

Filed pursuant to 47 C.F.R. § 64.6305

Effective date: **June 1st, 2026**

1. Provider Overview and Role in the Call Chain

IFR Technologies LLC (“IFR”) is a provider of interconnected Voice over Internet Protocol (VoIP) voice service. IFR furnishes voice service to a limited base of contracted business customers, which use the service for their own business communications.

IFR does not own or operate facilities that originate or terminate calls on the public switched telephone network (PSTN). All origination and termination of PSTN traffic is performed by IFR’s upstream, facilities-based carriers. For purposes of the Robocall Mitigation Database, IFR is a voice service provider without a STIR/SHAKEN implementation obligation.

2. STIR/SHAKEN Implementation Status and Basis for Exemption

IFR has not implemented the STIR/SHAKEN caller ID authentication framework on any portion of its network. IFR is exempt from the STIR/SHAKEN implementation obligation under 47 C.F.R. § 64.6305(d)(2)(i) because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN.

Specifically, IFR does not own or control the switching or interconnection points at which calls are originated onto the PSTN; those points are owned and operated by IFR’s upstream carriers. The telephone numbers IFR uses to provide service are assigned to and administered by those upstream carriers under their respective Operating Company Numbers; IFR does not obtain numbering resources directly from the North American Numbering Plan and holds no Operating Company Number, Service Provider Code (SPC) token, or STIR/SHAKEN certificate of its own. Because STIR/SHAKEN signing occurs at the originating carrier’s network edge, IFR has no technical ability to authenticate calls with its own certificate. IFR’s upstream carriers implement STIR/SHAKEN and authenticate the caller ID information for calls they originate on IFR’s behalf.

3. Reasonable Steps to Prevent Origination of Illegal Robocalls

IFR maintains the following affirmative measures to prevent its network and its customers from being used to originate illegal robocall traffic. These measures are applied to both new and renewing customers.

3.1 Customer Vetting and Know-Your-Customer (KYC)

IFR does not offer anonymous or self-service account provisioning. Every customer is on-boarded only under a written service agreement, and before activation IFR verifies the customer’s business identity and the legitimate nature of its business. IFR retains this identifying information for the duration of the customer relationship and re-verifies it upon any material change in the customer’s identity, ownership, or use of the service, consistent with its obligation to know its customers under 47 C.F.R. § 64.1200(n)(4).

3.2 Acceptable Use Requirements and Contractual Controls

IFR's written service agreements expressly prohibit use of the service to originate unlawful robocalls, to transmit inaccurate or unlawfully spoofed caller ID information, and to place calls in violation of the Telephone Consumer Protection Act, the Truth in Caller ID Act, or other applicable law. The agreements require that the service be used solely in connection with the customer's own legitimate business operations and prohibit resale or transfer of the service to third parties. IFR reserves, and exercises, the contractual right to suspend or terminate service immediately upon identifying a violation.

3.3 Customer Base and Traffic Profile

IFR's traffic profile is low-risk for illegal robocalling. IFR does not provide service to telemarketers, lead-generators, survey or polling operations, or high-volume automated-dialing customers. Outbound traffic consists of business calls placed by, or on behalf of, the customer's own enterprise. This narrow, known customer base materially reduces the risk that IFR's service could be used to originate illegal robocall campaigns.

3.4 Traffic Monitoring and Analytics

IFR monitors call detail records and traffic patterns for anomalies indicative of illegal or fraudulent calling. IFR additionally relies on the network-level fraud- and robocall-detection systems maintained by its upstream carriers, which apply analytics and traffic controls to traffic they originate and which notify IFR of suspected illegal or anomalous traffic.

3.5 Telephone Number Provisioning Controls

Telephone numbers are obtained from IFR's upstream carriers and are assigned only to vetted, contracted customers for use in their own operations. IFR does not maintain shared or anonymous number pools available for high-volume or automated dialing, and does not permit customers to originate calls using telephone numbers they are not authorized to use.

4. Know-Your-Upstream-Provider Procedures

IFR originates and terminates PSTN traffic exclusively through established, facilities-based carriers that are registered with the FCC and that maintain active filings in the Robocall Mitigation Database. These carriers implement STIR/SHAKEN and sign traffic they originate. IFR confirms that its upstream carriers are listed in the Robocall Mitigation Database and does not originate or accept traffic through providers that are not properly listed in the Database.

5. Response to Traceback Requests

IFR commits to respond fully and within 24 hours to all traceback requests it receives from the Federal Communications Commission, law enforcement, and the industry traceback consortium (the USTelecom Industry Traceback Group), and to cooperate with those entities in investigating and stopping any illegal robocaller that may use IFR's service to originate calls. Upon receipt of a traceback request, IFR will identify the originating customer associated with the identified traffic and take appropriate mitigation action as described in Section 6.

6. Mitigation and Enforcement Actions

Upon identifying, or receiving notice of, illegal robocall traffic originating from a customer, IFR will promptly investigate, notify and where appropriate require corrective action from the customer, and suspend or terminate the offending customer's service as warranted. IFR will coordinate with its upstream carriers to block or otherwise mitigate identified illegal traffic. IFR applies these measures to prevent both new and renewing customers from using the service to originate illegal calls, and will decline to onboard, or will discontinue service to, any customer that IFR determines presents an unacceptable risk of originating illegal robocall traffic.

7. Recordkeeping and Filing Maintenance

IFR maintains records of its customer vetting, traceback responses, and mitigation actions. IFR will update its certification and this Robocall Mitigation Program in the Robocall Mitigation Database within 10 business days of any material change to the information required under 47 C.F.R. § 64.6305, including any change to its role in the call chain, its STIR/SHAKEN implementation status, its corporate or contact information, or its upstream carrier relationships. IFR will recertify its filing during the annual recertification window as required by the Commission's rules.

8. Designated Contact for Robocall Mitigation

The individual within IFR Technologies LLC responsible for addressing robocall-mitigation-related issues, including traceback requests, is:

Eric Jiang

System Engineer

IFR Technologies LLC

16 Middle Neck Rd, Great Neck, NY 11021

legal@ifrtech.net