

IFN, LLC (hereinafter "IFN" or "Company") hereby submits this Robocall Mitigation Plan to the Federal Communications Commission ("FCC") pursuant to the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act and 47 CFR Part 64, Subpart Z.

1. Know Your Customer (KYC)

IFN does not offer online signup, self-provisioning, or automated customer onboarding of any kind. All prospective customers are screened by senior staff prior to acceptance. IFN's standard onboarding process includes in-person or on-site visits with prospective customers to verify the nature and legality of their business operations before any service is provisioned. IFN further collects and retains customer legal identification, business registration documentation, and references as part of the KYC process. Foreign providers, if any, are subject to the same or heightened scrutiny to ensure IFN's network is not used to carry illegal traffic originating from outside the United States.

IFN's small customer base makes comprehensive individual review operationally feasible, and this human-intensive approach is a core element of IFN's mitigation strategy.

2. Contractual Prohibitions

All IFN customers are subject to contractual terms that strictly prohibit the origination of robocalls of any kind — including calls that may be technically lawful under other regulatory schemes — from IFN's network. Violations of this prohibition result in immediate service termination without prior warning. IFN retains the right to terminate service based on reasonable suspicion of noncompliance, independent of any confirmed legal violation.

3. Network Security and Technical Controls

IFN maintains up-to-date software and firmware across its VoIP infrastructure, enforces strong credential management practices, and implements access controls to prevent unauthorized call injection by non-customers. When IFN identifies fraudulent, abusive, or anomalous traffic, it may take the following actions, as appropriate:

- Blocking or rejecting traffic using appropriate Session Initiation Protocol (SIP) response codes
 - Blacklisting known abusive numbers or originating endpoints
 - Suspending or terminating service to the offending customer
 - Reporting the activity to the ITG, FCC, or law enforcement as applicable
-

4. Traffic Monitoring

IFN personnel actively monitor network usage patterns for anomalies indicative of robocall traffic, including unusual call volumes, calling number patterns, or traffic spikes inconsistent with known customer behavior. Given IFN's small customer base, this monitoring is conducted through direct human review on a frequent basis. Anomalies are investigated promptly and escalated when warranted.

5. STIR/SHAKEN

IFN has implemented the STIR/SHAKEN call authentication framework and has engaged an STI-Certificate Authority (STI-CA) service provider. IFN ensures that only vetted and approved customers are authorized to sign calls, and that calls are signed exclusively with certificates issued at the national level through the STI-Policy Administrator (STI-PA).

6. Traceback Cooperation

IFN commits to fully cooperating with the USTelecom Industry Traceback Group (ITG) and will respond to all traceback requests within 24 hours of receipt. IFN will cooperate with the ITG, the FCC, and law enforcement agencies to investigate and stop illegal robocallers from utilizing IFN's network. IFN will take all steps necessary to avoid designation as a Non-Cooperative Voice Service Provider as defined by ITG Policies and Procedures.

When notified by the FCC's Enforcement Bureau of identified illegal traffic, IFN will block and report that traffic and any substantially similar traffic on an ongoing basis, unless IFN's own investigation determines the traffic is not illegal. In such cases, IFN will provide the FCC Enforcement Bureau with a written explanation of its determination and the steps taken to reach that conclusion.

7. Do Not Originate (DNO)

IFN implements Do Not Originate (DNO) procedures upon request from governmental agencies acting through USTelecom or the FCC. IFN will block traffic associated with numbers appearing on DNO lists and will report any blocked traffic as required. IFN also utilizes the Reassigned Numbers Database (RND) to verify whether a US geographic or toll-free telephone number has been permanently disconnected, as an additional fraud prevention measure.

8. Summary

IFN's robocall mitigation approach is built on four pillars: (1) a rigorous, in-person Know Your Customer process that prevents bad actors from accessing the network in the first place; (2) strict contractual prohibitions with immediate termination provisions; (3) technical security controls and active human traffic monitoring; and (4) full cooperation with FCC, ITG, and law enforcement traceback and enforcement efforts. IFN is committed to maintaining and improving these practices as regulatory requirements and industry standards evolve.