

Introduction

Fullnet Advanced Communications, Inc. (“FNACI”) is a non-facilities-based Telecommunications and VoIP service provider serving fewer than 100,000 voice subscriber lines. FNACI has fully implemented STIR/SHAKEN on all Internet Protocol (IP) portions of its network and signs all outgoing calls originated by its customers using its own certificate obtained from PeeringHub.

This Robocall Mitigation Plan describes the specific, reasonable steps FNACI takes — based on its role as an originating Voice Service Provider serving only verified end-user business customers — to prevent the origination of illegal robocalls. These measures can reasonably be expected to significantly reduce illegal robocall traffic. FNACI continuously monitors traffic, verifies customers, signs all calls, and fully cooperates with traceback efforts.

STIR/SHAKEN Implementation

FNACI has implemented STIR/SHAKEN across its entire originating network. All outbound calls are authenticated using a valid STIR/SHAKEN certificate obtained from PeeringHub. We assign the highest appropriate attestation level (typically Full A-level for our verified business customers) based on KYC verification of the calling party. This cryptographic authentication prevents spoofing and supports downstream labeling/blocking of any unsigned or improperly attested traffic.

Know Your Customer (KYC) Policy

At FNACI, our commitment to maintaining the integrity of our communications network and services is paramount. In alignment with this commitment, we have instituted a robust “Know Your Customer” (KYC) policy designed to verify the identities and operational legitimacy of all our clients. This policy is a cornerstone of our efforts to mitigate robocall activities and ensure compliance with all applicable regulations, including those mandated by the Federal Communications Commission (FCC).

Customer Onboarding and Verification

1. **Established Business Relationships:** We exclusively serve customers that are established businesses within our area and its surrounding regions. Our clientele encompasses a diverse range of sectors, underscoring our role as a trusted partner in the business community.
2. **Manual Account Setup:** To ensure the utmost accuracy and security, all customer accounts are set up manually by our dedicated employees. This hands-on approach allows us to conduct thorough due diligence and establish a personal connection with each customer.

3. **Business Verification:** Prior to account activation, we conduct a comprehensive verification process. This includes, but is not limited to, validating the business's registration details, physical location, and operational status through publicly available records and, when necessary, direct contact.
4. **No Automatic Sign-Ups:** We do not employ automatic or automated sign-up procedures, thereby eliminating the risk of fraudulent account creation. Each potential customer undergoes a personalized assessment to ensure alignment with our service criteria and regulatory obligations.
5. **End-User Sales:** Our services are tailored exclusively for end users, ensuring that the communication solutions we provide are directly utilized by the businesses themselves. This direct-to-user model allows for greater control and monitoring of service usage, aligning with best practices for robocall mitigation.
6. **Business-Centric Customer Base:** Approximately 99% of our clientele are businesses, reinforcing our specialized focus on serving the professional community. This business-centric approach further supports our commitment to maintaining a secure and compliant communication environment.

Continuous Monitoring and Compliance

Our KYC policy extends beyond initial customer onboarding. We continuously monitor account activity to ensure ongoing compliance with our standards and regulatory requirements. Any anomalies or suspicious activities are promptly investigated, and appropriate actions are taken to maintain the integrity of our services and protect our network from misuse.

In conclusion, FNACI's KYC policy is designed to foster a secure, reliable, and compliant telecommunications environment. By rigorously verifying our customers and maintaining a direct relationship with each, we uphold our responsibility to combat robocall proliferation and ensure the trustworthiness of communications facilitated through our network.

Traffic Monitoring and Call Analytics

FNACI utilizes Zabbix, an enterprise-grade monitoring platform, to detect anomalous traffic patterns indicative of illegal robocalls. Zabbix continuously monitors call volume on all customer trunks every minute against customer-specific normal usage baselines.

When call volume exceeds normal thresholds, staff receive immediate alerts via push notifications and email. Call Detail Records (CDRs) are then reviewed promptly to confirm the nature of the traffic.

Mitigation Actions Upon Detection

Upon receiving a Zabbix alert:

1. On-duty technical staff review the traffic within minutes.

2. The customer is contacted to verify legitimate business use.
3. If the traffic is confirmed or reasonably suspected to be illegal robocalling or in violation of our Acceptable Use Policy, FNACI immediately blocks the offending traffic, suspends the account, and/or terminates service as appropriate.

All customer agreements explicitly prohibit the origination of illegal robocalls or spoofed traffic and grant FNACI the right to suspend or terminate service immediately upon violation, with no liability to FNACI.

Know Your Upstream Providers

As a non-facilities-based provider, FNACI routes all originated traffic through vetted upstream termination providers: Sinch/Inteliquent (approximately 99% of outbound traffic), Bandwidth.com, and Telnyx.

We maintain active contracts with each provider requiring them to (1) maintain a valid RMD filing, (2) implement effective robocall mitigation, and (3) cooperate with traceback requests. We review each upstream provider's RMD status quarterly and monitor traffic patterns on our side for anomalies. We will immediately cease routing to any upstream provider whose RMD certification is removed or whose traffic shows repeated suspicious patterns.

Traceback Cooperation Policy

FNACI fully commits to cooperating with regulatory bodies, law enforcement, the Industry Traceback Group (ITG), and other providers in traceback investigations. We designate **John Fullington** as the primary contact and **commit to responding fully to all traceback requests within 24 hours** of receipt, providing all requested call detail records, customer information, and other data necessary to trace the origin of suspect calls.

At FNACI, we recognize the critical importance of addressing the challenge of unauthorized robocalls within the telecommunications ecosystem. In our ongoing efforts to safeguard the integrity of our network and protect our customers, we have established a comprehensive Traceback Cooperation Policy.

Active Engagement in Traceback Initiatives

1. **Collaboration with Authorities:** FNACI is fully committed to cooperating with regulatory bodies, law enforcement agencies, and industry partners in traceback investigations. Our team responds fully within 24 hours to traceback requests, providing essential information and support to trace the origin of suspect calls traversing our network.
2. **Internal Traceback Capabilities:** We have developed robust internal mechanisms to facilitate efficient traceback of calls within our network. By leveraging advanced technology and analytics, we can swiftly identify the path and origin of a call, aiding in the rapid resolution of investigations.

3. **Transparency and Communication:** FNACI maintains an open line of communication with all stakeholders involved in a traceback investigation. We ensure that relevant information is shared in a timely and secure manner, respecting privacy and confidentiality requirements while supporting the overarching goal of robocall mitigation.
4. **Continuous Improvement:** Recognizing the evolving nature of telecommunications fraud, FNACI continuously enhances its traceback capabilities. We invest in ongoing training for our staff and upgrade our technological tools to stay ahead of emerging threats and tactics used by malicious actors.
5. **Regulatory Compliance:** Our Traceback Cooperation Policy is designed to align with the FCC's expectations and requirements for service providers in combating illegal robocalls. We stay abreast of regulatory developments and adjust our practices as necessary to remain in full compliance.
6. **Industry Collaboration:** FNACI actively participates in industry-wide efforts and forums dedicated to robocall mitigation. By sharing insights and best practices with peers, we contribute to a collective approach to addressing and reducing the impact of unwanted robocalls.

Commitment to Customer Trust

FNACI understands that trust is the foundation of our relationship with customers. By proactively engaging in traceback efforts and working collaboratively with industry and regulatory partners, we aim to maintain a secure and trustworthy communication environment. Our Traceback Cooperation Policy is a testament to our unwavering commitment to combating robocalls and upholding the highest standards of service and integrity.

Additional Required Disclosures

- **Role in the call chain:** Originating Voice Service Provider serving end-user business customers only.
- **Enforcement history:** To the best of our knowledge after reasonable inquiry, neither FNACI nor any affiliate has been the subject of any FCC or law enforcement action or investigation in the prior two years related to illegal robocalling, spoofing, or RMD deficiencies.
- **Contact for tracebacks and robocall mitigation issues:**
John Fullington
President/CTO
fje@fullnet.com
(812) 482-3642