

Call.Net, LLC
FRN: 0030241046
4330 219th St SE
Bothell, WA 98021

Federal Communications Commission
45 L Street NE
Washington, DC 20554

Subject: Updated Robocall Mitigation Plan and STIR/SHAKEN Certification

Dear Sir or Madam,

Call.Net, LLC (“Call.Net”) respectfully submits this updated Robocall Mitigation Plan and certification information in response to the Commission’s requests regarding the Company’s Robocall Mitigation Database (“RMD”) filing.

Call.Net currently operates as a Mobile Virtual Network Operator (“MVNO”) and reseller of wireless and interconnected voice services utilizing the network infrastructure of upstream providers, including AT&T and related carrier partners. Call.Net does not own or operate the underlying switching, SIP authentication, or IP network infrastructure necessary to independently implement STIR/SHAKEN authentication in the IP portions of the call path.

Accordingly, Call.Net relies on its upstream providers and carrier partners to perform STIR/SHAKEN authentication, call signing, and related network-level robocall mitigation functions consistent with applicable FCC requirements.

Call.Net remains committed to complying with all applicable FCC robocall mitigation obligations and to cooperating with the Commission, law enforcement agencies, the Industry Traceback Group (“ITG”), and upstream providers to prevent illegal robocalling activity.

Operational Status

Call.Net functions primarily as an MVNO and reseller utilizing upstream carrier infrastructure. Call.Net does not possess its own Operating Company Number (“OCN”), SPC token, or direct SIP authentication/signing infrastructure and therefore relies on upstream voice service providers and carrier partners to implement STIR/SHAKEN authentication on applicable traffic transmitted through the public switched telephone network.

Robocall Mitigation Measures

Know Your Customer (“KYC”) Procedures

Call.Net maintains customer onboarding and verification procedures intended to reduce the risk of illegal robocalling, spoofing, SIM abuse, and fraudulent telecommunications activity.

For individual consumer accounts, Call.Net collects identifying customer information during account activation, including:

- Customer name;
- Physical address;
- Billing information;
- Email address; and
- Telephone contact information.

Call.Net validates customer information through payment verification methods in Stripe, fraud screening measures, account authentication procedures, and review of account activity indicators.

For business or commercial accounts, Call.Net conducts enhanced due diligence procedures, including:

- Verification of business registration information;
- Review of intended service usage;
- Verification of authorized representatives;
- Review of publicly available business information and websites where available; and
- Evaluation of potential high-risk usage patterns.

Accounts associated with telemarketing, bulk outbound calling, auto-dialing activity, or elevated fraud indicators are subject to additional review, restrictions, denial of service, suspension, or termination.

Call.Net also applies its KYC and fraud mitigation procedures to existing customers where unusual activity, complaints, traceback requests, or changes in account risk profile are identified.

Know Your Upstream Providers

Call.Net currently relies on upstream carrier providers and related carrier ecosystem partners for network connectivity, call routing, STIR/SHAKEN implementation, and additional robocall mitigation support functions.

Call.Net maintains commercial relationships and operational coordination with upstream providers, including AT&T and related carrier partners, and relies upon such providers to:

- Implement STIR/SHAKEN authentication where applicable;
- Assist in identifying suspicious traffic patterns;
- Cooperate with traceback investigations; and
- Support industry robocall mitigation efforts.

Call.Net works with upstream providers to address suspicious traffic, investigate complaints, and take appropriate mitigation actions where necessary.

Traffic Monitoring and Analytics

Call.Net does not currently utilize any third-party analytics vendors to monitor, analyze, score, block, or identify illegal robocall traffic. Call.Net monitors customer usage activity and account behavior for indicators associated with potentially unlawful robocalling activity or fraudulent telecommunications usage.

Instead, Call.Net relies on a combination of:

- Unusually high outbound call volumes;
- High-volume short-duration calls;
- Sequential dialing patterns;
- SIM misuse;
- Traffic spikes inconsistent with ordinary consumer usage; and
- Abnormal account behavior or calling patterns.
- Internal account review procedures.
- Usage monitoring and review of CDRs (Call Detail Records).
- Notifications and alerts from upstream carriers and network providers.

Call.Net utilizes internal monitoring procedures and also relies upon analytics, monitoring systems, fraud detection tools, and mitigation assistance provided by upstream providers and carrier partners.

Fraud Prevention and Controls

Call.Net maintains procedures intended to detect and prevent fraudulent activity, including:

- SIM abuse detection;
- Review of unusual traffic spikes;
- Monitoring for suspicious calling patterns;
- Account verification procedures; and
- Restrictions on accounts demonstrating elevated fraud risk.

Where suspicious activity is identified, Call.Net:

- Contacts the customer for re-verification;
- Temporarily suspend outbound calling;
- Restrict services;
- Block traffic;
- Terminate accounts; and/or
- Coordinate mitigation efforts with upstream providers.

Acceptable Use Policy (“AUP”)

Call.Net maintains and enforces an Acceptable Use Policy prohibiting:

- Illegal robocalling;
- Caller ID spoofing;
- Fraudulent communications;
- Unlawful automated calling activity;
- Transmission of deceptive or unlawful traffic; and
- Any activity violating FCC or applicable federal or state telecommunications regulations.

Violations of the AUP may result in suspension or termination of services.

Traceback Cooperation

Call.Net cooperates fully with traceback requests and investigations conducted by:

- The Federal Communications Commission;
- Law enforcement agencies;
- The Industry Traceback Group (“ITG”); and
- Upstream providers.

Call.Net commits to responding promptly to traceback requests and maintaining records reasonably necessary to support traceback investigations and mitigation efforts.

Remediation Actions

If suspicious or potentially unlawful traffic is identified, Call.Net may take remediation actions including:

- Customer notification;
- Enhanced account verification;
- Traffic restrictions;
- Blocking suspicious traffic;
- Suspension or termination of services; and
- Coordination with upstream providers and relevant authorities.

Certification

I, Sasi Mandava, CEO of Call.Net, LLC, certify under penalty of perjury that the information contained herein is true and correct to the best of my knowledge and belief.

Call.Net is committed to complying with applicable FCC robocall mitigation rules and to cooperating fully with traceback investigations and industry mitigation efforts.

Respectfully submitted,

Sasi Mandava
CEO, Call.Net, LLC
425-979-9091
smandava@call.net