

**PACOPTIC NETWORKS, LLC
ROBOCALL MITIGATION PLAN
(2024 Update)**

I. Background

Under the authority Congress granted the Federal Communications Commission ("FCC" or "Commission") in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Commission has adopted rules requiring voice service providers, like PacOptic Networks, LLC ("PacOptic Networks"), to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks. 47 CFR § 64.6301.

The FCC requires that all voice service providers certify in the Commission's Robocall Mitigation Database whether they have implemented STIR/SHAKEN and have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks. The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can "reasonably be expected to significantly reduce the origination of illegal robocalls" and the voice service provider complies with the practices it describes in its filings.

PacOptic Networks is dedicated to stopping illegal calls from originating on its network and undertaking commercially reasonable efforts to monitor the calls coming into its network, consistent with FCC regulations and its "Best Practices" guidance.

II. STIR/SHAKEN Implementation

PacOptic has fully implemented the STIR/SHAKEN authentication framework across the entire IP portion of its network, and all calls it originates are compliant with § 64.6301(a)(1) and (2). This compliance is by virtue of PacOptic's underlying service providers being STIR/SHAKEN compliant within the IP portions of their networks.

The Company uses a third-party vendor/underlying carrier to sign its calls and does not have its own token. PacOptic does not allow its customers to spoof CallerID, so any outgoing CallerID can easily be traced back to PacOptic's customer.

The Company does not use a third-party call analytics vendor (not including analytics provided by its underlying service provider(s)).

III. PacOptic Networks' Know Your Customer ("KYC") Standards

PacOptic Networks is a voice service provider that focuses its business and operations on the termination of voice traffic to business customers that receive voice calls. As such, PacOptic originates very little, if any, traffic. PacOptic nevertheless submits this plan to articulate its policies that would apply in the event it serves customers that originate voice calls.

As part of its customer-on boarding process, PacOptic Networks undertakes various commercially

reasonable precautions to verify a given customer's identity as part of entering into a formal written agreement. All prospective customers participate in an in-person or telephonic enrollment process. PacOptic Networks investigates the prospective customer's background, such as checking for a company website, the amount of time the business has been open, and confirming their corporate status with the applicable State Secretary of State's office or website, along with other indications of a legal, operating business. Among other data points collected and, as appropriate, verified, as part of those processes PacOptic Networks gathers the following customer-identifying facts and circumstances:

- Customer business name,
- state or country of incorporation,
- physical business location,
- contact person(s),
- federal tax ID number, and
- FCC Filer ID.

PacOptic Networks' verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers and the Commission's Robocall Mitigation Database. PacOptic Networks also conducts, as applicable, credit checks and reviews references with a prospective customer's other carrier-suppliers. If PacOptic Networks contracts with a customer who originated traffic on its network, it would continue to conduct its preliminary vetting, and the prospective customer.

IV. PacOptic Networks' Acceptable Use Policy

As part of its customer-onboarding process, all new PacOptic Networks' customers will be required to contractually agree to various terms and conditions, including a commitment to comply with PacOptic Networks' Acceptable Use Policy (AUP). Among other things, this AUP prohibits using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading. It likewise prohibits using the services in any way that violates applicable laws, which in the robocall context includes the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations, or creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

PacOptic Networks' contracts with its customers would stipulate that PacOptic Networks is authorized to suspend and/or terminate all Services in the event of an AUP violation.

V. Telephone Number Authorization

With very limited exception, PacOptic Networks' end users can only use telephone numbers to which they have subscribed from PacOptic Networks, such that PacOptic Networks has a documented,

verified relationship between the end user and their telephone number(s) used to receive their calls. In the rare exception in which the PacOptic Networks end user is using numbers secured from a different service provider, PacOptic Networks documents and verifies the end user's right to use the associated phone number(s) from the unaffiliated provider(s).

VI. Proactive Network Monitoring

If PacOptic Networks detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, PacOptic Networks would take prompt action to identify the party that is using its network to carry these calls and take appropriate action. If PacOptic Networks detected suspected unlawful traffic is discovered, PacOptic Networks would block any further traffic from being carried associated with the Media IP address of that suspicious traffic.

VII. Commitment to Traceback Cooperation

PacOptic Networks commits to timely cooperating with and responding to Traceback requests from the ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas, and other valid legal processes. PacOptic Networks will dedicate sufficient resources to provide prompt and complete responses to such requests. PacOptic Networks will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.

VIII. Updating PacOptic's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), PacOptic will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

The Company's RMP continues to develop as the Company and the industry gain expertise and deploy new robocall mitigation strategies and will be supplemented in future updates.