

Ifonoclast, Inc. DBA Phonevite
Robocall Mitigation Plan
As of February 26, 2026

Ifonoclast, Inc DBA Phonevite (“Phonevite”) is dedicated to stopping illegal calls from originating on its network, and this document outlines Phonevite’s Robocall Mitigation plan in compliance with the requirement of the Federal Communications Commission (“FCC” or “Commission”) that all voice service providers certify, in the Commission’s Robocall Mitigation Database (“RMD”), whether they have implemented STIR/SHAKEN and that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks.

In the Commission’s *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (2023) (“R&O”), it is stated that all voice service providers (“VSPs”) must file robocall mitigation plans (“RMPs”) that, among other things, outline “reasonable steps” taken to avoid originating illegal robocalls.

In addition to the “reasonable steps,” the FCC requires that a RMP include:

- “know your customer” procedures;
- “know your upstream provider”;
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that an RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

As certified in the FCC’s Robocall Mitigation Database, Phonevite has fully implemented STIR/SHAKEN. In compliance with the R&O, Phonevite submits this RMP and certification.

Know Your Customer (“KYC”)

Phonevite is a voice broadcasting provider primarily servicing schools, non-profits, and community organizations. Phonevite is a small company, and we have a small number of customers. As a result, we know our customers and understand their use cases.

In order to sign up for the Phonevite service, users must provide their name and email address. Furthermore, to start using the service, they must verify their email address and Caller ID, and provide organizational information. The email address is verified via an emailed link and an authorization code or via email interaction with our customer support team. The Caller ID is verified via an automated phone call and a security code confirmation or via phone interaction with our customer support team. Users can also purchase Caller IDs directly from us. In addition, we collect information about the organization using our service, their use cases and estimated call volumes. Our service is prepaid and we only accept credit card and Paypal payments, which can include echeck payments. Purchase transactions are monitored closely and funds are released to the account based on matching credit card information, established good usage, IP address consistency, and other internal security measures.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls*, and *Call Authentication Trust Anchor*, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404 (2023), at ¶¶ 49-51, Phonevite provides the following information concerning its upstream voice service carriers.

Phonevite has master service agreements with its upstream providers and has received assurances in writing from their officials that they have, and will continue to, sign calls transmitted to Phonevite and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Phonevite. Phonevite and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Phonevite maintains an [AUP](#) that subscribers must agree to before being permitted to use its software and services. Among other things, the AUP prohibits:

- using, or attempting to use, the Phonevite Service to convey any information that may be considered unlawful, harassing, libelous, abusive, threatening, obscene, hateful, offensive, harmful, vulgar, distasteful, defamatory, indecent, objectionable, or invasive of another person's privacy or proprietary rights;
- violating Phonevite's Terms of Service, and all applicable local, national, and international laws and regulations;
- using, or attempting to use, the Phonevite Service to send junk messages, spam, or messages that are duplicative, unsolicited in nature;
- sending, or attempting to send, messages to emergency lines, to any health care facility or similar establishment, to numbers assigned to radio common carrier services or to any service for which the called party is charged for the call;
- transmitting, or attempting to transmit, any material that may infringe the contractual, fiduciary, intellectual property rights, or other rights of third parties, including trademark, copyright or the right of publicity;
- initiating unsolicited political text messages or prerecorded political calls using the Phonevite Service;
- using the Phonevite Service to initiate voice calls or email messages that contain a marketing or promotional purpose;
- using the Phonevite Service to initiate any calls, emails or text messages to recipients if the subscriber has obtained their contact information from a third-party list provider;
- using the Phonevite Service to initiate any text message, email or phone call to recipients unless the subscriber have received the necessary consent and provided any necessary disclosures;
- impersonating, or attempting to impersonate, any other person, falsify contact information, misrepresent a relationship with any person or entity, including misrepresenting a relationship with Phonevite, or otherwise attempt to misleading others as to the identity of the sender or the origin of a message; and
- misrepresenting one's identity while using the Phonevite Service.

Phonevite Proactive Monitoring and Fraud Prevention

Phonevite works to detect a calling pattern consistent with illegal robocalls. If such a call is detected, we will identify the party who is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

Phonevite has various monitoring and fraud prevention measures to analyze traffic on its network for potentially suspicious traffic patterns that are potentially linked to illegal robocalls or other potentially unlawful usage.

Phonevite also conducts continuous analyses of customer calling patterns, to detect any usage that could potentially be in violation of its terms of service or be illegal.

Phonevite uses Transnexus' and its own solutions for traffic analytics.

Phonevite's procedures include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

Phonevite has also enabled additional features that allow call recipients to place themselves on the calling party's internal Do-Not-Call ("DNC") list, as well as in an overall DNC list from the whole Phonevite service.

Phonevite Traceback Cooperation with the FCC

Phonevite is committed to providing timely cooperation with regard to responding to Traceback requests from the FCC Enforcement Bureau, 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.

Phonevite commits to responding to all traceback requests from the Commission, law enforcement, and the registered traceback consortium within 24 hours. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Phonevite will investigate suspicious activity found by its monitoring systems, user activity, user reporting or third parties and take appropriate action. In addition, Phonevite has these

procedures in place to cooperate with any Traceback requests and to take appropriate actions as needed:

- As soon as a Traceback request is received from the FCC, Phonevite will investigate the call/s in concern, and contact the user, if needed or appropriate, to determine the nature of the call/s and whether they are in violation of Phonevite's Terms of Service (<https://phonevite.com/company/terms/>) and/or illegal in any other way. Phonevite will provide a response with an update to the ITG within 24 hours of the Traceback request.
- Upon determination of suspicious activity, Phonevite will immediately suspend the account.
- If and when a user is contacted and Phonevite does not receive a response within 12 hours of contacting the user, Phonevite will terminate the account permanently.
- If, based on the investigation of the calls, with or without contact with the user, Phonevite determines that the calls are in violation of its Terms of Service and/or illegal in any other way, Phonevite will terminate the account.

Phonevite Security Measures

Phonevite practices the following security measures, in addition to other proprietary processes, to safeguard the proper and legal usage of the Phonevite Service:

- US Service and Canada only: Our service is restricted to originating and receiving calls exclusively with telephone numbers based in the United States and Canada
- Phone Number Verification Requirement: each Caller ID that is used in Phonevite must be properly verified through an automated call and PIN verification, or through a direct call from or to our customer support staff
- Organizational Information reviewed and verified. No purchases allowed from new users without proper organizational information provided.
- Purchase Transaction Approval: Initial purchases are manually verified and approved to avoid fraudulent, illegal usage

Certification of John Nahm

I, John Nahm, CEO of Ifonoclast, Inc. DBA Phonevite, do hereby certify, under penalty of perjury, the following:

- (1) Phonevite has fully implemented STIR/SHAKEN in the IP portions of its network.
- (1) Phonevite's Business name and primary address are as follows:

Ifonoclast, Inc. DBA Phonevite
39899 Balentine Dr Suite 200
Newark, CA 94560
- (2) Phonevite uses the business names "Phonevite."
- (3) Phonevite has not previously used any other business name.
- (4) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (5) The following persons/entities own more than 10% of Phonevite each: John Nahm, Woohyoung Kim, Jin Ryoo.
- (6) The following persons exercise management and control over Phonevite: John Nahm, Woohyoung Kim, Jin Ryoo.
- (7) Phonevite has no subsidiaries/affiliates.
- (8) None of the persons/entities in items 5 – 7 above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (9) Phonevite's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (10) Phonevite has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (11) Phonevite is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (12) Phonevite's Operating Company Number is 256K.

/ John Nahm/

John Nahm

Date: February 26, 2026