

ROBOCALL

Mitigation Plan

Pursuant to 47 C.F.R. § 64.6305 Persistent Telecom Inc submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Persistent Telecom Inc (hereinafter also referred to as “Persistent Telecom” or “the company”) has in place to mitigate illegal robocalls. The company may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, its capabilities and its needs.

Persistent Telecom is judiciously working to prevent unlawful robocalls from originating on its network and has implemented the following robocall mitigation plan to address unlawful robocall traffic.

Persistent Telecom has enforceable terms of use and/or an acceptable use policy noted in its contracts. The policies are summarized as:

Terms for Termination of Service

Persistent Telecom Inc. may permanently terminate a customer's service under the following conditions:

- **Repeated or Severe Violations**
 - Repeated or severe violations of the terms of service, including but not limited to:
 - Origination of illegal calls.
 - Fraudulent or abusive use of services.

- **Failure to Cure Violations**

- The customer fails to remedy a violation or non-compliance issue within the specified timeframe after notice from Persistent Telecom.

- **Non-Payment**

- Continued non-payment of fees after the suspension period.

- **Violation of Legal or Regulatory Requirements**

- Engagement in activities deemed illegal or in violation of applicable regulations.

- **Threats to Public Safety or Security**

- Activities that pose a direct threat to public safety, national security, or the privacy of other users.

- **Fraudulent or False Representation**

- The customer provides fraudulent information or engages in deceptive practices.

Persistent Telecom confirms that the upstream providers have a certification in the Robocall Mitigation Database. The company will not accept voice traffic from an unregistered provider. The Company has been informed of the upstream providers “Know-Your-Customer” guidelines and have provided them with the necessary KYC documentation they’ve requested that the company completes.

Persistent Telecom follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that the company has an authenticated relationship with the customer. The Company uses this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

Persistent Telecom also validates, when possible, that the entity has a legitimate right to use its asserted calling numbers. The Company uses this information to support the attestation level it assigns to calls that it originates for that customer.

Persistent Telecom contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service.

Persistent Telecom requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.

Prior to installing services for new customers, the company takes the following measures to weed out end users that could potentially generate robocall traffic:

The Company uses a KYCs to confirm the following information for its customers:

- Full legal name.
- Date of birth.
- Residential address.
- Contact details (phone number and email).
- Government-issued photo identification (e.g., passport, driver's license, national ID).

The company Implements the following Know Your Customer (KYC) Practices

· Customer Onboarding Verification:

- Verify the identity of all customers (individuals and businesses) during onboarding using government-issued IDs, business registration documents, and other credible sources.
- Require customers to provide detailed information about the intended use of services (e.g., call volumes, destinations).

· High-Risk Customer Identification:

- Classify high-risk customers based on their industry (e.g., telemarketing) or history of suspicious activity and subject them to enhanced scrutiny.

· Enforce Caller ID Authentication (STIR/SHAKEN)

· Deploy STIR/SHAKEN Protocols:

Authenticate Caller ID information for all Voice over IP (VoIP) traffic using the STIR/SHAKEN framework. This ensures calls display accurate caller identities.

- **Check Unauthenticated Traffic:**

For calls without valid STIR/SHAKEN headers, perform additional checks before processing to assess potential risks.

- **Traffic Monitoring and Anomaly Detection**

- **Analyze Call Patterns:**

Use automated tools to monitor call traffic for unusual patterns indicative of robocalling, such as:

- High volumes of short-duration calls.
- Calls to large numbers of sequentially dialed numbers.
- Repeated calls to blocked or invalid numbers.

- **Flag and Review Suspicious Traffic:**

Automatically flag traffic that deviates from normal patterns and investigate potential illegal activity.

- **Block Known Illegal Traffic**

- **Use Call Blocking Technology:**

Implement tools to block calls from known illegal or fraudulent numbers, including:

- Numbers listed on industry-wide robocall blacklists.
- Invalid or unassigned numbers identified by the North American Numbering Plan Administrator (NANPA).

- **Dynamic Blocking:**

Automatically block or rate-limit traffic from customers exhibiting persistent suspicious behavior.

- **Periodic Audits and Reverification**

- **Review Existing Customers:**

Periodically audit active customer accounts, focusing on compliance with terms of service and call usage patterns.

- **Reverify Customer Information:**

Ensure customer records remain up-to-date, including Caller ID practices and business details.

- **Enforcement Actions Against Violators**

- **Immediate Suspension:**

Suspend service for customers found originating or facilitating illegal robocalls.

- **Service Termination:**

Terminate agreements with customers who fail to rectify identified violations or who knowingly engage in illegal practices.

- **Report to Authorities:**

Notify the FCC, FTC, or law enforcement agencies of confirmed cases of illegal robocalling.

- **Educate Customers on Compliance**

- Provide clear guidelines to customers about legal requirements for robocalling and Caller ID usage.

- Offer training or resources for high-risk industries to ensure compliance with laws such as the Telephone Consumer Protection Act (TCPA).

- **Submit and Maintain Robocall Mitigation Certifications**

- File certifications with the FCC's Robocall Mitigation Database describing the implemented mitigation practices.

- Include a detailed description of measures to prevent illegal robocalls, as required by the database.

- **Participate in Industry Collaboration**

- **Share Threat Intelligence:**

Collaborate with other voice service providers, regulators,

and industry groups to exchange information on illegal robocall trends and best practices.

- **Support Call Traceback Efforts:**

Participate in traceback initiatives to identify the source of illegal robocall traffic.

- **Maintain Records for Accountability**

- **Document Mitigation Efforts:**

Keep detailed records of all measures taken to prevent illegal robocalls, including traffic analysis reports and enforcement actions.

- **Regular Reporting:**

Submit reports to regulators demonstrating ongoing compliance and improvements in the robocall mitigation

Persistent Telecom uses proprietary call analytics software to monitor its outbound voice traffic in real-time as a method to prevent the origination or transit of illegal robocalls. When questionable activity is identified, the company takes the following actions:

Immediate Action

Temporarily suspend the customer's service to prevent further misuse while the issue is investigated.

Notify the customer of the suspension, specifying the nature of the questionable activity and any next steps.

Investigation Process

Conduct a detailed review of the flagged activities, including:

Traffic logs and call records.

Verification of the customer's Caller IDs and associated numbers.

Assessment of compliance with service terms and regulations.

Resolution

If the investigation finds no violation, restore the customer's service and provide a summary of findings.

If a violation is confirmed:

Notify the customer of the specific issues and required corrective actions.

Terminate service if corrective actions are not taken or if the violation is severe.

Reporting and Documentation

Report confirmed violations to relevant authorities, such as the FCC or law enforcement, as mandated by law.

Document all actions taken during the investigation and resolution process for auditing and compliance purposes.

Call Identification Details

To accurately trace the call, request the following:

- **Call Date and Time:** Exact timestamp, including time zone, for when the call occurred.
- **Calling Party Number (CPN):** The number displayed as the Caller ID.
- **Called Party Number:** The number that received the call.
- **Call Duration:** Duration of the call in seconds.
- **Call Termination Details:** Indication of whether the call was answered, forwarded, or resulted in voicemail.

Traceback Context

Understand the context of the traceback request:

- **Reason for Traceback:** Explanation of why the call is flagged (e.g., complaint of spam, fraudulent activity, regulatory issue).

- **Call Complaint Type:** Details about the nature of the call (e.g., scam, telemarketing, impersonation).
- **Regulatory References:** Any applicable regulatory concerns or violations tied to the traceback (e.g., TCPA violations, robocall mitigation issues).

Intermediate Provider Details

If the ITG provider is not the originating service provider, request:

- **Upstream Provider Information:** Details about the upstream provider that handed the call to the ITG provider.
- **Routing Path:** Information about the call's routing, including networks or providers involved.

Supporting Evidence

Request any available evidence or documentation related to the flagged call:

- **Call Logs:** Copies of call logs showing relevant details about the flagged call.
- **Recorded Call Content:** If available and permitted by law, request a recording of the call to verify its nature.
- **Customer Complaints:** Details about complaints received regarding the flagged number or call.

Technical Information

Gather technical details for validation and further analysis:\n

- **SIP Headers or Signaling Data:** Copies of the Session Initiation Protocol (SIP) headers to trace the call's origin.
- **Trunk or Circuit IDs:** Information about the circuits or trunks through which the call was routed.
- **Call Authentication Details:** Confirmation of whether the call was authenticated using STIR/SHAKEN and the associated attestation level (A, B, or C).

Customer Information

If applicable and permissible:

- **Originating Customer Details:** Information about the customer who originated the call, including their name, account details, and registered phone numbers.
- **Service Usage Records:** Historical call traffic data associated with the customer to identify patterns of misuse.

Requested Action

Clarify the next steps the ITG provider expects:

- **Immediate Action:** Determine whether the ITG provider is requesting call blocking, suspension, or other interim measures.
- **Follow-Up Requirements:** Understand any additional actions, such as submitting reports to regulatory bodies or further tracebacks up the chain.

Contact Information

Ensure clear communication:

- **ITG Provider Contact Details:** Request the contact information of the individual or team handling the traceback.
- **Response Timeline:** Clarify the deadline for responding to the traceback request.

Persistent Telecom will provide valid law enforcement and regulatory agencies with the relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated Robocall Mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. The company will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. The company will cooperate fully with such entities in investigating and stopping

any illegal robocallers that use the Company's service to originate, carry, or process illegal robocalls.

Requests from the valid agency must be submitted in writing and include the following information:

Law Enforcement Agency Name:

Agency Address:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

Persistent Telecom will comply fully with all conditions set forth in the FCC'S 2024 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

Persistent Telecom has designated an individual as a dedicated point of contact for addressing traceback requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>. The Company will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.

If a pattern of questionable activity is detected Persistent Telecom will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated. Requests from the ITG must be submitted in writing and include the following information:

Requests from the ITG must be submitted in writing and include the following information:

Company Name:

Company Address:

Phone Number in Question:

Requestor's Name:

Requestor's Title:

Requestor's phone number:

Requestor's e-mail:

Persistent Telecom performs the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. The Company has not had any agency action or investigation due to suspected unlawful robocalling or investigations.

Persistent Telecom is subject to any Commission, Law Enforcement, or Regulatory Agency Action or investigation due to suspected unlawful robocalling or spoofing and has not had any STIR/SHAKEN complaints.

Persistent Telecom does not wish to publicize any private and/or classified information that has the potential to expose the Company to fraud and/or anti-competitive actions. Therefore, the Company will submit a redacted version for the public site and requests that the FCC keep the unredacted version CONFIDENTIAL.