

High Powered Help, Inc Robocall Mitigation Plan

1. **Know your customers.** As a small provider, High Powered Help (HPH) has a personal relationship with all its customers. No entity may become a customer of HPH for voice services without having a personal call with HPH and then signing the voice services agreement. Additionally, customers must have valid, US based credit cards in order to order service.
2. **Know upstream providers.** HPH uses only a single provider: Bandwidth. HPH does not originate calls through any other provider, and HPH does not accept calls from any other provider. Additionally, all phone numbers are consolidated into Bandwidth. All calls are consolidated through Bandwidth, which simplifies compliance with STIR/SHAKEN because this allows Bandwidth to automatically sign calls with a full “A” attestation. ¹
3. **STIR/SHAKEN Implementation.**
 - a. **Inbound Calls.** By default, all inbound calls are evaluated based on the STIR/SHAKEN headers. Any inbound call that does not have an “A” attestation is blocked by the hangup command. Customers may submit a written request to loosen this restriction on their accounts to “B” attestations or “C” attestations. If the customer requests allowing “C” attestations thorough, they must e-sign an agreement that states they understand it increases the likelihood of spam calls.
 - b. **Outbound Calls.** Certification of outbound calls is directly related to our system’s confidence that the call is coming from an approved endpoint. All outbound calls are made by end point devices that use certificate authentication to connect to the provisioning system and download their configurations over TLS. These configurations use 16 character, randomly generated passwords to access the system, and where possible, certificate authentication. This gives us a high confidence that the endpoint belongs to the account and customer attempting to originate a call. Once the configurations are downloaded one time, the configuration is removed from the server preventing anyone from downloading it a second time without contacting our office to reprovision the phone or sending the phone in for service. All failed attempts to register or log into our systems are immediately blocked and banned by IP address for 24 hours on the first offence, 48 hours on the second offense, a week on the third offense, and permanently on the 4th or higher attempts. The IP addresses themselves must be manually removed at the request of the customer and a manual review of the authentication requests.
4. **Analytics system used to identify and block illegal traffic.**
 - a. **Inbound.** See 3.a above. Because all our traffic comes through Bandwidth, we rely heavily on the attestation accompanying the call in the headers.
 - b. **Outbound.**
 - i. **Device Security.** Outbound calls coming from known devices are allowed, but subject to the following:

¹ <https://www.bandwidth.com/understanding-stir-shaken/>

1. **Call pattern analysis.** Call patterns from endpoints that deviate from normal usage for that endpoint cause that endpoint to be disabled and blocked. “Normal usage” statistics include calls per minute, number of short calls, number of bad numbers dialed. Spikes in non-normal usage are used to detect potentially compromised credentials. If a spike is detected, it triggers an alarm in the system, which notifies administrators to analyze the logs at which point administrators may unblock the endpoint if the alarm was an obvious false-positive. Otherwise, administrators must call the customer to verify the traffic as well as verify that the customer is complying with HPH terms of service for voice services.

2. **Dial Pattern Recognition.** Attempts to call premium, restricted, or high risk numbers cause an endpoint to be immediately blocked and marked for administrator review.

- ii. **Geofencing.** Calls originating from outside the United States are not allowed. Registration attempts and / or call attempts originating from outside the US are blocked at the firewall.
- iii. **Brute force attack detection.** On the perimeter, we use fail2ban to block brute force registration and call attacks. To deal with attacks that are spread out over time, we use a week long window to detect attacks and initiate bans immediately after any failures. Additionally, we ban the entire subnet belonging to the IP address as reported by a WHOIS lookup. Since we are a small provider, the likelihood of two customers being on the same subnet is minimal.

c. **Non-Realtime Analysis.** Occasionally, CDR samples are uploaded to AI using the ChatGPT system to detect any call anomalies other systems may have missed. We currently have plans to implement a specialized AI system dedicated to real-time call analysis for detection of fraud or spoofing attempts.

5. **Other Robocall mitigation.**

- a. **Whitelist.** Some endpoints may opt to turn on a white-list feature to allow only pre-authorized callers. This directs all inbound calls to a voice prompt that requires the user enter in the answer to a question. Failure to enter anything or failure to enter the correct information as prompted allows the system to assume the caller is non-human, and adds the call source to a blacklist. Successful completion of the prompt places the call source on a whitelist, and future calls are allowed from that source.
- b. **Blacklist.** The blacklist (mentioned in “Whitelist” above) can also be augmented to include CIDs and other call source information from published lists of spam callers and other fraudsters.

6. **Extensions.**

- a. Inbound calls are only accepted to full ten digit numbers that are registered through Bandwidth and are delivered to our servers in full. Both inbound and outbound calls must be valid north American numbering plan numbers.

- b. Endpoints may dial extensions that specifically “live” in their account, and may not dial extensions or numbers that are not “internal” to them without it being processed as a regular outbound call, and therefore subject to robocall mitigation.

7. Safety

- a. **No blocking 911.** 911 is specifically prevented from being blocked.
- b. **Government Emergency Numbers.** Known government emergency numbers cannot be blocked.

8. Standard Procedures for responding to traceback requests

a. Receipt of Traceback Request

- i. **Acknowledge:** Upon receiving a traceback request from entities like the USTelecom Industry Traceback Group (ITG), the Federal Communications Commission (FCC), or law enforcement, acknowledge the receipt of the request promptly.
- ii. **Documentation:** Log the request with details like the date, time, requester, and any specific call information provided (e.g., called number, calling number, time of call).

b. Initial Assessment

- i. **Verify Authority:** Confirm the legitimacy of the request by ensuring it comes from an authorized entity.
- ii. **Check Internal Records:** Review internal call detail records (CDRs) or logs to locate the specific call in question. This might involve searching by call timestamp, origin, or destination number.

c. Data Collection

- i. **Call Path Analysis:** Trace the path of the call back through your network. This involves:
- ii. **Identifying the Direct Upstream Provider:** Who sent the call to you?
- iii. **Identifying the Downstream Provider:** If applicable, who did you pass the call to?
- iv. **Gather Evidence:** Collect all relevant data such as:
 - 1. Caller ID information.
 - 2. Time of call.
 - 3. Duration.
 - 4. Any STIR/SHAKEN attestation information.
 - 5. The IP addresses or trunk IDs involved in the call.

d. Communication with Upstream Provider

- i. **Request Information:** Contact the immediate upstream provider with the details of the call, asking for information on where they received the call from.
- ii. **Follow the Chain:** Continue this process upstream until you reach the originator of the call or the point where further tracing is not possible due to lack of information or cooperation.

e. Documentation and Reporting

- i. **Record Keeping:** Document every step of the traceback process, including all communication with other providers, the information gathered, and any obstacles encountered.

- ii. **Response to Requester:** Compile a report or provide the information back to the entity that requested the traceback:
 - 1. Include details like the source of the call, intermediate providers, and any issues encountered.
 - 2. Mention if the call was authenticated (STIR/SHAKEN) and the attestation level if applicable.
- f. **Cooperation and Compliance**
 - i. **Compliance with Regulations:** Ensure you comply with legal obligations to cooperate with traceback requests, which is mandated by regulations like the TRACED Act.
 - ii. **Timely Response:** Recognize that timely responses are critical; the FCC expects providers to respond to traceback requests within a reasonable timeframe (often within hours for urgent cases).
- g. **Mitigation Steps**
 - i. **Analyze Results:** If the traceback identifies a source of illegal robocalls, consider mitigation steps:
 - 1. Block the source if it's within your control.
 - 2. Inform your customers or upstream providers about the issue.
 - 3. Update your robocall mitigation strategies based on the findings.
 - ii. **Follow-Up**
 - 1. **Maintain Records:** Keep records of tracebacks for future reference or for compliance audits.
 - 2. **Feedback Loop:** Use feedback from tracebacks to improve your systems, policies, or to alert other industry players about emerging threats.
- h. **Legal and Policy Updates**
 - i. Consult attorneys for legal updates.
 - ii. Keep up-to-date with changes in regulations or best practices for traceback procedures through industry groups or regulatory updates.