



Robocall Mitigation Plan

1. Provider Information

- **Company Name:** TelephoneYacht, LLC
- **Address:** 111 North Wabash Ave, Suite 2013, Chicago, IL 60602
- **Contact Person:** Ather Mahmood
- **Contact Email/Phone:** amahmood@telephonyacht.com (312)878-5500

2. Overview

TelephoneYacht, LLC ("TelephoneYacht") is a Chicago based Telecommunication Service provider focusing on providing cost effective, turnkey, business solution to Customers, nationwide.

TelephoneYacht recognizes the importance of preventing unlawful robocalls originating on its network to protect Americans from the consequences of these unwanted and illegal robocalls. As such, TelephoneYacht has taken its robocall-related obligations seriously, including preparing and implementing an effective robocall mitigation plan in accordance with the FCC's mandate, and selecting a wholesale provider partner that shares these values.

In the call path, TelephoneYacht acts as a Voice Service Provider, and does not have a STIR/SHAKEN obligation because it is a reseller and lacks control over the infrastructure necessary to implement STIR/SHAKEN. As discussed herein, TelephoneYacht's provider partner is IntelPeer Cloud Communications LLC ("IntelPeer"), which is STIR/SHAKEN compliant. This filing describes the "reasonable steps" TelephoneYacht has taken to prevent the origination of illegal robocall traffic as part of its robocall mitigation program (the "Plan"). All TelephoneYacht traffic is subject to this Plan.

3. Policies and Procedures to Identify and Mitigate Robocalls

A. Traffic Monitoring and Analysis; Call Analytics

1. We have implemented tools to monitor voice traffic for patterns consistent with robocalls. For instance, we obtain CDRs on our PBX's that are internally reviewed and if robocalls are suspected we immediately contact our customers. We also incorporate analytics from our partner provider that provides immediate notification of high call volumes.
2. As a reseller, TelephoneYacht relies on analytics software adopted by its wholesale

provider, IntelPeer, to monitor call traffic, which is described in more detail in RMD0004630. TelephoneYacht does not utilize any other solutions from third-party vendors.

- These solutions identify high call volumes, short-duration calls, or anomalous calling patterns. For instance, calls exceeding certain thresholds (e.g., over 100 calls per minute or calls lasting less than 5 seconds) will trigger further internal investigation pursuant to IntelPeer's analytics.
- If IntelPeer identifies a high call volume, it will send an immediate notification to TelephoneYacht, including a picture and trunk location so that TelephoneYacht can reach out its customer to investigate and mitigate if necessary. If TelephoneYacht is not satisfied by this investigation then it will take action, which may include initiating a traceback investigation, verifying the STIR/SHAKEN information, and/or blocking calls from that originator.

B. Call Originating Policies

1. Knowing Our Customers Policy:

- Verify business customers' identity, legitimacy, and use of numbers to ensure compliance with FCC rules.
 - We fully vet all customers before granting service by collecting contact names, email addresses, and billing information. We also check and confirm their state business registration to confirm they are a legitimate company. We meet our customers in person and confirm the signatory is authorized by the company.
- Periodically audit existing customers to ensure compliance.
- Retain contractual rights to terminate customer if our services are used for unlawful purposes such as robocall generation. We also do not allow for telemarketing in our contracts.
 - As part of our onboarding process, we educate customers about the dangers of illegal robocalling and their role in compliance.
 - We also provide customers with resources to identify and report unlawful robocalls.

2. Network Access Controls:

- Restrict access to the network for customers who fail to comply with applicable laws and policies.
- Enforce contractual obligations prohibiting unlawful robocall generation, as discussed above.
- Customers are only permitted to originate traffic from their Office IP address – the source address is otherwise locked. So, for instance, a customer could not bring a device to their home and start calling from a different location using our services, the services must be used at a customer's office address.

3. Knowing Our Providers Policy:

- TelephoneYacht's partner provider, IntelPeer has registered in the Robocall Mitigation Database (RMD0004630) and reports that it has completed its STIR/SHAKEN implementation for all roles that it plays in the call path.
- TelephoneYacht and IntelPeer have a continuous dialogue on this issue and each take robocall prevention and mitigation seriously. We work together and share information about unlawful robocall sources.
- As discussed in further detail in Section E of IntelPeer's RMD filing (RMD0004630), the parties have certain provisions in their agreement aimed at further combating illegal robocalling, including authorization to respond to traceback requests, the right for suspension/termination due to fraudulent activity, among other provisions.

C. Handling of Suspected Robocall Traffic

1. Identification and Investigation:

- Immediately investigate flagged traffic using the above-described analytics tools and "Knowing Our Customer" information.
- Document findings and take corrective action as discussed below.

2. Blocking or Mitigating Calls:

- Block unlawful calls in compliance with FCC rules.
- Notify customers of call blocking when required and provide a method to dispute erroneous blocks.

3. Repeat Offenders:

- Terminate services to customers repeatedly identified as originating illegal robocalls, in accordance with contractual provisions.

4. STIR/SHAKEN Implementation

As discussed herein, TelephoneYacht is a reseller and relies on its underlying provider, IntelPeer as the SIP Provider for all of its customers. As such, TelephoneYacht "lacks control of the network infrastructure necessary to implement STIR/SHAKEN"¹ and is considered a provider "without" a STIR/SHAKEN implementation obligation.² IntelPeer has registered in the Robocall Mitigation Database (RMD0004630) and reports that it has completed its STIR/SHAKEN implementation for all roles that it plays in the call path.

¹ 35 FCC Rcd. 3241, 3260, para. 40.

² 38 FCC Rcd. 2573, 2592, fn. 137 ("When referencing those providers 'without' a STIR/SHAKEN implementation obligation, we mean those providers . . . that lack control over the facilities necessary to implement STIR/SHAKEN.")



5. Reporting and Recordkeeping

1. Robocall Mitigation Database:

- Submit this Robocall Mitigation Plan to the FCC's Robocall Mitigation Database ("RMD").
- Update the Plan as necessary, and file such material updates in the RMD within 10 business days or otherwise in accordance with the FCC prescribed timeframes, to reflect changes in processes or technology.

2. Records Retention:

- Maintain records of:
 - Traffic analytics and investigations.
 - Customer vetting procedures.
 - Actions taken to mitigate unlawful robocalls.

3. Annual Reviews:

- Conduct internal audits to ensure continued compliance with this Plan.

6. Company Enforcement

As discussed herein, and pursuant to our contractual provisions with customers, non-compliance with our robocall mitigation policies may result in:

- Suspension or termination of services for violators.
- Reporting unlawful activity to the FCC or relevant law enforcement agencies.

7. Traceback Requests

TelephoneYacht is committed to responding fully and within twenty-four (24) hours of receipt to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that use TelephoneYacht's service to originate calls.

Authorized Signatory: 

Date: 12/26/2024