



Robocall Mitigation Plan

B'yond Platforms Pte Ltd (B'yond) is headquartered at 36 Robinson Road, #20-01, City House, Singapore 068877. We are a foreign gateway voice service provider based in Singapore, our operations fall under FCC 47 CFR § 64.6305 and we are not capable of implementing STIR/SHAKEN in our network. We do pass all traffic to our next hop downstream carriers who have implemented STIR/SHAKEN protocols in their IP voice networks.

Our role in the call chain:

- We are a Gateway Provider without a STIR/SHAKEN obligation
- Our next hop Intermediate Carriers are Telekom Deutschland GmbH (RMD0031081664), DIDWW Ireland Ltd (RMD0003808) and Tata Communications, Inc. (RMD0003179)

We have not been prohibited from filing a certification in the Robocall Mitigation Database.

B'yond or any of its executives or principals do not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations or related state law violations.

We use the affirmative and effective measures detailed below to prevent the origination or transit of illegal robocalls.

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use 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.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Know Your Up-Stream Provider

We require that upstream providers have a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers, and use call analytics to identify suspicious traffic.

We establish an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider or a foreign intermediate provider.

Our contractual provisions with upstream providers prohibit them from sending us illegal robocalls. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Traceback

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

Robocall Mitigation Program

Combining behavioral analytics, caller authentication and verification, our software solution, provided by TransNexus, features:

- **Fraud Detection:** Detection of high volume robocalling, spoofing and spam call activity.
- **Subscriber Notification:** Caller ID Name override to warn subscribers of suspicious calls.
- **Call Blocking Support:** Accurate identification enabling you to block fraudulent phone calls.
- **Business Number Verification:** Register legitimate business numbers to prevent unintentional call blocking.
- **Do Not Call Registry:** We comply with the FTC's rules for the Do Not Call Registry.