



Robocall Mitigation Plan

This robocall mitigation plan is for BBH Connectivity, Inc., with headquarters at 121 E. 24th St., 6th Floor, New York, NY 10010.

We perform the following roles in the call chain:

- A voice service provider without a STIR/SHAKEN implementation obligation serving end-users.
- IntelPeer is our next hop carrier and they are currently signing our calls.
- We are performing Robocall Mitigation.

BBH Connectivity, Inc., has not been prohibited from filing a certification in the Robocall Mitigation Database.

BBH Connectivity, Inc., does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

BBH Connectivity, Inc., uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

We follow 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.

In accordance with the ATIS Requirements for a full attestation, BBH Connectivity knows which customer is authorized to use which calling number, and we maintain this information in the DID database provided by IntelPeer and filled out by BBH Connectivity.

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.

In addition, we have implemented a Call Abuse Policy, as it pertains to the TRACED Act, and have published the following policy to our terms of use, and have notified our customers of the policy as copied below:



“Any call originated on the network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”

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

We use call analytics software provided by Cisco Call Manager to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.

The software provides detailed reporting to identify suspected illegal robocalls.

Combining behavioral analytics, caller authentication and verification, our solution 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 as per the TRACED Act (2019)
- Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.
- Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

We immediately investigate any identified suspicious calls to determine if the caller is attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.



STIR/SHAKEN

BBH Connectivity, Inc provides voice services exclusively as reseller of IntelPeer Networks, LLC.'s SIP Trunking services for all inbound and outbound calling. No other carrier services are used for inbound or outbound call routing. All DID and 800 numbers are numbers that are IntelPeer assigned or are numbers ported to IntelPeer, and IntelPeer performs all inbound routing. It is not possible for callers to spoof a number for our hosted services as they have no control over the CLID settings.

IntelPeer has fully implemented STIR/SHAKEN and filed as such under the Robocall Mitigation Database RMD0004555 and is currently providing full attestation given the above conditions.

BBH Connectivity, LLC does not have the framework for STIR/SHAKEN and all STIR/SHAKEN activities are handled by our upstream provider, IntelPeer.