



Robocall Mitigation Measures

Bluerock Communications will incorporate the following to manage and adhere to the Robocall Mitigation guidelines.

- Bluerock requires all customers to provide information such as physical business location, business contact(s), state or country of incorporation, federal Tax ID, and understanding the nature of the customer's business, including website, landing pages, express written consent content, and privacy notices.
- Bluerock will incorporate robocall mitigation language into our contracts, terms of service, acceptable use policy, as appropriate, prohibiting use of our platforms to make or receive illegal calls.
- Bluerock has fully implemented STIR/SHAKEN caller ID authentication technology.
- All outbound caller IDs are limited to only those telephone numbers registered in customer's accounts. No spoofing capabilities.
- When non-compliant calls are brought to our attention, through our upstream providers or through our own analysis, Bluerock will take necessary action with the customer to identify and cease the non-compliant activity.
- Bluerock will not provide to or receive services from any service provider not listed in the FCC mitigation database.
- Bluerock's robocall mitigation practices shall be applied in a non-discriminatory manner.
- Bluerock has provided a point of contact in charge of responding to traceback requests within 24 hours of such notifications (carriersupport@1bluerock.com). Bluerock will also work diligently with all Local, State and Federal government agencies on all requests regarding information pertaining to robocall activity and other legal matters.
- Bluerock Communications will respond within 24 hours of receipt to traceback requests sent via email to carriersupport@1bluerock.com or via US Postal Service: Bluerock Communications, 110 East Broward Blvd, 17th Floor, Fort Lauderdale, FL 33301