

CompassMSP

Robocall Mitigation Plan

This robocall mitigation plan is for CompassMSP, LLC., with headquarters at 67 Prospect Ave Suite 202 Harford, CT 06106

We perform the following roles in the call chain:

- A Voice Service provider with a STIR/SHAKEN implementation obligation serving end-users.
- CompassMSP, LLC uses Coredial , LLC (RMD0002771) and CloudCo Partner (RMD0007967) for Hosted VoIP partners.
- Our next hop intermediate carrier is FlowRoute (RMD0011709)

CompassMSP, LLC., has not been prohibited from filing a certification in the Robocall Mitigation Database.

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

CompassMSP, LLC., 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.

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.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

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.

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 TransNexus and our hosted VoIP partners 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. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

As part of CompassMSP's, RMP, we provide the following affirmative, effective measures to help minimize the impact of illegal or unwanted robocalls, and prevent new and renewing customers from using our network to originate illegal calls:

- **Automatic Number Identification Management:** CompassMSP shall block originating telephone numbers if identified based upon patterns of activity.
- **Proactive Blocking.** CompassMSP requests underlying carriers to block calls from phone numbers on Do-Not-Originate lists published by US Telecom and Neustar.
- **General Terms and Conditions.** CompassMSP prohibits Customers from originating fraudulent calling using any fraudulent means, devices, or technologies. In fact, CompassMSP end user Customer Terms and Conditions permit CompassMSP, without notice, to discontinue, block or suspend services if necessary to prevent fraud, scams, tampering, schemes, false or invalid numbers. In short, CompassMSP shall block or suspend the service of any Customer(s) originating unlawful robocalls through BlackPoint IT Services. CompassMSP's Robocall Mitigation Program includes an increasing investment in resources over time to further strengthen adherence to compliance requirements by Customers.
- **Acceptable Use Policy.** CompassMSP's Acceptable Use Policy ("AUP") also prohibits Customers from utilizing the Service for any illegal, fraudulent, objectionable and/or unauthorized manner, reserving the sole and absolute right to deny, restrict or immediately suspend or terminate service if the use of the Service by the Customer, or anyone having access to or using the Service, either violates the CompassMSP AUP or includes unlawful conduct.
- **Underlying Network Provider.** CompassMSP works with underlying providers and supports the benefit of deploying systems to detect potential robocall activity relying upon statistics such as average call duration, ASR, and call count carrier/consumer reports. CompassMSP's regulatory compliance counsel confirms that CompassMSP's underlying carriers maintain compliance with fully implemented STIR/SHAKEN protocols through the date of this RMP.
- **Traffic Reports and Industry Information.** Reports generated by Call Detail Record and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints, may identify potential unlawful robocalling. We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was 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

We have registered with the STI-PA using OCN 838L. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.