

Robocall Mitigation Program

As a reseller operating without direct network infrastructure, Point5 Managed Services Robocall Mitigation Program (RMP) focuses heavily on contractual obligations, diligence regarding our upstream providers, robust customer vetting, and full cooperation with traceback requests. Point5's RMP, is should be structured around the following core commitments and procedures:

Know Your Customer (KYC) Procedures and Vetting

As the primary touchpoint with the end-user/customer, robust KYC is our most effective control point for robocall mitigation as Point5 does not maintain network components but is still responsible for robocall mitigation as the main point of contact with the end customers.

Procedure	Description	Responsibility
New Customer Vetting	Point5 collect and verifies business registration, contact information, intended use of service, and expected traffic profile (e.g., call volume, call duration, ASR). Screen against known robocaller or fraud databases.	Onboarding Team
Acceptable Use Policy (AUP)	Point5 maintains an AUP prohibiting illegal, fraudulent, or abusive traffic (including illegal robocalls) as part of our Master Services Agreement that is required for customers to sign upon service order.	Compliance
Traffic Profile Review	Compare customer traffic patterns (ASR, CPL, call attempts per number) against stated intended use and industry norms. Deviations are flagged for immediate investigation by the Network Operations team and forwarded to Compliance as needed.	Operations

Procedure	Description	Responsibility
Customer Training/Awareness	Provide clear guidance on legal calling practices (TCPA, TSR compliance) and the consequences of illegal traffic (service termination, traceback cooperation) to customers during the delivery process.	Service Delivery

Upstream Vetting and Contractual Diligence

As a reseller Point5 relies on wholesale providers, who are diligently selected and managed. d

Procedure	Description	Responsibility
Provider Selection Criteria	Point5 only utilizes upstream providers that are properly registered in the FCC's RMD and certify their own robocall mitigation efforts.	Executive Team
Contractual Requirements	Incorporate specific clauses requiring the upstream provider to: 1) Support and cooperate with all traceback requests; 2) Immediately notify the reseller of any high-risk traffic alerts associated with the reseller's traffic; 3) Maintain their own mitigation program.	Compliance
Monitoring and Review	Periodically review the upstream provider's RMD status and performance in handling traceback requests. Reviews are undertaken and documented as part of scheduled vendor quality and relationship cadence.	Compliance

Traffic Monitoring and Analysis

Although Point5 does not own the network, we monitor customers' activity via the data provided by our upstream partners as part of our obligations under the FCC filings for the Robocall Filing Database.

Procedure	Description	Responsibility
High-Risk Traffic Alerts	Receive alerts (FCC/Traceback Group notifications, high-volume anomaly reports, STIR/SHAKEN status failures) provided by the upstream carrier.	Operations
Immediate Suspension Protocol	Suspension protocol: -Immediate notification of pending suspension or termination of customer service upon confirmation of illegal robocalling activity -Customer must cease confirmed illegal activity and per agreement. Failure to comply will result in immediate suspension -Document suspension process and outcome	Operations and Compliance
Data Retention	Maintain detailed records (CDR data, customer identity, AUP acceptance) necessary for traceback for a minimum of 18 months.	Operations

Traceback Cooperation and Enforcement

Point5's cooperation is non-negotiable and must always be swift and comprehensive.

Commitment	Description	Timeline
Designated Contact	Point5 has appointed a single, always-available point of contact (POC) for all traceback and law enforcement inquiries in the RMD and with our upstream provider.	Ongoing

Commitment	Description	Timeline
Response Protocol	Immediately investigate and respond to all traceback requests from the FCC, law enforcement, or the Industry Traceback Group (ITG). Responses include relevant CDRs and customer identity information as required.	Within 24 hours of receipt
Enforcement Action	All enforcement actions taken against customers identified through traceback (warnings, service suspension, termination) are documented.	Immediately upon action

Compliance and Program Review

In addition, Point5 undertakes ongoing compliance activities to ensure that mitigation programs and efforts are in place, properly followed, and adjusted as appropriate.

Area	Review Frequency	Ownership
RMP Review	Annually	Compliance
RMD Filing Confirmation	Biannually (to confirm continued status)	Compliance
Employee Training	Annually (covering KYC, AUP, and Traceback Procedures)	Operations/Compliance