

There are a variety of mitigation techniques that Commsgroup use to mitigate or entirely prevent the transmission of illegal robocall traffic. An overview of these approaches is discussed below.

Know Your Customer: Commsgroup should confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state or country of incorporation, tax ID, and the nature of customer's business. This can help prevent Originating Providers allowing illegal calls from gaining access to our voice network.

Monitor Network Traffic: Commsgroup analyse high-volume voice network traffic to identify and monitor patterns consistent with robocalls. This information can assist in the traceback process to identify the source of illegal calls.

Require Traceback Cooperation in Contracts: For all new and renegotiated contracts governing the transport of voice calls, Commsgroup use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.

Rejection by the Provider/Carrier: When the provider/carrier learns that their platform is being used as a conduit for illegal robocalls, they identify the offending customer from the call examples provided by the relevant party (e.g., call samples provided to them), and then examine the call detail records (CDRs) for that customer. The provider will examine the CDRs for signs of illegal robocall traffic, such as high call volumes, low duration calls, sequential dialling patterns, and call volumes to telephone numbers on the Do Not Call list. The provider may then impose network-level constraints, which can include throttling the rate at which the customer can initiate calls, restricting the number of concurrent calls, and limiting the caller-ID value(s) available for the customer's use. The provider may also decide that discontinuance of service is appropriate, especially if violations are on-going. New and existing overseas customers may warrant appropriate scrutiny before calls are allowed to be generated.

If the Originating Provider fails to mitigate the illegal calls or cooperate with contractual traceback commitments, downstream providers (which are receiving the calls from the Originating Provider) may want to consider whether they should continue to accept that provider's traffic. A downstream provider could notify an offending Originating Provider of terms-of-service and/or acceptable-use-policy violations, the terms of which generally prohibit the sending of illegal calls, and often have even more rigorous restrictions. If the traffic continues, the downstream provider could act according to the terms of its contract with the Originating Provider.

Government Enforcement Against the Robocaller: Gov enforcement also have to investigative authority to address crimes committed using illegal robocall technology. They often bring civil enforcement actions against a party placing illegal calls. This could then lead to additional criminal enforcement actions. Call records obtained from the Originating Provider could buttress these actions.