



Robocall Mitigation Plan

AVANSER's Robocall Mitigation Plan is based upon three key technical and operational areas – Prevention, Detection and Mitigation.

PREVENTION

AVANSER has a strict customer on-boarding process starting with "Know Your Customer" screening. The identity of commercial customers is confirmed by collecting the primary account person's contact details, business registration information and nature of the customer's business.

AVANSER also includes in its Terms & Conditions that services must not be used for unlawful purposes, and considers illegal robocalling as one such service that is unlawful.

DETECTION

AVANSER's team of network engineers have implemented monitoring systems to detect any analyse the traffic and calls on its network. These include (but are not limited to) monitoring, low call duration and low completion percentages, large bursts of traffic during a short timeframe, and high call volume from invalid numbers.

Abnormal or unusual traffic patterns are then further investigated to determine whether robocalling or other illegal activity might be occurring on the network. AVANSER constantly reviews its monitoring systems to ensure that opportunities to improve its monitoring applications will lead to greater efficiencies to identify and respond to potential robocall activities.

MITIGATION

In the event that robocalling activity is identified and confirmed, AVANSER's team will take action to stop this activity with high priority. The information that is collected and analysed is used in the traceback process to assist with identifying the source of illegal robocalls.

AVANSER's system rejects calls directed to numbers that are not part of the AVANSER inventory. Inbound calls that pass through screening, but should not be handled, will stop at the system's automated call routing with a warning message. Outbound calls directed to the public network are restricted by AVANSER to be either:

a) expected by the receiving party as an outcome of AVANSER's service; or

b) placed by KYC authenticated entities.

When an abuse is detected AVANSER shuts the Account/Extensions public access pending further investigation.

Additionally, AVANSER's carrier suppliers have STIR/SHAKEN features and call blocking tools that prevent the delivery of robocalling traffic as well as calls from invalid or illegal telephone numbers in line with industry best practices.