

CSC TELECOM Robocall mitigation plan

All customers of CSC TELECOM are contractually obliged to comply with the legal requirements of the respective country from which the telephone number they use originates, in this case the regulations of the USA. Customers who use international telephone numbers are also contractually obliged to use a telephone number as the calling line identification (CLI) when making outgoing calls, which they have either received directly from CSC TELECOM for use or for which they have provided proof of a right of use.

24/7 monitoring of the quality parameters – short calls , ACD, ASR, NER on daily basis with proactive system s alarms. Alarms are automatically send by email to our NOC/NMC team. Suppliers will be given direct line numbers for the NOC to get immediate contact to fast track any action required.

Monitoring activities for abnormal traffic patterns which can also detect robocalls include (but are not limited to):

- Search for burst traffic
- Variety of target numbers (B-party)
- Volumes of traffic within timeframes

In addition, set algorithms analyses the calling behaviour of customers in outbound calls as part of fraud prevention measures to identify and limit abusive calls (e.g. robocalls) and to intervene against them within the scope of legal possibilities. Among other things, the time, number and duration of outbound calls are analysed.

CSC TELECOM fully supports fraud prevention activities and will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. CSC TELECOM will cooperate with such entities in investigating and stopping any illegal robocalling activities that use its services to originate calls.

Cooperation with the Telecommunication Authorities, law enforcements and other authorities to investigate and stop any illegal calls.

Cooperation with the telecommunication partners on the domestic and International level to detect and stop or block any spam or fraudulent traffic. Partners will be asked to prove they have adequate monitoring and blocking processes in place themselves before they will be allowed to send USA traffic.