

Infosys Limited – Robocall Mitigation Program Description

Infosys Limited implements a robocall mitigation program designed to prevent the origination, transmission, or facilitation of illegal robocalls and unlawful caller ID spoofing across its voice and communication services. The company complies with applicable FCC regulations, TRACED ACT, and industry best practices for call authentication and traffic monitoring.

Infosys Limited employs reasonably know your customer (KYC) procedure, traffic validation controls, and ongoing monitoring mechanisms to identify suspicious calling patterns, anomalous traffic volumes, invalid numbering formats and potentially fraudulent communications activity. Appropriate mitigation actions, including call blocking, traffic suspension, escalation, and customer remediation are applied when unlawful or suspicious activity is detected.

Where technically feasible, Infosys limited support industry standard caller authentication frameworks including STIR/SHAKEN, directly or through up/ downstream carrier relationships. The company also cooperates with law enforcement agencies, regulators and industry traceback consortiums to investigate and mitigate illegal Robocall activity.

Infosys Limited maintains internal policies, compliance processes and operational safeguards intended to reduce the risk of illegal robocalls being originated or transmitted through its network infrastructure and services.