

Robocall Mitigation Plan – Core Telecom Limited

Customer Vetting and Onboarding

Core Telecom Limited maintains a robust onboarding process to prevent access by fraudulent or illegitimate entities. Every entity undergoes verification via an account manager and due diligence process to confirm their legitimacy as a registered business or organisation. This process ensures that only vetted entities can access Core voice services.

Traffic Monitoring and Detection

Core Telecom employs automated monitoring tools across its voice network to track call volumes, destinations, and durations. These systems are designed to detect anomalies or patterns commonly associated with robocall activity. Suspicious behaviour triggers alerts for manual investigation or automatic action.

Thresholds and Automated Controls

Core enforces configurable traffic thresholds and implements automatic barring if a customer exceeds defined limits. This helps prevent high-volume, potentially abusive traffic from reaching downstream carriers, including calls to U.S. destinations.

Contractual Provisions Against Robocalling

All Core Telecom partners are bound by Terms and Conditions which include fair usage clauses and prohibit abuse of any services. Contracts allow for immediate suspension or termination of service if an entity is found to be engaging in behaviour indicative of robocalling or service misuse.

Network and Geographic Scope

Core Telecom does not operate an IP-based network within the United States and does not originate calls itself. However, Core's network may be used by partners to terminate calls to the U.S. As such, Core Telecom has filed this mitigation plan in accordance with FCC requirements for foreign voice service providers.