

Digicel Caribbean Ltd Robocall Mitigation Plan

Digicel Caribbean Ltd., on behalf of itself and each of its affiliates (together, “Digicel”) has adopted this Robocall Mitigation Plan to take measures to limit the potential for the transmission of unlawful robocalls from its network to be terminated in the United States of America.

Customer/Subscriber Screening (KYC)

Digicel collects and maintains, in a secure database, information relating to its subscribers in markets where subscriber information collection is mandated by the respective regulatory bodies, and or by law. In markets where there exists no mandatory requirements, Digicel, to the extent possible, and where permitted within privacy requirements, maintains its customer base. Digicel also maintains and updates policies, which its customers are bound by, setting out use of its equipment, including any numbers and connections thereto. This prohibits activities by customers that may fall foul of applicable laws, regulations and policies, and Digicel takes immediate actions where necessary in order to prevent fraudulent or unacceptable activities. These are consistently reviewed by group functions in order to pre-empt illegal and fraudulent activities, and to implement further restrictions, policies or guidance, as and where necessary. Digicel does not hesitate to enforce its policies, or terms of any contracts and takes immediate steps where any issues are brought to its attention.

Support of Industry Traceback Group and Law Enforcement Requests

Digicel has a long history of supporting and responding to lawful requests made in accordance with the laws under, which it is licensed to operate. These requests include those received from United States law enforcement agencies (LEAs).

Digicel commits to continuing this level of support and response to such requests, which is extended to the Industry Traceback Group (ITG) in accordance with the respective laws and regulations under which it operates and specifically in relation to the investigation of robocallers.

Anti-Fraud Support and Strategy

Digicel has processes in place and remains vigilant in detecting and mitigating fraud on its networks. As part of this process, incidents are without unnecessary delay brought to the attention of the executive management of the organization for visibility and support. As a result, incidents are treated with urgency and given the attention required, and dealt with swiftly.

This process is extended to Digicel’s Robocalling Mitigation Plan and Digicel is committed to evolve in this process in order to ensure efficiency and effectiveness when dealing with fraudulent activity on its networks with changes to technology and keeping up to date with other technological advancements.

Control Strategy (Solutions)

Digicel operates an industry leading Fraud Management System (FMS), which uses Call Detail Records (CDRs) and other high standard mechanisms to detect irregular usage on its networks, which includes continual review of voice calls, which are terminated to United States telephone numbers.

The FMS operates and generates alerts 24/7/365, which importantly triggers automated mitigations to limit fraud and abuse of Digicel networks and services that in turn may impact the networks as well as its partner networks.

Operational Strategy (Human Resources)

Digicel has a centralized Revenue Assurance and Fraud Management (RAFM) operations team, which monitors outbound international Voice calls and alerts (including those to United States telephone numbers) from Digicel's subscribers and networks. The RAFM team operates seven (7) days a week and diligently monitor all relevant calls and are swift to action when necessary.

In addition, Digicel's Global Network Operations Centre (Global NOC) monitors network performance and receive escalations alerting the necessary support teams including the International Voice and RAFM operations teams. Digicel's GNOC also operates 24/7/365.

The RAFM operations team reviews all FMS alerts and executes granular analysis to confirm the legitimacy of the alert, conclude a root cause analysis, and execute final actions, which may include suspension, termination or resumption of services.

All actions are taken in accordance with the laws and regulations that govern Digicel's operations in respective operating jurisdictions.

Industry Affiliations in Support of Anti-Fraud

Digicel RAFM members are members of the Fraud and Securities Group (FASG) of the GSM Association (GSMA).

Digicel RAFM members are well versed in their respective rights and to that end previously attended and presented at Communications Fraud Control Association (CFCA) conferences where it remains a strong voice against fraudulent activities and finding new measures to ensure better, swifter and high level control.