



Robocall Mitigation Program

Executive Summary

Telecommunications Services of Trinidad and Tobago (TSTT) is Trinidad and Tobago's largest and most advanced provider of integrated communications solutions to the residential and commercial markets. TSTT is proud to be the sole National full-service communications provider in Trinidad & Tobago. Its leading-edge products are designed around an IP-based core infrastructure and marketed under its bMobile brand. In addition to fixed-line and first in Trinidad and Tobago 4G mobile communications, the Company offers wireless data using HSPA+ and LTE technologies; Data Services; Cloud Services; Hosted PBX; subscription-based IPTV, and business/home alarm monitoring services.

TSTT, on behalf of itself and its subsidiary (AMPLIA), has implemented the following Robocall Mitigation Plan, which outlines the measures adopted to reduce illegal robocalls on its TSTT's network:

- a) TSTT will work with the FCC, law enforcement, and the industry traceback consortium (subject to the limitations of applicable laws in Trinidad & Tobago) to investigate and stop illegal robocallers from using TSTT's services to originate calls. TSTT's point of contact for the FCC has been set as the shared mailbox robocall@tstt.co.tt, with Ms.Gillian Goodridge currently set as the POC for the department.
- b) TSTT has implemented a Know Your Customer ("KYC") protocol for all new and existing customers requesting services from TSTT's network. Customers must provide their name, valid national identification, proof of billing address via utility bills, phone, and email contact. In addition to the information above, businesses are required to provide business registration id, type of Company, approved signatory(s) Value Added Tax (VAT) number, and all company documents must have affixed their company stamp.
- c) Trinidad and Tobago Data protection form will be issued to any non-Trinidad and Tobago (local) agency, provider, law enforcement, before the disclosure of any customer personal information, stating that there are similar



provisions/safeguards to protect the customers' personal information to those that are established in our local market. This is to adhere to section 36 of the Data Protection Act of Trinidad and Tobago.

- d) TSTT also assesses a customer's creditworthiness using previous payment history patterns in cases where the customer was an existing customer of TSTT and/or may employ a credit reference agency to assist in this assessment before providing services to the customer.
- e) All customer contracts must be signed by the registered customer. In the case of a company, by an authorized representative of the customer.
- f) TSTT's terms and conditions of service (which a customer is obligated to agree to before service provision) provides that a customer must not use any of TSTT's services for fraudulent or illegal activities. These terms and conditions are subject to change due to updated regulatory and legal compliance laws.
- g) Call Detail Records (CDRs) are available for all calls originating and terminating on TSTT's network and can be accessed as required up to a maximum of two (2) years (archived). CDRs include the Originating and Terminating number, trunk group, timestamp of call origination, and call duration. Our Fraud Management Team will use this information to identify the customer who originated the call to take action.
- h) Calls are monitored continuously by TSTT's Carrier team and Fraud Department to identify any suspicious or abnormal traffic patterns. Once an incident is discovered, the offending customer or Carrier will be notified. Services to the customer may be suspended until the issue is rectified to limit additional exposure to TSTT. Further investigations will be done to determine the root cause of the incident with the customer and what measures should be put in place to limit its future occurrence.
- i) TSTT's US-bound traffic enters the US via intermediate and direct carriers, which are listed in FCC's Robocall Mitigation Database. These carriers would have either deployed STIR/SHAKEN or some appropriate Robocall mitigation plan.
- j) TSTT does not provide customers with US-based DID's, all traffic to US destinations will adopt the following CLI format of 1(868)-NXX-XXXX unless a



customer is roaming on TSTT's network with a US-based or other foreign numbers.

- k) Customers roaming on TSTT's network will first register with their home providers' networks (US Territory Carriers) via existing 3rd Generation Partnership Project existing authentication/authorization framework **3GPP TS 33.102**. The framework outlines how the roaming customer communicates to the home providers' network to authenticate the roaming customer when connecting to TSTT's Wireless network. The sole responsibility for authorizing the roaming customer to make calls will therefore be the responsibility of the home provider. Additionally, if the roaming customer is being investigated for Robocalling, **any** and **all** responsibility for providing KYC information will be the responsibility of the home provider (US Territory Carriers).