

## **Robocall Mitigation Plan**

Introduction As part of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Federal Communications Commission (FCC/Commission) adopted rules requiring voice service providers to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks.

The FCC requires that all providers certify in the Robocall Mitigation Database that they have fully implemented STIR/SHAKEN or have instituted a Robocall Mitigation program to ensure that they are not originating illegal robocalls.

The Commission requires voice service providers to develop a Robocall Mitigation plan that:

- Details the reasonable steps taken to avoid originating illegal robocalls
- Demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls
- Is filed in the Robocall Mitigation Database.

The Commission stated that a robocall mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

---

### **KYC Process**

Tecxar Consultants Pvt. Ltd. has established and implemented comprehensive Know Your Customer (“KYC”) policies for any new and existing customers. The objective of the KYC policy is to prevent Tecxar Consultants Pvt. Ltd. from being used, intentionally or unintentionally, for spoofed or illegal traffic. KYC procedures enable Tecxar Consultants Pvt. Ltd. to know and understand its customers and their use policy better, which in turn helps Tecxar Consultants Pvt. Ltd. manage unacceptable traffic.

---

### **TRAFFIC FILTRATION AS PART OF THE ROBOCALL MITIGATION PROGRAM**

- **Callee Number Management:** Utilized for customer traffic which is sent to Tecxar Consultants Pvt. Ltd. via a LCR engine. Callee Number Management is used to identify and block originating telephone numbers that are deemed abusive based on repeat attempts to reach the Tecxar Consultants Pvt. Ltd. network.

Through reports generated by Call Detail Record (“CDR”) and pattern trends, proactive monitoring and complaints, Tecxar Consultants Pvt. Ltd. can identify potential unlawful robocalling. In some situations, when Tecxar Consultants Pvt. Ltd. suspects it has identified unlawful calling, in addition to taking the steps identified above, it also may contact the party sending Tecxar Consultants Pvt. Ltd. the 3 calls (i.e., Tecxar Consultants Pvt. Ltd.’s carrier/provider customer), and request that they work to investigate their customers (e.g., to identify the party sending them the calls, determine whether the calls are unlawful, and then to eliminate the source of the calling). When Tecxar Consultants Pvt. Ltd. believes it has identified fraudulent activity, it reserves the right to take any action it deems necessary to eliminate the fraudulent activity.

When the Company identifies potentially fraudulent, abusive, suspicious, or robocalling traffic patterns; it acts swiftly to mitigate this activity. Mitigation includes, but is not limited to,

- (1) Blocking or rejecting known fraudulent/abusive traffic or invalid calling numbers utilizing the appropriate Session Initiation Protocol (SIP) response codes.
- (2) Blacklisting a known abusive number
- (3) Tracing the call traffic back to the originating party
- (4) Reporting instances of irregular traffic activity to our carrier customer
- (5) Requiring the customer to remediate and detail the cause of said irregular traffic
- (6) Acting such as suspension or termination for violations.

All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

**Robocall Mitigation Program** We use software provided by 46 Labs to monitor our outbound voice traffic to identify calling patterns consistent with the origination of robocalls. We immediately investigate any identified calls suspected of being unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

---

#### **Traceback**

Tecxar Consultants Pvt. Ltd. commits to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. Tecxar Consultants Pvt. Ltd. will cooperate with such entities in investigating and stopping any illegal robocalls that use its service to originate calls.

---

#### **STIR/SHAKEN**

Tecxar Consultants Pvt. Ltd. at this time is still working on getting setup with our upstream carriers to verify that calls we send them are signed properly for STIR/SHAKEN. We plan on having this in place quickly and are also working on putting in place the ability for us to sign the calls directly in our soft switches for customers that are known to us and using Caller ID sources that are numbers that they have purchased from us through one of our many upstream carriers.