

TIDEWATER TELECOM, INC. ROBOCALL MITIGATION PLAN

Tidewater Telecom, Inc. (Tidewater) has implemented the following Robocall Mitigation Plan to detect and prevent unlawful robocalls from originating on its network.

All calls that originate on Tidewater's network are subject to the described robocall mitigation program.

Tidewater is currently in the process of transitioning all TDM traffic to our IP switch. Tidewater is included in the signed agreement it's affiliate, Lincolnville Communications, has with Inteliquent to provide SHAKEN authentication services and verification services on the IP switch. Tidewater continues our existing practice to limit the opportunity for fraudulent activity by only programming active and assigned numbers in our switch. Tidewater uses it's affiliate, Lincolnville Communications, Inc., SPC token and digital certificate and all originating calls are signed using this SPC token.

Inteliquent has multiple network tools outlined in their RMP to combat illegal robocalls, that include proactive blocking using DNO lists from US Telecom, SOMOS and Neustar.

Analytics

Inteliquent informs customers by using Tidewater's CNAM service. If a call is suspected to be an illegal robocall or spam call the CNAM information will be replaced with "robocall" or "spam" or a similar designation.

Inteliquent has systems designed to monitor outbound traffic anomalies, trends and activity directed to and from known fraudulent areas. Tidewater is notified of potentially fraudulent activity and investigates the activity within 24 hours. Treatment is applied on the originating ANI until Inteliquent receives a response from Tidewater with a request to remove it.

Our billing vendor, Mid America Computer Corporation (MACC), performs analytics on our switch data and will inform Tidewater of any suspicious activity. LCI investigates the activity, takes appropriate action and communicates the findings to MACC within 24 hours.

Traceback

Tidewater is committed to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. Tidewater commits to responding to traceback requests within 24 hours.

Customer Vetting

Tidewater has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. Tidewater thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Upstream providers

Tidewater's immediate upstream provider, Inteliquent dba ANPI, LLC, is not using its network to carry or process a high volume of illegal traffic. Inteliquent has a RMP in the Robocall Mitigation Database. Tidewater does not directly receive traffic from any foreign originating or intermediate provider. No provider is using Tidewater's network to carry or process a high volume of illegal traffic.

Enforcement

If it is determined a Tidewater customer is originating prohibited unlawful robocalls on our network, Tidewater will either warn the customer to stop or terminate their service as allowed per Tidewater's policies that define the circumstances by which Tidewater will suspend or terminate service to a customer. The policies can be viewed here: <https://tidewater.net/documents/voice-service-use-policy.pdf>

Customer Education

Tidewater posts information on its website to educate customers on how to protect themselves from becoming a victim of unlawful robocallers and a process to report complaints related to robocall activity. Education can be viewed here: <https://tidewater.net/index.php/robocalling-101/>

Updated 2/20/2026