

STIR/SHAKEN Implementation Status and Robocall Mitigation Plan

Tychron Corporation is an active member of the Communications Fraud Control Association (CFCA), along with other major telecommunications carriers and businesses in the United States. According to the summary at <https://cfca.org/>, “the CFCA is a not-for-profit International Association committed to risk management, loss prevention, and fraud control through education, information sharing, and collaboration. The association is comprised of security and risk management professionals from communications service providers, vendor partners, and law enforcement entities working together to stop communication fraud.” Our membership can be verified here: <https://cfca.org/member-companies/>.

The FCC Order lists three affirmative obligations for voice service providers:

- (1) Respond to traceback requests from the Commission, civil and criminal law enforcement, or the Industry Traceback Consortium.
- (2) Take steps to effectively mitigate illegal traffic when it receives notification of such traffic from the Commission through its enforcement bureau.
- (3) implement effective measures to prevent new and current customers from using its network to originate illegal calls.

ROBOCALL MITIGATION

1. Traceback

Tychron agrees to comply with efforts to traceback the source of suspected robocalls.

- We will respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.
- We shall continue to cooperate with traceback requests received directly from carriers, industry associations, law enforcement, and other authorities.
- Call records are created for all calls and are searchable.

Name
Tychron Fraud
Department

Contact Information
Phone: +18448924766
Email: fraud@tychron.com

2. Take Steps to Mitigate Illegal Traffic

Tychron will continue to assist with mitigating suspected illegal activity when the Commission has notified it through its Enforcement Bureau.

3. Measures to Prevent the Origination of Illegal Calls

Know Your Customer:

Tychron’s completion of millions of consumer-consented texts and calls every month illustrates that Tychron has committed substantial resources to its efforts and has significantly strengthened its practices to ensure the legitimacy of messages and calls that traverse our network.

For example, before Tychron initiates service for a new customer, Tychron requires that the new customer provide detailed traffic-profile information including, but not limited to the average length of call (“ALOC”), estimated call types (including how calls will be generated, and whether the traffic is opt-in or otherwise), projected call volumes, and similar information.

Tychron remains alert and responds to reports from consumers and other carriers of suspected fraud calling. If fraudulent calls are detected, Tychron takes steps ranging from requiring the customer to demonstrate traffic legitimacy and explain the discrepancies to suspending traffic from the offending customer until the traffic is verified to be legitimate and compliant.

Tychron's process is dynamic and evolves to address changes in fraud-calling patterns using metrics to identify specific factors.

Tychron currently collects information regarding the new clients that utilize our services and validates that the client is not currently or has not in the past had spam-related complaints; Tychron does not allow the use of dialer traffic on our network as outlined in our AUP, violation of our AUP can result in account termination.

Cease and Desist, and Service Termination:

Tychron issues cease and desist notices to customers whose traffic-origination practices violate laws, rules, and terms and conditions. Tychron continues its traffic-monitoring practices to ensure customer compliance and removes customers who do not respond to such notices and remain non-compliant.

Internal Network Control Flags and Triggers for Mitigating Illicit Robocalling

STIR/SHAKEN IMPLEMENTATION:

Tychron has implemented the STIR/SHAKEN authentication framework in its Internet protocol networks under 47 C.F.R. § 64.6301 as of June 8th, 2021.

TYCHRON