

Robocall Mitigation Plan

KYC Process

A2Z Global 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 A2Z Global from being an intermediate gateway, intentionally or unintentionally, for spoofed or illegal traffic. KYC procedures enable A2Z Global to know and understand its customers and their use policy better, which in turn helps A2Z Global manage unacceptable traffic.

Traceback

A2Z Global commits to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. A2Z Global will cooperate with such entities in investigating and stopping any illegal robocalls that use its service to originate calls.

STIR/SHAKEN Extensions

A2Z Global is a small voice service provider, serving fewer than 100,000 voice service subscriber lines and therefore qualifies for an extension until June 30, 2023 of STIR SHAKEN Implementation under 47 C.F.R. §64.6304(a), which reads:

§64.6304 Extension of implementation deadline.

(a) Small voice service providers. (1) Small voice service providers are exempt from the requirements of §64.6301 through June 30, 2023.

(2) For purposes of this paragraph (a), “small voice service provider” means a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all the provider's affiliates).

Robocall Mitigation Plan

A2Z Global have implemented dialing rules directly on switch to block such fraudulent calls proactively.

- Proactive Plan: Invalid Calling Number Blocking on Switch: A2Z Global’s switch will automatically block all calls that originate from invalid numbers, like short digits, alphanumeric.

In some situations, when A2Z Global suspects it has identified unlawful calling, in addition to taking the steps identified above, it also may contact the party sending A2Z Global the calls (i.e., A2Z Global’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 A2Z Global 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.