

Robocall contact:
Lance Brimhall
Associate General Counsel
lance.brimhall@alianza.com
801-901-3305

Alianza Robocall Mitigation Plan

As part of its Robocall Mitigation Database filing required under the FCC's *Sixth Caller ID Authentication Report and Order* (Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023)), this document describes Alianza's certifications and robocall mitigation plan to detect and prevent unlawful robocalls from originating on its network.

1. Alianza's corporate information

Alianza, Inc. is a Delaware corporation. Its primary address is provided within the Robocall Mitigation Database.

Alianza certifies it has not been prohibited from filing in the Robocall Mitigation Database and Alianza has not been subject to any Commission, law enforcement, or regulatory agency action or investigation arising from suspected unlawful robocalling or spoofing.

In accordance with 47 CFR § 64.6305(e), Alianza has designated a point of contact to receive notice of any illegal robocall traffic or other robocall mitigation-related issues. That person's name, title, address, phone number, and email address are available within the Robocall Mitigation Database.

2. STIR/SHAKEN certification

Alianza hereby certifies that all voice traffic originating on its network is authenticated in compliance with applicable standards under 47 CFR § 64.6301.

3. Know-your-upstream-provider procedures

Alianza has existing agreements with Tier-1 carrier service providers from which it facilitates the provision of carrier services to its service provider customers. Alianza has confirmed that each of those carriers are listed in the RMD. Alianza also enables its customers to contract directly with carrier service providers to enable those customers' use of Alianza's Cloud Communications Platform. In each case, Alianza has provided detailed onboarding and fraud detection guidance to require and enable its customers to comply with their obligations to prevent and mitigate illegal robocalling.

4. Know-your-customer procedures

Alianza's customers are internet or telephony service providers who resell Alianza's cloud communications services to their end users. Accordingly, they have their own STIR/SHAKEN obligations. While Alianza's STIR/SHAKEN compliance efforts work hand-in-hand with its customers' STIR/SHAKEN

compliance efforts, each service provider customer must develop and file its own robocall mitigation plan.

At the beginning of each customer relationship, Alianza's sales and customer success teams engage in a discovery process with each potential customer to understand the customer's subscriber base and to educate those potential customers about the operation of Alianza's Cloud Communications Platform. During the discovery process, Alianza shares critical information about its fraud detection and prevention processes. That information remains available to each service provider after it transitions to become Alianza's customer.

5. Contractual terms and other conditions

Alianza's customer agreements allow Alianza to immediately terminate any services to any subscriber that engages in automated call blasting, mass calling, or other fraudulent, illegal, or prohibited activity.

Alianza's agreements with its underlying carriers also include provisions requiring the parties' compliance with applicable robocall prevention and mitigation standards.

6. Fraud detection and mitigation

Alianza has implemented a proprietary fraud detection and mitigation process through which it analyzes high-volume network traffic to evaluate compliance with a variety of fraud detection indicators and fraud prevention best practices. As part of this process, Alianza notifies customers of potentially fraudulent activity occurring in any of their subscriber accounts. Detailed information about this fraud detection and mitigation process is provided to each customer through Alianza's knowledge base and support resources. If Alianza takes action against a customer's subscriber, it will notify the customer and share required steps to restore service, if any.

Alianza does not use a third-party vendor for call analytics and blocking.

Additionally, Alianza complies with FCC requirements to maintain and enforce a Do Not Originate (DNO) list designed to block calls from numbers that should not place outbound calls.

7. Enforcement

Alianza will respond to traceback requests within 24 hours. Alianza also cooperates with law enforcement and with its carrier partners to investigate illegal robocallers and prevent them from using Alianza's services to originate calls. Alianza employees engage directly with Alianza's customers to suspend or disable subscriber accounts identified as originating unlawful robocalls through Alianza's network.

8. Updates

Alianza will update this robocall mitigation plan within 10 days of any change.