

Astrea 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 Astrea's certifications and robocall mitigation plan to detect and prevent unlawful robocalls from originating on its network.

1. Astrea's Corporate Information

CCI Systems, Inc. D/B/A Astrea is a Michigan corporation. Its primary address is provided within the Robocall Mitigation Database.

Astrea certifies it has not been prohibited from filing in the Robocall Mitigation Database and Astrea 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), Astrea 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

Astrea 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

Astrea has existing agreements with its direct upstream providers who in turn have existing agreements with Tier-1 carrier service providers from which it facilitates the provision of carrier services to its service provider customers. Astrea has confirmed that each of those carriers are listed in the RMD. In each case, Astrea's providers have 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

Upon request, Astrea shares critical information about its provider's fraud detection and prevention processes with customers.

5. Contractual Terms and Other Conditions

Astrea's customer agreements contain fair use and protection policies that allow Astrea to immediately terminate any services to any subscriber or device to prevent automated call blasting, mass calling events, and other fraudulent or illegal activity.

Astrea agreements with its underlying carrier services providers also include provisions requiring the parties' compliance with applicable robocall prevention and mitigation standards.

6. Fraud Detection and Mitigation

Astrea's provider 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. Through this fraud detection and mitigation process, Astrea's provider then notifies Astrea of potentially fraudulent activity occurring in any of that customer's subscriber accounts. Detailed information about this fraud detection and mitigation process is provided to each customer through Astrea's knowledge base and support resources. Astrea may take remedial action against any subscriber's account to prevent or remediate robocalling or other fraudulent activity. If Astrea's provider takes any such action, its fraud detection system triggers notification to Astrea of that action and any remedial steps that may be taken to restore service .

7. Enforcement

Astrea and its providers promptly responds to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group. Astrea and its providers also cooperates with those entities and with its carrier partners to investigate and prevent any illegal robocallers from using Astrea's services to originate calls. Astrea employees engage directly with Astrea's customers to suspend or disable subscriber accounts identified as originating unlawful robocalls through Astrea's network.