

**Jackson Energy Authority
Robocall Mitigation Plan
FRN 0008197303**

Consistent with FCC regulations,¹ Jackson Energy Authority submits this Robocall Mitigation Plan.

STIR/SHAKEN COMPLIANCE

Implementation Status. We have implemented the STIR/SHAKEN authentication framework on our network through our partnership with TransNexus and all calls originating on our network are compliant with 47 CFR § 64.6301(a)(1) and (2).

Call Chain. We are registered with the STI-PA under OCN 150G and serve end-users as a voice service provider.

Traceback Requests. We respond within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. We have designated a point of contact and that person's name, title, address, phone number and email address are in the Robocall Mitigation Database portal.

Eligibility. We have not been prohibited from filing a certification in the Robocall Mitigation Database and do not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations or related state law violations.

EFFORTS TO PREVENT ILLEGAL ROBOCALL TRAFFIC

Investigation and Enforcement. We have implemented a STRIR/SHAKEN solution supplied by TransNexus and use call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list. We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

Know Your Customer – Commercial. We diligently verify the identities of new commercial customers by gathering essential information, including the physical address, contact individuals, federal tax identification, and an understanding of the customer's business nature. This includes assessing whether and how they intend to use auto-dialers or similar robocall mechanisms in

¹ 47 C.F.R. §§ 64.6303-6305.

their operations. Our contracts and policies incorporate specific language aimed at mitigating robocalls, explicitly forbidding the use of our platforms for making or receiving unlawful calls. We conduct thorough evaluations of each customer.

Know Your Customer – Residential. We diligently verify the identities of new residential customers by gathering essential information, including name, physical address and social security number(s). Our contracts and policies incorporate specific language aimed at mitigating robocalls, explicitly forbidding the use of our platforms for making or receiving unlawful calls. We conduct thorough evaluations of each customer.

Know Your Upstream Provider. We diligently verify our upstream providers – providers that send us voice traffic that we terminate or transit to other providers – and do not accept voice traffic from unregistered providers. We mandate that our upstream providers implement effective robocall mitigation strategies, including customer and provider vetting processes, and employ call analytics to detect suspicious traffic. Our agreements with these providers strictly prohibit the transmission of illegal robocalls to our network. Should we identify an upstream provider transmitting suspect robocalls, they are initially warned, and persistent non-compliance results in the termination of their services.

Additional Steps. As part of our robocall mitigation program, we have also implemented a variety of measures to prevent illegal robocalls from originating on our network. Together, these measures seek to prevent illegal robocall activity and proactively identify and investigate calling patterns indicative of illegal robocall activity. These measures include robocall mitigation language in all contracts, actively monitoring traffic moving through our network, real-time controls on customer traffic, Caller-ID confirmation checks, and monitoring industry-wide trends.

Updated February 26, 2026