

Daztel Communications maintains a comprehensive robocall mitigation framework designed to comply with all current FCC requirements, STIR/SHAKEN authentication standards, and industry best practices. Our network is fully STIR/SHAKEN compliant, and we cooperate completely with the USTelecom Industry Traceback Group (ITG), submitting timely responses and supporting investigations whenever necessary. We operate with a proactive, zero-tolerance approach toward illegal or fraudulent traffic, and our policies are designed to protect our upstream partners, our own network, and the telecom ecosystem as a whole.

To ensure that only legitimate traffic enters our network, we apply strict verification measures during onboarding and throughout the customer lifecycle. Every customer must undergo a detailed Know-Your-Customer (KYC) process in which we review their business model, call types, campaign descriptions, volume expectations, duration norms, and intended use cases. We require all customers to demonstrate a clear understanding of their own clients and the nature of the traffic they originate. In addition, we require customers to be registered and cooperative with the Industry Traceback Group; this ensures transparency and accountability should any inquiries arise.

Caller authentication and attestation are managed under a controlled policy. Daztel assigns only Attestation A or B based on the level of verification we obtain; we do not issue Attestation C. When a customer cannot meet the criteria necessary for authenticated signing, is blocked entirely. U.S. domestic caller IDs may only be used by providers based within the United States, and any customer outside the U.S. requesting the use of a U.S. caller ID must provide a valid business justification and proof of legitimate number ownership. Wireless ANIs are blocked by default for short-duration traffic, and are only enabled when we review and approve a verifiable, lawful business use case. Daztel also enforces compliance with all Do-Not-Call (DNC) requirements and expects customers to maintain appropriate internal processes to honor consumer consent rules.

Our monitoring and blocking framework combines automated systems with active oversight from our NOC. We continuously observe call patterns to identify anomalies, short-duration spikes, suspicious ANI behavior, reputation alerts, or any indicators of spoofed or non-compliant campaigns. Daztel performs calling-number reputation checks and validation using multiple industry resources. Any call presenting a number outside the NANP range or failing to comply with E.164 formatting, or any call with unclear jurisdiction, may be treated as indeterminate and handled accordingly—either rerated, restricted, or blocked depending on risk.

When a traceback request is received, we respond immediately and follow a clear escalation workflow. We review the call source, analyze metrics, verify campaign details, and listen to audio when available. We then notify the customer, require corrective action, and take protective measures on our side, such as suspending traffic or blocking specific ANIs if necessary. We fully cooperate with the ITG through the portal, submit comments and supporting details promptly, and assist until the matter is resolved. All incidents, responses, and customer interactions are documented and used to strengthen future monitoring.

Our operations are fully IP-based, simplifying the enforcement of STIR/SHAKEN requirements and eliminating complications associated with non-IP traffic. As part of our adherence to the 2025 FCC Order, we have integrated expanded record-retention practices, internal compliance escalation procedures, and enhanced gateway-level verification controls. We continue to refine our monitoring processes to ensure that emerging threats, new regulatory expectations, and evolving industry patterns are addressed immediately and consistently.

Overall, Daztel is committed to maintaining a highly compliant, transparent, and secure telecom environment. Our internal policies, traffic monitoring, customer verification, and traceback cooperation efforts collectively ensure that only lawful, authenticated, and responsible traffic flows across our network. This framework protects our partners and reinforces our commitment to upholding the highest standards of network integrity.