

Crown Correctional Telephone, Inc. Robocall Mitigation Plan

COMPANY OVERVIEW

Crown Correctional Telephone, Inc. (“Crown Correctional” or “Company”) provides incarcerated people’s communications services (“IPCS”) to correctional facilities within the United States. These services allow incarcerated individuals to place **outgoing voice calls only** to approved called parties outside the correctional facility. Crown Correctional does not permit inbound voice calling to incarcerated individuals.

Crown Correctional is a non-facilities-based voice service provider and reseller. The company does not own or operate network facilities used to originate calls into the public switched telephone network (PSTN). All calls placed through Crown Correctional’s system are originated, transmitted, and authenticated by the Company’s contracted underlying carriers.

Crown Correctional relies on its underlying originating providers, including Network Communications International Corp. (NCIC) and Encartele to originate calls and apply STIR/SHAKEN authentication and attestation. Each underlying provider is responsible for implementing STIR/SHAKEN in accordance with the FCC rules and maintaining its own certification in the FCC Robocall Mitigation Database.

STIR/SHAKEN IMPLEMENTATION STATUS

Crown Correctional is a non-facilities-based reseller and does not control the network infrastructure used to originate calls to the PSTN. Crown Correctional does not possess an Operating Company Number (OCN) and is not eligible to obtain a Service Provider Code (SPC) token under Secure Telephone Identity Governance Authority policies. As a result, Crown Correctional is unable to implement STIR/SHAKEN directly.

All calls placed through Crown Correctional’s system are originated and authenticated by its contracted underlying carriers, including NCIC and an additional originating provider. Those carriers apply STIR/SHAKEN attestation consistent with their FCC Robocall Mitigation Database certifications. Crown Correctional contractually requires its underlying providers to comply with all applicable FCC robocall mitigation and call authentication requirements.

Robocall Mitigation Program

Crown Correctional has implemented a Robocall Mitigation Program (“RMP”) designed to prevent, detect, and mitigate illegal robocall traffic consistent with FCC requirements outlined in the Commission’s recent release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023). In compliance with the Report & Order, Crown Correctional Communications submits this RMP and certification.

CONTROLLED CALLING ENVIRONMENT

Crown Correctional's services operate within a highly controlled correctional facility environment:

- Calls may only be placed by authenticated incarcerated individuals
- Each incarcerated user is assigned a unique account or identifier
- Calls must be manually initiated by the user; automated dialing capability is not available
- Calls may only be placed to approved numbers
- Called parties must affirmatively accept calls before completion
- Facilities monitor and record calls in accordance with correctional policies
- Call duration and frequency are subject to system controls

Because of this controlled environment, the risk of illegal robocall origination is significantly limited.

KNOW YOUR CUSTOMER (KYC) PROCEDURES

Crown Correctional's customers are government-operated correctional facilities and their authorized users.

Mitigation and customer verification measures include:

- Contracts executed with correctional facilities
- Verification of facility authority and service eligibility
- Authentication of incarcerated users through facility systems
- Assignment of individual inmate calling accounts
- Monitoring of account usage and call patterns
- Ability to suspend or terminate accounts if misuse is suspected

Crown Correctional does not provide anonymous voice services.

TRAFFIC MONITORING AND MITIGATION

Crown Correctional works in coordination with its underlying carriers to monitor and mitigate potentially unlawful traffic.

Mitigation steps include:

- Monitoring call volumes and patterns for anomalies
- Reviewing reports or notifications from underlying carriers
- Investigating suspicious activity
- Suspending or terminating service if illegal robocalling is suspected
- Cooperating with underlying carriers to block or restrict traffic where necessary

Crown Correctional relies on its underlying carriers' network-level analytics and mitigation tools to detect and block illegal robocalls.

CALL BLOCKING AND CONSUMER CONTROLS

Crown Correctional's system allows called parties to request blocking of calls from specific incarcerated individuals. Upon request, numbers can be placed on a do-not-call or block list to prevent further calls. Because Crown Correctional does not accept inbound PSTN calls, it does not receive traffic from providers that would require Robocall Mitigation Database monitoring for inbound calls.

TELEPHONE NUMBER AUTHORIZATION

Crown Correctional does not obtain numbering resources directly from numbering authorities. All telephone numbers used in connection with Crown Correctional's services are obtained and managed by its underlying originating carriers in compliance with FCC numbering rules.

TRACEBACK COOPERATION

Crown Correctional commits to respond fully and within twenty-four (24) hours to all traceback requests from the Federal Communications Commission, law enforcement, and the Industry Traceback Group. Crown Correctional will cooperate with its underlying carriers, including NCIC and its additional originating provider, to investigate and mitigate any suspected illegal robocall traffic and will provide relevant call records as required.

If Crown Correctional identifies or is notified of illegal robocall activity originating from its services, it will take immediate action, including suspension or termination of service where appropriate.

Traceback Contact Information

Name	Title	Contact Information
RYAN BARTULA	PRESIDENT	888-639-6789 RYAN@CROWNPHONESERVICE.COM

ONGOING COMPLIANCE

Crown Correctional will:

- Maintain accurate information in the FCC Robocall Mitigation Database
- Update its filing within 10 business days of any material change
- Continue to require its underlying carriers to maintain STIR/SHAKEN compliance
- Cooperate with regulators and industry traceback efforts

CONCLUSION

Crown Correctional Telephone, Inc. submits this Robocall Mitigation Plan in compliance with FCC rules and the requirements of the Robocall Mitigation Database. As a non-facilities-based reseller that relies on underlying originating carriers for call authentication, Crown Correctional has implemented reasonable and appropriate mitigation measures to prevent its services from being used to originate illegal robocalls and will continue to monitor and update its program as necessary.