Colorado River Communications, Inc.

ROBOCALL MITIGATION PROGRAM

Non-Facilities-Based Voice Service Provider and White-Label Reseller

FCC Registration Number (FRN)	0027578970
Operating Company Number (OCN)	Not Applicable
Underlying Wholesale Provider	SkySwitch (contracting legal entity to be verified)
Services	White-label SIP Trunking and UCaaS
Customer Classes	Residential and commercial end users; approved reseller/wholesale accounts
Effective Date	August 1, 2026
Version	1.0
Compliance Officer	Bryan Toy, Vice President

This program is designed to support CRC's FCC Robocall Mitigation Database filing. It must accurately describe CRC's actual practices on the date signed. It is not a substitute for advice from telecommunications regulatory counsel.

Document Control and Pre-Signature Verification

Document owner: Vice President / Compliance Officer

Applies to: Colorado River Communications, Inc. ("CRC"), its employees, contractors, customer-facing personnel, provisioning personnel, and any third party acting on CRC's behalf in connection with voice services.

Document status: Version 1.0, prepared for adoption effective August 1, 2026.

Approval Record

Role	Name	Approval / Signature	Date
Compliance Officer	Bryan Toy		8/1/2026
Authorized Representative	Bryan Toy		8/1/2026

Table of Contents

Document Control and Pre-Signature Verification 2
Approval Record 5
1. Executive Summary 5
2. Purpose, Scope, and Policy Objectives 5
2.1 Purpose 5
2.2 Scope 5
2.3 Objectives 5
2.4 No Guarantee of Legality 5
3. Regulatory Framework and Filing Commitments 5
3.1 Core Commitments 6
3.2 Public Filing Considerations 6
3.3 Material Changes 6
4. Business and Service Delivery Model 6
4.1 CRC Role 6
4.2 SkySwitch Role 6
4.3 Shared and Coordinated Responsibilities 6
4.4 Customer Classes 6
5. Governance, Roles, and Accountability 6
5.1 Compliance Officer 6
5.2 Responsibilities by Function 7
5.3 Escalation Authority 7
6. Customer Identification and Risk-Based Onboarding 7
6.1 General Standard 7
6.2 Minimum Residential Verification 7
6.3 Minimum Commercial Verification 7
6.4 Enhanced Review Triggers 7
6.5 Reseller and Wholesale Accounts 7
6.6 Renewal and Material Change Review 8
7. STIR/SHAKEN and Caller ID Authentication 8
7.1 Stated Implementation Status 8
7.2 Third-Party Authentication Arrangement 8
7.3 Attestation Controls 8
7.4 Caller ID Authorization 8
7.5 Verification of Inbound Calls 8
8. Know-Your-Upstream-Provider and Vendor Oversight 8
8.1 Upstream Provider Identification 8
8.2 Initial and Periodic Due Diligence 8
8.3 No Blind Reliance 8
8.4 Alternative or Additional Providers 8
9. Customer Agreements and Acceptable Use Controls 8
9.1 Prohibited Uses 8
9.2 Customer Representations 9
9.3 Audit and Information Rights 9
9.4 Emergency and Public Safety Protections 9
10. Monitoring, Data Analytics, and Complaint Intake 9
10.1 CRC Monitoring Model 9
10.2 Underlying Provider Analytics 9
10.3 Risk Indicators 9
10.4 Complaint Intake 9
10.5 Data Analytics Statement for RMD 9
11. Investigation and Risk Assessment Procedures 10
11.1 Intake and Triage 10
11.2 Risk Levels 10
11.3 Decision Standard 10

11.4 False Positives and Redress 10
12. Mitigation, Suspension, and Termination 10
12.1 Available Mitigation Measures 10
12.2 Customer Non-Cooperation 10
12.3 Related Accounts 10
12.4 Post-Termination Controls 10
13. Traceback Response Program 11
13.1 Commitment 11
13.2 Internal Service Levels 11
13.3 Response Content 11
13.4 Coverage and Continuity 11
13.5 Traceback Follow-Up 11
14. Regulatory Notices and Suspected Illegal Traffic 11
14.1 Notification Handling 11
14.2 Immediate Containment 11
14.3 Preventive Measures for New and Renewing Customers 11
14.4 Communications 11
15. Record Retention, Confidentiality, and Evidence Preservation 12
15.1 Seven-Year Retention Standard 12
15.2 Covered Records 12
15.3 Preservation Hold 12
15.4 Confidentiality and Access 12
16. Training, Testing, and Program Review 12
16.1 Training 12
16.2 Annual Review 12
16.3 Sample Testing 12
16.4 Corrective Action 12
17. RMD Filing Administration 12
17.1 Filing Responsibility 12
17.2 Current CRC Filing Profile 13
17.3 Update and Recertification Calendar 13
17.4 Supporting File 13
Appendix A - Customer Onboarding and KYC Checklist 13
Appendix B - Investigation and Mitigation Worksheet 14
Appendix C - Traceback Response Worksheet 14
Appendix D - Annual RMD and Program Review Checklist 15
Appendix E - Regulatory Reference Matrix for CRC Review 15
Appendix F - Revision History 16
18. Authorized Representative Certification and Signature 17

Page numbers reflect this version. Review and update the table after material edits.

1. Executive Summary

Colorado River Communications, Inc. ("CRC") is a non-facilities-based voice service provider and white-label reseller. CRC obtains the underlying SIP Trunking and Unified Communications as a Service ("UCaaS") platform from SkySwitch and offers CRC-branded services to residential and commercial end users. CRC may also serve approved business or reseller accounts where the intended use and downstream responsibilities are documented.

SkySwitch operates the core hosted platform, switching environment, network interconnections, and network-level technical functions available under CRC's wholesale arrangement. CRC does not claim to own or independently operate those facilities. CRC nevertheless remains responsible for the regulatory obligations that apply to CRC as the provider serving its customers, including accurate RMD filing, customer identification and due diligence, prevention of customer misuse, cooperation with traceback requests, response to suspected illegal traffic, and maintaining an appropriate robocall mitigation program.

This Program establishes specific reasonable steps CRC will use to avoid originating illegal robocall traffic associated with CRC customers. Those steps are risk-based and include customer verification, intended-use review, contractual restrictions, account and telephone-number controls, review of available call and complaint information, coordination with SkySwitch, timely investigation, service restriction or termination, traceback cooperation, record retention, training, and periodic review.

2. Purpose, Scope, and Policy Objectives

2.1 Purpose

The purpose of this Robocall Mitigation Program ("Program" or "RMP") is to document the controls CRC uses to prevent, identify, investigate, and mitigate illegal robocalls and unlawful caller ID spoofing. The Program is intended to support CRC's certification in the FCC Robocall Mitigation Database ("RMD") and CRC's ongoing compliance with applicable caller ID authentication, call-blocking, traceback, and customer due-diligence requirements.

2.2 Scope

This Program applies to all voice traffic associated with CRC customer accounts and all CRC activities related to marketing, onboarding, provisioning, number assignment, service changes, billing, customer support, complaint handling, regulatory response, and termination of voice service. It applies to residential accounts, commercial accounts, SIP trunking, UCaaS, and any approved reseller or wholesale arrangement.

2.3 Objectives

- Know CRC's customers and understand the expected use of voice services.
- Prevent new and renewing customers from using CRC-branded services to originate illegal calls.
- Maintain clear responsibility between CRC and SkySwitch without treating outsourcing as a transfer of CRC's regulatory duties.
- Identify suspicious calling activity using information reasonably available to CRC.
- Respond fully and within applicable time limits to traceback requests and regulatory inquiries.
- Take prompt, proportionate action to stop identified or reasonably suspected illegal traffic.
- Keep the RMD filing accurate, current, and consistent with actual operational practices.

2.4 No Guarantee of Legality

STIR/SHAKEN authentication, a valid caller ID, or successful completion of onboarding does not establish that a call is lawful. CRC treats authentication, customer verification, traffic characteristics, complaints, and traceback information as separate inputs to a risk-based compliance determination.

3. Regulatory Framework and Filing Commitments

CRC maintains this Program under the federal framework addressing illegal robocalls and caller ID authentication, including the TRACED Act, 47 CFR Part 64, and FCC orders and guidance concerning the RMD, STIR/SHAKEN, traceback, customer due diligence, and mitigation of illegal traffic.

3.1 Core Commitments

- Implement and maintain an appropriate robocall mitigation program for calls associated with CRC customers.
- Describe the specific reasonable steps used to avoid originating illegal robocall traffic, rather than relying on general or conclusory statements.
- Know CRC's end-user customers and exercise due diligence to prevent use of CRC services to originate illegal traffic.
- Describe procedures used to know CRC's upstream provider, SkySwitch.
- Respond fully to traceback requests from the FCC, law enforcement, and the registered traceback consortium within 24 hours, using the timing rules applicable to such requests.
- Update the RMD filing within 10 business days of any change to filed information and recertify annually on or before March 1.
- Ensure all filed information is accurate and truthful and promptly correct any identified deficiency.

3.2 Public Filing Considerations

CRC understands that the RMP description submitted to the RMD may be publicly accessible. CRC will avoid including customer-specific confidential information, security-sensitive technical details, account credentials, or contractual terms that are not necessary to describe its mitigation program. CRC will evaluate whether any limited confidential-treatment request is appropriate before filing information that identifies vendor analytics or other commercially sensitive material.

3.3 Material Changes

A change is material when it could make a statement in CRC's RMD filing inaccurate, including changes in ownership, principals, affiliates, addresses, contact information, STIR/SHAKEN status, underlying provider, services offered, customer classes, or mitigation procedures. The Compliance Officer will evaluate and file required updates within 10 business days.

4. Business and Service Delivery Model

4.1 CRC Role

CRC markets, sells, provisions, bills, and supports CRC-branded SIP Trunking and UCaaS services. CRC is the principal customer-facing entity for residential and commercial end users served under CRC's brand. CRC performs or controls customer onboarding, identity verification, intended-use review, account approval, account administration, customer communication, acceptable-use enforcement, and escalation to SkySwitch.

4.2 SkySwitch Role

SkySwitch is CRC's underlying white-label platform and wholesale service provider. Subject to the applicable agreement and technical configuration, SkySwitch supplies the hosted voice platform, switching and routing functions, platform-level provisioning, network interconnection, telephone-number and carrier interfaces, call detail and operational reporting, and network-level technical controls used to deliver service.

4.3 Shared and Coordinated Responsibilities

CRC and SkySwitch may each possess different information needed to investigate a call. CRC generally possesses customer identity, account history, billing, service requests, and customer communications. SkySwitch generally possesses or controls platform-level routing, signaling, authentication, carrier-interface, and network mitigation information. CRC will promptly coordinate with SkySwitch when a complaint, traceback, or investigation requires information or action not independently available to CRC.

4.4 Customer Classes

Customer class	Typical use	Primary compliance focus
Residential	Personal household calling	Identity, address, payment consistency, unusual volume, complaints
Commercial end user	Business communications, contact centers, offices, remote workers	Business legitimacy, intended campaigns, caller ID authority, volume profile
SIP trunk / high-volume business	PBX, contact center, application calling	Enhanced KYC, use-case approval, traffic profile, number authorization, monitoring
Approved reseller / wholesale	Downstream service or resale only when approved	RMD status if applicable, downstream KYC, contractual flow-down, nested-reseller controls

5. Governance, Roles, and Accountability

5.1 Compliance Officer

Name: Bryan Toy
Title: Vice President
Telephone: (928) 505-7301
Email: bryan@crc-inc.net

The Compliance Officer owns this Program and has authority to require records, pause provisioning, restrict traffic, suspend or terminate service, direct communications with SkySwitch, and retain outside counsel or technical assistance when appropriate.

5.2 Responsibilities by Function

Function	Responsibilities
Sales	Accurately describe services; collect intended-use information; avoid promising unrestricted or anonymous calling.
Provisioning / Operations	Verify approvals; provision only approved numbers and services; preserve account and configuration records; implement restrictions.
Customer Support	Log complaints; preserve call examples; escalate spoofing, fraud, or high-volume complaints promptly.
Billing / Administration	Maintain payment and account records; report inconsistent identity or payment information.
Compliance Officer	Approve higher-risk accounts; manage investigations and traceback; coordinate with SkySwitch and regulators; maintain RMD accuracy.
Management	Provide resources and support enforcement decisions, including suspension or termination when required.

5.3 Escalation Authority

Any employee may escalate suspected illegal calling to the Compliance Officer without first obtaining customer approval. The Compliance Officer may impose temporary restrictions while an investigation is pending when delay could allow continued illegal traffic or impair CRC's ability to respond to a traceback or regulatory notice.

6. Customer Identification and Risk-Based Onboarding

6.1 General Standard

CRC will know its end-user customers and exercise due diligence to ensure its services are not used to originate illegal traffic. No account will be activated solely on the basis of an online order or payment where material identity, intended-use, or risk questions remain unresolved.

6.2 Minimum Residential Verification

- Full legal name and date of birth or other reasonable identity verification information.
- Physical service address and billing address; explanation of material discrepancies.
- Reliable telephone number and email address.
- Payment method reasonably associated with the subscriber or an explained authorized payer.
- Intended service location and anticipated number of users or lines.
- Acknowledgment of CRC's acceptable-use and caller ID requirements.

6.3 Minimum Commercial Verification

- Legal business name, trade name, entity type, formation jurisdiction, and active registration where applicable.
- Employer Identification Number or other tax identifier when reasonably available.
- Physical business address, website/domain, business telephone number, and business email domain.
- Identity and authority of the individual ordering and administering service.
- Description of business operations and intended calling use, including expected monthly volume and peak calling patterns.
- Identification of automated, prerecorded, predictive-dialer, lead-generation, debt-collection, political, charitable, healthcare, or contact-center use.
- Evidence of authority to use caller ID numbers not assigned through the CRC/SkySwitch service.

6.4 Enhanced Review Triggers

Enhanced review is required when one or more risk indicators are present, including unusually high requested capacity; rapid activation; multiple unrelated caller ID numbers; virtual or non-verifiable addresses; anonymous payment methods; inconsistent identity information; use cases historically associated with illegal calling; offshore control; previous service termination; adverse complaints; inability to explain traffic; or requested resale to downstream users.

6.5 Reseller and Wholesale Accounts

CRC will not knowingly permit an account to resell or provide voice service to downstream end users unless the arrangement is disclosed and approved in writing. CRC may require the account to provide its FRN and RMD filing information, identify principals and downstream customer classes, maintain its own KYC procedures, flow down acceptable-use requirements, respond to CRC inquiries, and prohibit undisclosed nested resellers. Approval may be withheld where CRC cannot reasonably identify the responsible party for traffic.

6.6 Renewal and Material Change Review

CRC will treat a material ownership change, major traffic expansion, new call-center use, new geographic market, new reseller activity, or repeated compliance issue as a renewal event requiring updated KYC and risk review. CRC may require periodic re-verification of customer information even where no specific change is reported.

7. STIR/SHAKEN and Caller ID Authentication

7.1 Stated Implementation Status

CRC has represented that STIR/SHAKEN is fully implemented for applicable IP-based calls through its arrangement with SkySwitch. SkySwitch performs platform-level technical functions. CRC will not rely on the existence of a vendor arrangement as a substitute for satisfying any caller ID authentication obligation that applies directly to CRC.

7.2 Third-Party Authentication Arrangement

Before signing this Program and selecting a full-implementation certification in the RMD, CRC will document whether CRC is registered with the STIR/SHAKEN Policy Administrator, possesses its own SPC token and certificate where required, makes attestation-level decisions, and ensures calls are authenticated using the certificate required by FCC rules. CRC will retain written confirmation from SkySwitch or other competent technical evidence supporting the selected RMD status.

7.3 Attestation Controls

CRC will assign or cause the assignment of attestation levels only when supported by the relationship to the customer and the customer's right to use the calling number. CRC will not treat an A-level attestation as appropriate merely because a customer pays for service or supplies a caller ID. Customer identity and number authorization must support the attestation decision.

7.4 Caller ID Authorization

- Numbers assigned through the CRC/SkySwitch service may be used by the assigned customer subject to account controls.
- Use of externally obtained numbers requires reasonable evidence that the customer is authorized to use the number.
- CRC may reject or restrict invalid, unallocated, unassigned, malformed, or misleading caller ID information.
- Customers may not alter caller ID to impersonate another person or entity, evade blocking, conceal the source of calls, or facilitate fraud.
- CRC may require remediation or suspension when caller ID use creates repeated complaints or traceback activity even if formal illegality has not yet been established.

7.5 Verification of Inbound Calls

To the extent inbound verification information and call treatment are provided through SkySwitch, CRC will use available results for customer support, fraud review, and mitigation. CRC will not represent to customers that verification proves the legality or identity of a caller.

8. Know-Your-Upstream-Provider and Vendor Oversight

8.1 Upstream Provider Identification

CRC's primary underlying provider is SkySwitch. CRC will maintain the applicable contract, legal entity name, business address, compliance contact, technical escalation contact, and RMD information reasonably necessary to identify and communicate with SkySwitch.

8.2 Initial and Periodic Due Diligence

- Verify SkySwitch's identity and contracting entity.
- Confirm that the applicable SkySwitch entity appears in the RMD where required and retain evidence of the review.
- Understand the division of STIR/SHAKEN, traceback, traffic-monitoring, and blocking responsibilities.
- Confirm how CRC can obtain call detail, routing, signaling, and customer-level information needed for investigations.
- Maintain current contacts for urgent traceback and suspected-illegal-traffic requests.
- Review material notices, service changes, enforcement actions, or RMD changes affecting the relationship.

8.3 No Blind Reliance

CRC will not state that SkySwitch is solely responsible for robocall compliance. Outsourcing technical functions does not eliminate CRC's obligation to know its customers, respond to traceback, keep its RMD filing accurate, or take reasonable measures to prevent customer misuse.

8.4 Alternative or Additional Providers

Before adding another upstream carrier, platform, number provider, or authentication vendor, CRC will perform equivalent due diligence, document responsibilities, and evaluate whether the addition requires an RMD update within 10 business days.

9. Customer Agreements and Acceptable Use Controls

9.1 Prohibited Uses

CRC customer agreements, service terms, or acceptable-use policies will prohibit:

- Illegal robocalls or calls made without required consent or other legal authority.
- Unlawful spoofing, impersonation, fraud, phishing, extortion, threats, or deception.
- Use of invalid, unallocated, unassigned, or unauthorized caller ID information.
- Traffic pumping, artificial inflation of traffic, one-ring scams, or other schemes intended to generate improper compensation or consumer response.
- Circumvention of call blocking, labeling, authentication, traceback, or compliance controls.
- Resale or downstream provisioning without CRC's prior written approval.
- Failure to provide accurate account information or cooperate with a compliance investigation.

9.2 Customer Representations

CRC may require customers to represent that they will comply with the Telephone Consumer Protection Act, Telemarketing Sales Rule, Do-Not-Call requirements, caller ID laws, consent requirements, state law, and industry rules applicable to their calls. CRC does not undertake to determine every legal requirement applicable to a customer's campaign and may require the customer to obtain its own legal advice.

9.3 Audit and Information Rights

CRC may require call samples, consent records, scripts, campaign descriptions, customer lists or lead-source descriptions, number-authorization records, and other information reasonably necessary to investigate suspected illegal traffic. Failure to provide timely and credible information is an independent basis for restriction or termination.

9.4 Emergency and Public Safety Protections

Mitigation actions will be designed to avoid improper interference with 911 calls, public safety answering points, and government emergency numbers. When technically feasible, CRC will coordinate targeted restrictions with SkySwitch rather than broadly blocking lawful traffic.

10. Monitoring, Data Analytics, and Complaint Intake

10.1 CRC Monitoring Model

CRC does not represent that it independently operates a proprietary network-wide robocall analytics platform. CRC uses information reasonably available through CRC systems and the SkySwitch platform, including account information, provisioning records, call detail records, traffic reports, customer support data, payment information, complaints, traceback requests, and notices from SkySwitch or other providers.

10.2 Underlying Provider Analytics

To the extent CRC relies on network-level analytics or traffic analysis performed by SkySwitch, CRC identifies SkySwitch as the underlying provider supporting those functions. CRC will describe that reliance accurately in its RMD plan and will not identify a specific third-party analytics vendor unless CRC has verified the vendor and the role it performs.

10.3 Risk Indicators

- A sudden or unexplained increase in outbound traffic, concurrent calls, or telephone numbers.
- High volumes of short-duration, unanswered, or sequentially dialed calls.
- Traffic inconsistent with the stated residential or business use case.
- Repeated changes in caller ID, use of unrelated numbers, or calls presenting invalid numbering information.
- High complaint, blocking, labeling, or traceback activity associated with an account or campaign.
- Rapid customer growth or requested capacity without a credible operational explanation.
- Payment, identity, or location anomalies associated with high-volume calling.
- A customer's refusal or inability to provide call purpose, consent, number authorization, or end-user information.
- Repeated attempts to re-open service after suspension or to move traffic among related accounts.

10.4 Complaint Intake

CRC will accept complaints from customers, consumers, carriers, SkySwitch, the FCC, law enforcement, and the Industry Traceback Group. A complaint record should include the calling number, called number, date and time with time zone, call description, recording or voicemail if available, complainant contact information, account association, and actions taken.

10.5 Data Analytics Statement for RMD

Recommended filing language, subject to CRC verification: "CRC does not independently operate a proprietary robocall analytics platform. CRC reviews customer account information, call detail and traffic information available through its underlying provider SkySwitch, consumer and carrier complaints, traceback requests, and other operational information. CRC coordinates with SkySwitch for network-level analysis and mitigation when required."

11. Investigation and Risk Assessment Procedures

11.1 Intake and Triage

1. Create an incident record and preserve the initiating complaint, traceback, notice, or alert.
2. Determine whether immediate restriction is necessary to prevent ongoing harm or preserve CRC's ability to respond within a regulatory deadline.
3. Identify the CRC customer, account, telephone number, campaign, device, trunk, reseller, or upstream source associated with the traffic.
4. Request relevant CRC and SkySwitch records, including CDRs, routing information, signaling details, authentication data, and account changes.
5. Review onboarding records, intended use, payment history, prior complaints, prior tracebacks, and number authorization.
6. Contact the customer when appropriate and require a prompt, specific response supported by documents.
7. Assign a risk level and determine mitigation, monitoring, reporting, and retention actions.

11.2 Risk Levels

Level	Examples	Default response
Low	Isolated complaint; plausible lawful use; complete records; no pattern	Document, educate, monitor, close with rationale
Moderate	Multiple complaints; unexplained traffic change; incomplete customer response; questionable caller ID	Restrict capacity or numbers, enhanced monitoring, written remediation, management review
High	Traceback to customer; strong fraud indicators; invalid caller ID; repeated violations; non-cooperation	Immediate suspension or blocking, SkySwitch escalation, preserve records, evaluate termination
Critical	FCC/law-enforcement notice; continuing illegal traffic; imminent consumer harm; deliberate evasion	Immediate containment, executive escalation, response within required deadline, termination and reporting as appropriate

11.3 Decision Standard

CRC need not wait for a final governmental determination before protecting its services and downstream networks. CRC may act on credible evidence, contractual rights, risk to consumers, inability to verify a customer, or failure to cooperate. Decisions will be proportionate, documented, and reviewed by the Compliance Officer.

11.4 False Positives and Redress

Where a customer supplies credible evidence that traffic is lawful or incorrectly attributed, CRC will reassess restrictions and coordinate with SkySwitch where necessary. Restoration may be conditioned on corrected caller ID, reduced capacity, additional documentation, monitoring, or a written compliance plan.

12. Mitigation, Suspension, and Termination

12.1 Available Mitigation Measures

- Written warning, compliance education, or corrective-action plan.
- Requirement for additional identity, consent, caller ID, or campaign documentation.
- Removal or restriction of specific telephone numbers or caller ID presentation.
- Reduction of concurrent calls, rate limits, destination restrictions, or temporary provisioning freeze.
- Blocking or rejection of identified traffic in coordination with SkySwitch.
- Temporary account suspension pending investigation.
- Permanent termination and refusal of related or successor accounts.
- Notice to SkySwitch, affected carriers, the FCC, law enforcement, or the Industry Traceback Group when appropriate.

12.2 Customer Non-Cooperation

A customer that does not respond within the deadline set by CRC, provides materially false information, deletes requested records, or cannot identify the purpose and source of traffic may be suspended or terminated even if CRC has not independently proven every call was illegal.

12.3 Related Accounts

CRC may treat accounts as related based on common ownership, management, addresses, payment methods, domains, devices, traffic, telephone numbers, or other evidence. A violation by one account may justify review or restriction of related accounts to prevent evasion.

12.4 Post-Termination Controls

After termination for compliance reasons, CRC will preserve relevant records, prevent unauthorized reactivation, document associated identities and payment methods, and notify SkySwitch where necessary to prevent migration of the same traffic through another CRC account.

13. Traceback Response Program

13.1 Commitment

CRC commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the registered traceback consortium. CRC will treat a traceback request as a priority compliance matter and will coordinate immediately with SkySwitch when the requested routing or network information is not independently available to CRC.

13.2 Internal Service Levels

Elapsed time	Required internal action
As soon as received	Log request, preserve original message, alert Compliance Officer, identify deadline.
Target: within 4 business hours	Acknowledge request where appropriate; identify customer/account; send SkySwitch escalation if needed.
Before regulatory deadline	Provide complete routing/customer response or explain specifically what remains unavailable and actions taken to obtain it.
After response	Preserve records, evaluate customer risk, initiate mitigation if traffic originated from or was enabled by CRC customer.

13.3 Response Content

A complete response should identify whether CRC originated or received the call; the CRC customer or upstream provider; the next provider in the call path; relevant date, time, calling and called numbers; routing or trunk information reasonably available; actions taken; and the responsible compliance contact. CRC will not omit known information merely because SkySwitch also possesses it.

13.4 Coverage and Continuity

The Compliance Officer will maintain a backup contact and access method sufficient to receive and respond to requests during absences. CRC will not rely on an unmonitored personal inbox as its sole traceback mechanism. Contact changes will be reflected in the RMD within 10 business days where required.

13.5 Traceback Follow-Up

A traceback associated with a CRC customer triggers an investigation under Section 11. Repeated tracebacks, non-cooperation, or traffic inconsistent with the customer's approved use generally warrants high-risk treatment and immediate restrictions.

14. Regulatory Notices and Suspected Illegal Traffic

14.1 Notification Handling

A notice of suspected illegal traffic from the FCC, SkySwitch, a downstream provider, or the Industry Traceback Group will be escalated immediately to the Compliance Officer. CRC will identify the required response and mitigation deadlines, preserve evidence, and coordinate network-level action with SkySwitch.

14.2 Immediate Containment

Where a notice identifies continuing or likely illegal traffic, CRC may temporarily suspend the relevant account, trunk, campaign, or caller ID before completing the full investigation. CRC will prioritize effective mitigation over customer convenience when credible evidence indicates ongoing consumer harm or network risk.

14.3 Preventive Measures for New and Renewing Customers

When CRC receives evidence that its onboarding or renewal controls have been exploited, CRC will implement targeted corrective measures, which may include stronger identity verification, additional documentation for high-risk use cases, delayed activation, reduced initial capacity, enhanced number authorization, reseller restrictions, or executive approval.

14.4 Communications

Regulatory responses will be accurate, complete, timely, and approved by the Compliance Officer. CRC will not speculate, conceal known facts, or certify remediation that has not occurred. Counsel may be consulted when a notice creates enforcement, litigation, privacy, or contractual risk.

15. Record Retention, Confidentiality, and Evidence Preservation

15.1 Seven-Year Retention Standard

CRC will retain records supporting this Program for a minimum of seven (7) years from creation or closure of the relevant account or matter, whichever is later, unless a longer period is required by law, contract, litigation hold, regulatory request, or company policy.

15.2 Covered Records

- Customer applications, identity and business verification, intended-use descriptions, approvals, and risk assessments.
- Customer agreements, acceptable-use acknowledgments, amendments, renewals, and service-change records.
- Telephone-number assignments and authorization to use externally obtained caller ID numbers.
- Call detail records, traffic reports, signaling or authentication records available to CRC, and SkySwitch responses supporting investigations.
- Complaints, call examples, recordings or voicemails supplied by complainants, and customer support records.
- Traceback requests and responses, FCC or law-enforcement communications, and notices from carriers or SkySwitch.
- Investigation notes, evidence, risk decisions, mitigation actions, suspensions, terminations, and restoration approvals.
- RMD filings, updates, annual recertifications, supporting verification, and evidence of timely submission.
- Training records, annual reviews, audits, and prior versions of this Program.

15.3 Preservation Hold

Upon receipt of a traceback, subpoena, regulatory inquiry, suspected-illegal-traffic notice, threatened claim, or other material incident, CRC will suspend ordinary deletion of relevant records and issue an internal preservation instruction as appropriate.

15.4 Confidentiality and Access

Access to KYC, call, complaint, and investigation records will be limited to personnel with a business need. CRC will use reasonable safeguards for personal information, credentials, and security-sensitive technical data. Records disclosed in response to a lawful request will be limited to information reasonably responsive to that request.

16. Training, Testing, and Program Review

16.1 Training

Personnel involved in sales, onboarding, provisioning, billing, support, network operations, and management will receive training appropriate to their role. Training will address customer verification, risk indicators, prohibited uses, complaint logging, traceback escalation, preservation of evidence, and the authority to suspend service.

16.2 Annual Review

The Compliance Officer will review this Program at least annually and following any material regulatory, ownership, vendor, service, platform, or operational change. The review will determine whether stated controls are actually performed, whether records exist to demonstrate performance, and whether the RMD filing remains accurate.

16.3 Sample Testing

- Review a sample of residential and commercial onboarding files for required KYC elements.
- Review all reseller or unusually high-volume accounts.
- Test the traceback escalation process and 24-hour response capability.
- Confirm SkySwitch compliance and technical contacts and evidence of RMD review.
- Compare the signed RMP to the live RMD filing and CORES information.
- Review complaints, tracebacks, suspensions, and terminations for recurring control failures.
- Confirm retention and preservation procedures are operating as described.

16.4 Corrective Action

Identified deficiencies will be assigned an owner and due date. Material deficiencies affecting an RMD statement will be corrected operationally and in the RMD within the required period. The Compliance Officer will document closure and retain evidence of corrective action.

17. RMD Filing Administration

17.1 Filing Responsibility

The Compliance Officer is responsible for preparing, reviewing, submitting, and retaining CRC's RMD filing. Only an authorized user associated with CRC's business-type FRN may submit or modify the filing.

17.2 Current CRC Filing Profile

Field	Program information
Legal name	Colorado River Communications, Inc.
FRN	0027578970
OCN	None / Not Applicable
Provider type	Domestic voice service provider; non-facilities-based white-label reseller
Services	SIP Trunking and UCaaS
End users	Residential and commercial; approved reseller arrangements if applicable
Underlying provider	SkySwitch - exact legal entity to be verified
Compliance contact	Bryan Toy, Vice President, (928) 505-7301, bryan@crc-inc.net
Retention period	Seven years
STIR/SHAKEN	Full implementation stated by CRC, subject to Section 7 verification before certification

17.3 Update and Recertification Calendar

- Within 10 business days: update changed RMD information and changed CORES information where applicable.
- Annually on or before March 1: review, recertify, and resubmit the RMD filing.
- Immediately upon discovery: investigate and correct false, inaccurate, inconsistent, or deficient filing information.
- Before introducing a new upstream provider or materially changing authentication: evaluate RMD and Program updates.

17.4 Supporting File

CRC will retain a compliance file containing the filed RMP, submission confirmation, screenshots or exported filing information, supporting STIR/SHAKEN verification, SkySwitch due-diligence evidence, principal and affiliate information, prior enforcement disclosures if any, and documentation of annual review.

Appendix A - Customer Onboarding and KYC Checklist

Use the checklist appropriate to the account. Mark "N/A" only when the item is not reasonably applicable and explain material omissions.

Item	Residential	Commercial	Reseller / High Volume
Legal name / entity name	Required	Required	Required
Government ID or authorized representative ID	Required	Risk-based	Required
Physical and billing address	Required	Required	Required
Telephone and verified email	Required	Required	Required
Business registration / formation	N/A	Required	Required
Tax identifier	N/A	Risk-based	Required
Website / business domain	N/A	Risk-based	Required
Intended use and expected volume	Basic	Required	Detailed
Automated / prerecorded / dialer disclosure	N/A unless used	Required if applicable	Required
Caller ID ownership / authorization	Required	Required	Required
Payment consistency review	Required	Required	Required
RMD / FRN review	N/A	If provider/reseller	Required if applicable
Downstream KYC and nested-reseller controls	N/A	If reselling	Required
Compliance approval	Exceptions only	High-risk	Required

Reviewer notes: _____

Risk level: [ ] Low [ ] Moderate [ ] High [ ] Critical **Approved by:** _____ **Date:** _____

Appendix B - Investigation and Mitigation Worksheet

Incident number	
Date/time received	
Source of complaint/traceback/notice	
Regulatory response deadline	
Calling number(s)	
Called number(s)	
Call date/time/time zone	
CRC customer/account	
SkySwitch ticket/reference	
Customer approved use	
Traffic indicators	
Caller ID authorization reviewed	
Customer explanation and evidence	
Risk level	[ ] Low [ ] Moderate [ ] High [ ] Critical
Immediate containment	
Final decision	
Notifications made	
Records preserved through	

Appendix C - Traceback Response Worksheet

Internal target: begin investigation immediately; target initial action within four business hours; complete response within 24 hours under applicable FCC timing rules.

Requesting entity	
Traceback ID	
Received date/time/time zone	
24-hour deadline	
Request recipient / mailbox	
Calling number	
Called number	
Call date/time/time zone	
CRC role in call path	[ ] Originating [ ] Terminating [ ] Unknown / investigate
CRC customer identified	
Next upstream/downstream provider	
SkySwitch escalation date/time	
SkySwitch response	
Information supplied	
Mitigation initiated	
Response date/time	
Responder	
Follow-up investigation number	

Appendix D - Annual RMD and Program Review Checklist

- [ ] Legal name, FRN, business address, and CORES information are accurate.
- [ ] Principals, affiliates, subsidiaries, parent companies, and required enforcement disclosures are accurate.
- [ ] Provider role and service descriptions are accurate.
- [ ] SkySwitch contracting entity, contacts, RMD status, and responsibilities are current.
- [ ] STIR/SHAKEN status is supported by current technical and governance evidence.
- [ ] KYC procedures in the RMP match actual onboarding practice.
- [ ] Data analytics statement accurately identifies whether CRC relies on SkySwitch or another vendor.
- [ ] Traceback contact and backup contact are monitored and tested.
- [ ] Traceback responses during the review period met the 24-hour rule.
- [ ] Complaints, investigations, and mitigation actions were reviewed for trends.
- [ ] Customer agreements and acceptable-use provisions remain current.
- [ ] Seven-year retention and preservation processes were tested.
- [ ] RMD filing was updated for all changes within 10 business days.
- [ ] Annual recertification is submitted on or before March 1.
- [ ] This Program and revision history are updated and approved.

Review completed by: _____ **Date:** _____
Corrective actions: _____
_____

Appendix E - Regulatory Reference Matrix for CRC Review

This matrix identifies the principal authorities used to structure this Program. CRC should verify current text and effective dates before filing or signing.

Authority	Program topic
47 CFR Section 64.6300	Definitions, including voice service provider and intermediate provider.
47 CFR Section 64.6301	Voice service provider STIR/SHAKEN implementation obligations, including third-party technological arrangements.
47 CFR Section 64.6305	Robocall mitigation program, RMD certification, plan content, updates, call acceptance restrictions, and annual recertification.
47 CFR Section 64.1200(n)(1)	Full response to traceback requests within 24 hours.
47 CFR Section 64.1200(n)(2)-(4)	Response to suspected illegal traffic, mitigation, and obligations to prevent new and renewing customers from originating illegal calls.
47 CFR Section 64.1200(n)(4)	Know-your-customer and due diligence obligations for originating providers.
47 CFR Section 1.80	Forfeiture framework, including RMD false/inaccurate information and failure to update.
47 CFR Section 1.8002(b)(2)	CORES information update obligation.
FCC DA 26-72 (Jan. 22, 2026)	RMD effective-date notice and Frequently Asked Questions for filers, including resellers, third-party authentication, analytics, KYC, 10-business-day updates, and annual March 1 recertification.
FCC DA 26-174 (Feb. 20, 2026)	Enforcement advisory confirming reseller/MVNO filing, mitigation, KYC, and traceback obligations.
FCC DA 23-965 (Oct. 16, 2023)	Enforcement action emphasizing that mitigation plans must identify specific reasonable steps.
FCC 23-37 (May 19, 2023)	Seventh Call Blocking Order adopting the 24-hour traceback response requirement for all voice service providers.

Appendix F - Revision History

Version	Effective date	Description	Approved by
1.0	August 1, 2026	Initial adoption of comprehensive Robocall Mitigation Program for CRC's SkySwitch white-label SIP Trunking and UCaaS services.	Bryan Toy

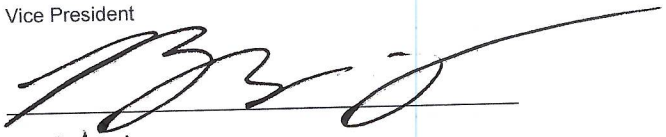
18. Authorized Representative Certification and Signature

I, the undersigned authorized representative of Colorado River Communications, Inc., certify that I have reviewed this Robocall Mitigation Program and the Pre-Signature Verification Checklist. To the best of my knowledge, information, and belief, this Program accurately describes the specific reasonable steps CRC has implemented or formally adopted to avoid originating illegal robocall traffic, to know its customers and upstream provider, to cooperate with traceback requests, and to comply with applicable FCC Robocall Mitigation Database requirements.

I further certify that CRC will maintain this Program, provide resources reasonably necessary to implement it, investigate suspected illegal traffic, coordinate with SkySwitch where network-level action is required, update its RMD filing within applicable deadlines, and revise this Program when operational or regulatory changes make an existing statement inaccurate.

SIGNATURE CONDITION

The authorized representative should not sign this certification until each item in the Pre-Signature Verification Checklist has been completed or resolved, particularly the STIR/SHAKEN third-party authentication verification in Section 7.

Authorized Representative	Bryan Toy
Title	Vice President
Signature	
Date	8/1/2026

Compliance contact: Bryan Toy, Vice President | (928) 505-7301 | bryan@crc-inc.net
Company: Colorado River Communications, Inc. | **FRN:** 0027578970 | **OCN:** Not Applicable

End of document.