

RMD Plan, KYC Onboarding and Traceback Rules

A practical operating standard for lawful U.S. voice traffic, customer due diligence, robocall mitigation, and rapid traceback cooperation.

US DIRECT TELECOM LLC

Wholesale and retail telecommunications operations

Registered address	8735 DUNWOODY PLACE, STE 400, ATLANTA, GA 30350
County	Fulton County
Telephone	877-264-1364
Legal email	legal@usdirecttele.us
Website	Not provided
Chief Executive Officer	Sanum Asnee
CEO email	Sanum@usdirecttele.us
Formation state	Not provided
Formation date	Not provided
State entity ID	Not provided
EIN	414305783

Purpose of this manual

This manual establishes minimum controls for onboarding customers, accepting and monitoring voice traffic, maintaining the company's Robocall Mitigation Database posture, and responding to traceback requests. It is designed for use by executive management, legal/compliance, billing, NOC, sales, and vendor-management personnel.

Document owner: Chief Executive Officer, Sanum Asnee

Review cycle: At least annually and whenever a material regulatory, network, or business-model change occurs

Classification: Internal operational policy; share externally only with executive approval

00

Document control and use

This policy is intended to be adopted as an operational control document and adapted to the company's actual network architecture, service contracts, and regulatory profile.

Policy title	RMD Plan, KYC Onboarding and Traceback Rules
Legal entity	US Direct Telecom LLC
Version	1.0
Effective date	September 19, 2026
Policy owner	CEO / Legal and Compliance function
Primary contact	legal@usdirecttele.us 877-264-1364
Supersedes	New policy

Contents

- 01 Policy principles and accountability
- 02 Robocall Mitigation Database (RMD) plan
- 03 Customer KYC onboarding rules
- 04 Traceback response rules
- 05 Monitoring, records, training and enforcement
- Appendix A Operational checklists and templates
- Appendix B Regulatory reference list

Important limitation

This is an internal compliance and operations template, not a legal opinion. The company should have U.S. telecom counsel review the policy against its actual role in each call path - originating provider, gateway provider, intermediate provider, reseller, or other role - and against state-specific telemarketing rules.

01

Policy principles and accountability

US Direct Telecom LLC will accept and carry voice traffic only when the company can identify the customer, understand the campaign, verify the authority to use the caller ID resources, and respond to a lawful investigation or traceback.

1.1 Core principles

- Know the customer and the traffic. No production access is granted until required KYC, ownership, use-case, and routing information is reviewed and approved.
- Use authorized identity. Customers may use only telephone numbers, caller IDs, DIDs, and calling name data that they own, lease, or are expressly authorized to use.
- Prevent illegal traffic. The company will use reasonable technical and operational measures to avoid originating, carrying, or processing illegal robocall traffic, consistent with its role in the call path.
- Cooperate quickly. Traceback requests from the FCC, law enforcement, or the industry traceback consortium receive priority handling and are not delayed for commercial reasons.
- Document decisions. KYC approvals, exceptions, traffic alerts, complaints, blocks, suspensions, traceback responses, and corrective actions must be recorded in a retrievable case log.
- Escalate uncertainty. If a team member cannot determine whether traffic is lawful, the traffic is paused or restricted while Legal/Compliance reviews it.

1.2 Accountability matrix

Role	Minimum responsibility	Backup / escalation
CEO / executive owner	Approves this policy, high-risk customers, material exceptions, and termination decisions.	Legal/compliance lead
Legal / compliance	Interprets requirements, approves KYC exceptions, manages traceback responses, and maintains regulatory records.	CEO
NOC / network operations	Implements blocks, rate limits, CLI restrictions, monitoring, evidence preservation, and emergency suspension.	Engineering lead
Sales / onboarding	Collects complete KYC, describes prohibited uses, obtains signed certifications, and does not promise activation before approval.	Legal/compliance
Billing / finance	Verifies payer identity, payment source, account ownership, and suspicious payment changes.	CEO / compliance

No self-approval rule

The person who sells or provisions an account may not be the sole approver for a high-risk customer, a material KYC exception, or a traceback-related suspension.

02

Robocall Mitigation Database (RMD) plan

The RMD plan is organized around the FCC requirement that a voice service provider maintain an appropriate robocall mitigation program, take reasonable steps to avoid illegal robocall traffic, and commit to responding to qualifying traceback requests within 24 hours. The exact obligations depend on the company's regulatory role and applicable exceptions.

2.1 RMD governance and filing maintenance

- Maintain a single controlled copy of the company's RMD filing, supporting certifications, contact details, and filing history.
- Assign legal@usdirecttele.us and at least one monitored operational contact for regulatory and traceback communications. Monitor the mailbox continuously during business operations and establish an after-hours escalation method.
- Review the RMD filing at least quarterly and after any material change to legal name, address, ownership, responsible personnel, telephone number, email, website, filing certifications, STIR/SHAKEN status, or mitigation program.
- Update the RMD filing within 10 business days after a change to information required in the filing, using the FCC process applicable at the time of the change.
- Retain the filing confirmation, the submitted answers, supporting evidence, and a dated internal review note. Do not represent that a certification is current unless the filing has been checked.

2.2 Minimum mitigation controls

Control domain	US Direct Telecom LLC minimum standard	Evidence to retain
Customer admission	No customer receives production voice access without approved KYC, signed acceptable-use terms, an identified responsible party, and a defined use case.	KYC packet, approval record, contract, customer risk rating
Traffic purpose	Record campaign type, expected call direction, calling countries, target geography, average duration, CPS/channels, caller IDs, DIDs, and whether automation or prerecorded content is used.	Traffic profile, campaign declaration, sample script if applicable
Caller ID and DIDs	Reject unauthorized, invalid, unassigned, or misleading caller ID. Require proof of control or authority for customer-provided numbers and promptly block disputed or abusive numbers.	DID inventory, authorization evidence, block history
STIR/SHAKEN	Authenticate calls where required and technically applicable; preserve attestation and verification data; do not knowingly pass altered or misleading identity information.	SIP identity headers, signing/verification logs, carrier records
Analytics and alerts	Monitor complaint signals, answer-seizure changes, short-duration patterns, burst activity, failed-call ratios, unusual destination patterns, and number rotation.	Daily/weekly dashboards, alert tickets, investigation notes
DNC and consent	Require customers to maintain applicable federal, state, internal, and campaign-specific do-not-call controls and lawful consent records for the call type.	Customer certification, suppression-list controls, consent evidence
Downstream controls	Require resellers and downstream users to identify the end user, flow compliance obligations down, and cooperate with investigations. Unknown or concealed end users are not approved.	Downstream schedule, end-user declaration, contract flow-down

2.3 Traffic acceptance and risk triggers

- Place new or materially changed traffic into a monitored test or probation state before unrestricted production routing.
- Require pre-approval for high-volume campaigns, rapid number rotation, government or financial-institution branding, lead-generation campaigns, political activity, debt collection, healthcare, emergency-service references, or any campaign using prerecorded or artificial voice.
- Immediately investigate complaints alleging impersonation, fraud, threats, extortion, account takeover, Social Security or tax authority impersonation, bank or insurance impersonation, or deceptive caller ID.
- Use graduated controls: warning and remediation, rate limit, number block, campaign pause, customer suspension, and termination. The severity and urgency of the facts determine the control; commercial value does not override safety.

02A

RMD incident and change-management workflow

The following workflow is the internal operating sequence for a material change, suspected illegal robocall, or RMD-related compliance issue.

Stage	Required action	Owner / target
1. Detect	Record the alert, complaint, traceback, carrier notice, government notice, abnormal traffic signal, or customer disclosure.	Any employee; immediately
2. Triage	Assign a case ID, identify affected customers/numbers/routes, preserve current logs, and determine whether emergency blocking is warranted.	NOC + compliance; within 1 hour
3. Contain	Pause, rate-limit, block, or isolate the suspected source. Preserve unaffected customer service where technically safe.	NOC; immediately for high severity
4. Investigate	Map customer, reseller, end user, CLI/DID, SIP source, campaign, invoices, and route history. Contact the responsible customer through verified channels.	Compliance + NOC; same business day
5. Correct	Require documented remediation, new consent or campaign proof, password/IP changes, number replacement, or termination as appropriate.	Compliance + account owner
6. Report / update	Respond to the requesting party, update the RMD filing if required, and record the final disposition and date.	Legal/compliance; statutory deadline applies
7. Review	Conduct root-cause review and update controls, training, customer terms, or vendor selection if a control failed.	CEO + compliance; within 10 business days

Material change rule

If a change affects the accuracy of the RMD filing or the company's stated mitigation program, compliance must open a change ticket before the change is treated as complete. The ticket must identify what changed, why it changed, who approved it, and whether an RMD update is required.

2.4 Management reporting

- Monthly: active customers, new approvals, suspensions, terminations, complaints, blocked numbers, significant alerts, traceback cases, and open remediation items.
- Quarterly: RMD filing review, contact test, access-control review, sample KYC audit, customer risk re-rating, and vendor/upstream review.
- Annually: CEO sign-off on this plan, staff training completion, a tabletop traceback exercise, and legal review of the company's role and obligations.

03

Customer KYC onboarding rules

KYC is a risk-control gate, not a sales formality. The goal is to identify the legal entity, the individuals who control it, the intended use of the service, the source of traffic, and the party responsible if the traffic is challenged.

3.1 Required onboarding file

Category	Required information or document	Decision rule
Legal identity	Certificate of formation or state record; legal name; state/entity number; formation date; EIN or tax status as applicable; principal and mailing address; registered agent.	Must be consistent across documents or explained in writing.
Management and ownership	CEO or authorized officer; controlling person; owners or members as applicable; government ID for authorized signatory; beneficial ownership information requested by policy or partner.	Unexplained ownership or signatory mismatch = pending review.
Contact verification	Business domain email, legal contact, billing contact, NOC/technical contact, phone number, website, and an alternate escalation contact.	Free-mail-only or unverifiable contact requires executive review.
Telecom profile	FCC/FRN/RMD/499A/OCN details if applicable; carrier relationships; network role; DIDs and caller ID resources; STIR/SHAKEN posture; upstream and downstream relationships.	Missing data may be acceptable only when not applicable and documented.
Traffic profile	Call purpose, campaign description, target market, origination countries, destinations, expected minutes, CPS/channels, ACD/ASR expectations, automation/prerecorded/artificial voice, scripts, and sample caller IDs.	No vague or contradictory descriptions.
Compliance controls	DNC process; consent or lawful-basis process; complaint handling; end-user verification; recording/retention practice; traceback contact; abuse-response commitment.	Must identify an accountable person and operating process.
Commercial and security	Payment source, billing contact, credit terms, IP addresses, SIP credentials, password controls, access list, and any reseller/end-user schedule.	No shared credentials; no anonymous payment or access.

3.2 Risk-rating guide

Rating	Typical facts	Required approval
Low	Known business, clear use case, verified ownership, stable traffic, clear caller-ID authority, complete documentation.	Onboarding + compliance
Medium	New entity, reseller structure, higher volume, multiple downstream users, incomplete history, unusual campaign, or material traffic variance.	Compliance + NOC; enhanced monitoring
High	Impersonation allegation, unexplained caller ID, refusal to name end user, prior traceback, suspicious payment/access pattern, misleading marketing, or repeated policy breach.	CEO/compliance; written conditions or decline

3.3 Approval states

1. Pending. Documents or answers are incomplete; no production voice traffic.
2. Conditional approval. Limited test access is allowed under written limits, monitoring, and an expiration date.
3. Approved. KYC is complete, terms are signed, the traffic profile is accepted, and technical controls are active.
4. Suspended. Pause traffic or account access pending investigation, remediation, or a third-party response.
5. Terminated. Close service for material breach, illegal traffic, fraud, non-cooperation, or unacceptable risk.

03A

KYC approval, contracting and ongoing review

Every approved customer must understand that access is conditional on continuing compliance. The customer agreement should be consistent with these rules and should require the customer to flow equivalent obligations to any downstream user.

3.4 Minimum customer representations

- The customer is accurately identified, has authority to enter the agreement, and will promptly report material changes in ownership, address, contacts, business model, or traffic source.
- The customer will not use the service for fraud, impersonation, threats, extortion, unlawful telemarketing, illegal robocalls, caller-ID spoofing, traffic pumping, artificial traffic, or any prohibited activity.
- The customer will use only numbers and caller ID resources it owns, leases, or is authorized to use and will provide proof when requested.
- The customer will maintain applicable consent, DNC, campaign, script, recording, and complaint records and will produce them promptly for investigation.
- The customer will identify each downstream end user and will impose written flow-down obligations on resellers, agents, call centers, and other downstream participants.
- The customer will respond to a compliance or traceback request through the verified contact channel and will not delete, alter, or conceal relevant records.

3.5 Technical activation controls

- Create a unique customer account and unique credential set; do not reuse passwords or shared logins.
- Restrict SIP access to approved source IPs, certificates, trunks, or other authenticated methods when technically available.
- Record the approved caller-ID ranges, DIDs, rate limits, CPS, channel limits, destination scope, and any campaign restrictions.
- Enable monitoring before production activation and verify that blocking, rate limiting, logging, and alerting operate as intended.
- Do not activate a new route or customer solely on the basis of a payment, a referral, or a verbal promise of compliance.

3.6 Ongoing review triggers

- Annual KYC refresh for every active customer, or more frequently for medium- and high-risk accounts.
- Immediate refresh after a traceback, material complaint, change in ownership, new end user, new campaign, new country of origination, new caller-ID range, or significant traffic increase.
- Reconcile billing identity, technical identity, contract identity, and RMD/telecom identity. Escalate mismatches instead of silently updating one record.
- If the customer misses a compliance deadline, restrict traffic until the required information is received and approved.

KYC stop condition

Do not onboard or reactivate an account when the company cannot identify the legal customer, the person responsible for the traffic, the source of the caller ID, or the downstream end user where the business model involves reselling or downstream origination.

04

Traceback response rules

A traceback is a priority compliance event. The objective is to identify the originating customer and end user, preserve evidence, stop harmful traffic when warranted, and provide a complete, accurate, and timely response to the requesting authority or consortium.

4.1 Response standard

Clock	US Direct Telecom LLC internal target	Required action
0-1 hour	Immediate	Acknowledge internally, assign a case ID, identify the request source and deadline, preserve logs, and alert compliance/NOC.
1-4 hours	Initial response target	Confirm receipt to the requesting party when appropriate; identify the customer, route, CLI/DID, and time window; begin containment if risk is active.
4-12 hours	Investigation target	Map the call path using available records; contact the customer; obtain campaign and end-user details; document contradictions and missing data.
By 24 hours	Regulatory baseline	Provide a full and accurate response to qualifying requests from the FCC, law enforcement, or the industry traceback consortium, or explain specifically what is still pending and when it will be delivered.
After response	Closure target	Complete remediation, customer disposition, root-cause review, and evidence retention. Update the requester if material facts change.

4.2 Required traceback intake fields

- Requesting organization, authorized contact, email domain, telephone number, request timestamp, stated deadline, and any ticket or reference number.
- Called number, calling number, date/time with time zone, call direction, destination, carrier or route information, and any SIP/Call-ID or trace identifier supplied.
- Customer account, trunk, source IP, DID/CLI owner, reseller or downstream end user, and the responsible account manager.
- Evidence preserved, systems queried, search window, investigator, findings, customer response, blocks or suspension applied, and final disposition.

4.3 Response workflow

1. Validate and log. Confirm the request is from a recognized traceback, government, law-enforcement, carrier, or other authorized channel. If authenticity is uncertain, contact the organization through a trusted published channel while preserving the deadline.
2. Preserve. Put a legal/compliance hold on relevant CDRs, SIP logs, authentication data, account changes, tickets, emails, billing records, KYC files, and routing records.
3. Trace. Correlate the called number, calling number, timestamp, route, source IP, account, and downstream customer. Use UTC and the original time zone in the case notes.
4. Contain. Block the abusive number, suspend the source, rate-limit the route, or isolate the campaign when the facts indicate ongoing harm or high risk. Record who approved the action and when.
5. Contact and require answers. Ask the customer for the end user, campaign, authorization for the CLI, consent/DNC evidence, and corrective action. Set a short written deadline; non-response is an escalation factor.
6. Respond accurately. Provide facts, not speculation. Distinguish confirmed facts, customer statements, technical findings, and open questions. Never alter records to fit a requested narrative.
7. Close and learn. Record the outcome, customer status, blocks, refunds or credits if applicable, root cause, control failure, and prevention steps.

04A

Traceback severity, evidence and closure

The response level should match the risk. When in doubt, use the higher severity until the investigation lowers the risk with reliable evidence.

4.4 Severity matrix

Severity	Examples	Immediate response
Critical	Government impersonation, financial theft, emergency-service abuse, active high-volume fraud, threats, or clear caller-ID deception.	Immediate block/suspension; executive and legal escalation; preserve evidence; respond on an accelerated basis.
High	Credible complaint, repeated policy breach, unexplained high-volume traffic, unknown end user, or customer refusal to cooperate.	Pause or rate-limit source; enhanced KYC; compliance approval required for reactivation.
Moderate	First-time anomaly, incomplete records, unusual campaign behavior, or disputed number authority without active harm evidence.	Investigate promptly; monitor and impose corrective deadline.
Low	Administrative mismatch or informational request with no current abuse signal.	Correct records and document the decision; continue monitoring.

4.5 Minimum evidence package

- Original traceback request and all correspondence, including attachments and timestamps.
- Customer KYC and contract record, authorized contacts, downstream schedule, and risk rating.
- CDRs, SIP signaling, Call-ID, source IP, authentication/verification information, routing records, and relevant billing data.
- Caller-ID/DID authorization evidence and number inventory history.
- Traffic graphs or alerts, complaint details, test-call notes, blocking/suspension records, and customer explanation.
- Final response, remediation evidence, reactivation approval or termination decision, and root-cause report.

4.6 Closure rules

- A traceback is not closed merely because a response email was sent. Closure requires a documented disposition and evidence of containment or remediation.
- If the customer is suspended, keep the account restricted until compliance approves reactivation in writing. A password change alone is not sufficient when the source, campaign, or end user remains unexplained.
- If the customer is terminated, block associated accounts, credentials, IPs, DIDs, and known aliases as appropriate; flag re-onboarding attempts for executive review.
- If the trace cannot be completed, document the exact limitation, systems queried, time window, missing data, and the next action. Do not claim completion when the evidence is incomplete.

No obstruction rule

Employees and customers must not delete, alter, conceal, fabricate, or delay records relevant to a traceback or lawful investigation. Suspected obstruction is a critical escalation and may result in immediate suspension or termination.

05

Monitoring, records, training and enforcement

The controls in this manual are effective only when they are tested, documented, and enforced consistently.

5.1 Recordkeeping standard

- Keep KYC files, contracts, traffic declarations, RMD evidence, customer approvals, alerts, complaint records, traceback files, and termination records in access-controlled storage.
- Use a case ID and consistent timestamps. Retain original files and preserve the chain of custody for exported logs or screenshots.
- US Direct Telecom LLC internal standard: retain compliance and traceback records for at least five years unless a longer period is required by contract, law, litigation hold, regulator request, or company policy.
- Restrict access to people with a business need. Record who exports, edits, approves, or deletes a compliance record. Do not store unnecessary sensitive identity information in unsecured chat or email.

5.2 Training

- New staff training before access to sales, provisioning, NOC, billing, or compliance systems.
- Annual refresher covering KYC red flags, caller-ID authority, DNC/consent basics, RMD updates, evidence preservation, and traceback response.
- Targeted training after a material incident or control failure, with attendance and completion recorded.

5.3 Enforcement ladder

Action	When used	Approval / record
Education / warning	Minor or first-time issue with no active harm and credible remediation.	Account owner + compliance note
Restriction	Traffic exceeds approved profile, records are incomplete, or risk increases.	NOC applies limit; compliance ticket
Pause / suspension	Credible abuse, non-cooperation, unknown end user, or serious KYC inconsistency.	Compliance + NOC; executive notice
Termination	Illegal traffic, fraud, impersonation, repeated breach, obstruction, or unacceptable residual risk.	CEO or delegated executive; termination record

5.4 Approval record

Approved by	Sanum Asnee, Chief Executive Officer
Signature	_____
Date approved	_____
Next scheduled review	_____
Legal review notes	_____

A

Operational checklists and templates

These compact checklists may be copied into the company ticketing, CRM, or compliance system.

A.1 KYC approval checklist

☐	Legal entity and state record verified
☐	EIN or tax status documented where applicable
☐	CEO/authorized signer and controlling person verified
☐	Owners/members and beneficial ownership information reviewed as applicable
☐	Business address, website, domain email, phone, and contacts verified
☐	RMD/FRN/499A/OCN/STIR-SHAKEN information reviewed where applicable
☐	Traffic purpose, countries, campaign, CPS/channels, and caller IDs documented
☐	DNC/consent/complaint process described and accepted
☐	Downstream end user/reseller structure identified
☐	Contract and acceptable-use terms signed
☐	Risk rating assigned and approval authority recorded
☐	Technical limits, IPs, credentials, and monitoring enabled

A.2 Traceback case template

Case ID	_____
Requesting party / ticket	_____
Received date/time and time zone	_____
Called number / calling number	_____
Call date/time and time zone	_____
Customer / account / route	_____
Downstream end user	_____
Evidence preserved	_____
Containment action and time	_____
Response sent and time	_____
Final disposition	_____
Approver / closure date	_____

B

Regulatory reference list

The following official sources were reviewed when preparing this policy. Verify the current text before relying on any rule, deadline, exemption, or filing instruction.

FCC RMD FAQ for Filers

Official FCC FAQ describing who must file and the requirement to update information that changes within 10 business days.

<https://www.fcc.gov/sites/default/files/rmd-faq.pdf>

47 CFR Part 64, Subpart HH - Caller ID Authentication

Current eCFR subpart containing the caller ID authentication and robocall mitigation provisions.

<https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-HH>

47 CFR 64.6305 - Robocall mitigation and certification

Includes the reasonable-steps mitigation requirement and the 24-hour traceback response commitment.

<https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/section-64.6305>

47 CFR 64.6301 - Caller ID authentication

Caller ID authentication requirements, subject to the rule's applicable exceptions and provider role.

<https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/section-64.6301>

FTC Telemarketing Sales Rule

Official FTC overview of 16 CFR Part 310, including disclosures, misrepresentations, calling times, do-not-call requests, and payment restrictions.

<https://www.ftc.gov/legal-library/browse/rules/telemarketing-sales-rule>

FCC Consumer Guide - Stop Unwanted Robocalls and Texts

FCC consumer and provider reference for unwanted calls, spoofing, and complaint-related controls.

<https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>

Implementation note

This manual should be paired with: (1) an executed customer master service agreement and acceptable-use policy, (2) a KYC intake form, (3) a traceback ticket template, (4) a number and caller-ID authorization process, and (5) a technical monitoring and blocklist procedure.

Prepared for US Direct Telecom LLC

8735 DUNWOODY PLACE, STE 400, ATLANTA, GA 30350

legal@usdirecttele.us | 877-264-1364 | Website not provided