Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in the United States

COUNTRY United States

INDUSTRY Telecom & Mobile Services

LAST UPDATED 16 October 2026

KEY REGULATORS Federal Communications Commission · Universal Service Administrative Company

Key takeaways

- Telecom providers in the United States are not covered by federal anti-money-laundering rules. Identity duties come from Federal Communications Commission (FCC) rules on account security, robocall prevention and the Lifeline subsidy.
- Today, carriers must verify a customer before releasing call records or account data. They may not use easily found facts such as Social Security number (SSN) digits, date of birth or home address as proof of identity, and in a store they must check a valid photo ID.
- The FCC adopted rules in 2023 requiring secure authentication, alerts and free account locks before a SIM change or number transfer. As of October 2026 none of these rules is yet required, and the FCC has not set a compliance date.
- Online and in-store channels differ mainly in how identity is checked before account data is released: a password and non-biographical authentication online, photo ID at the counter. The SIM-swap rules, once in force, will apply the same standard to every channel.
- Voice providers must already "know their customers" before letting them make calls. An FCC proposal from May 2026 would require name, address, a government ID number and document checks for new and renewing customers. It is proposed, not yet law.

The US market is open: mobile carriers, mobile virtual network operators (MVNOs), eSIM providers and cloud voice companies can onboard customers fully online, and no federal rule requires a customer to appear in person. Identity obligations are narrower than in finance but are concentrated on the moments fraudsters target: account access, SIM changes, number transfers and access to the voice network.

The FCC is the principal regulator, with the Universal Service Administrative Company (USAC) running Lifeline eligibility and identity checks. State consumer protection and privacy laws sit on top of the federal rules.

The biggest obstacle for a new entrant is uncertainty: the SIM-swap rules and the proposed customer identification rules for voice providers could take effect with a single Federal Register notice, so onboarding and account-change flows should be built to meet them now.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 Identity framework (AML rules do not apply)
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
- Sources

1 Who regulates this sector

Body	Remit	Level	Official site
Federal Communications Commission (FCC)	Customer data and account security rules, number portability, robocall and caller ID rules, Lifeline, enforcement and forfeitures	Federal	fcc.gov
Universal Service Administrative Company (USAC)	Administers Lifeline, the National Verifier and the National Lifeline Accountability Database under FCC rules	Federal (FCC-designated administrator)	usac.org
Cybersecurity and Infrastructure Security Agency (CISA)	Security guidance for communications, including SIM-swap risks; not a licensing or enforcement body for carriers	Federal	cisa.gov
Department of Justice	Collects unpaid FCC forfeitures through civil suits	Federal	justice.gov
State public utility commissions and attorneys general	State licensing, consumer protection and privacy enforcement	State	Varies by state

2 Licensing and authorisation

Authorisation depends on the service rather than the channel. Wireless carriers hold FCC spectrum licences. MVNOs and resellers resell capacity from those carriers; they are not exempt from customer data rules. The SIM-swap and port-out rules expressly cover "resellers of wireless service" (47 CFR 64.2010(h)). Interconnected Voice over Internet Protocol (VoIP) providers fall within the customer data rules by definition (47 CFR 64.2003(o)).

Any voice service provider must file a robocall mitigation plan in the FCC's Robocall Mitigation Database. The filing must describe how the provider meets its obligation to know its customers (47 CFR 64.6305). Other carriers may accept traffic directly from a domestic voice provider only if its filing appears in the database and has not been removed, so an unlisted provider is effectively cut off from the network. Annual recertification of database filings has applied since 1 March 2026 (91 FR 5242).

Carriers that want to offer Lifeline must be designated as eligible telecommunications carriers (ETCs) and follow the program's enrolment and identity rules. State certificates and registrations apply in addition to federal authorisation and differ from state to state.

3 Identity framework (AML rules do not apply)

Telecom providers are not financial institutions under the Bank Secrecy Act. They have no customer identification programme, suspicious activity reporting or cash reporting duties for their telecom services. Identity obligations come instead from four FCC rule sets.

Customer proprietary network information (CPNI)

Section 222 of the Communications Act and 47 CFR Part 64, Subpart U (64.2001 to 64.2011) protect call records, location and service data, and require authentication before disclosure. `In force`

SIM change and port-out protection

47 CFR 64.2010(h) and 52.37 govern how wireless providers verify customers before moving a number.

`Adopted, compliance not yet required`

Voice provider know-your-customer

47 CFR 64.1200(n)(4) requires affirmative, effective measures to stop new and renewing customers from originating illegal calls. `In force`

Lifeline

47 CFR 54.404 and 54.410 set identity, eligibility and duplicate checks for subsidised service. `In force`

The voice know-your-customer duty is outcome-based: the rule does not list data elements, documents or verification methods. The FCC's May 2026 proposal describes this as a gap between the current requirement and the rigorous steps needed to protect consumers (91 FR 30596).

4 Identity verification and onboarding

Account access and changes

Carriers must take reasonable measures to discover and protect against attempts to gain unauthorised access to CPNI. They must authenticate a customer before disclosing CPNI, whether the contact comes by phone, online or in a store (47 CFR 64.2010(a)). Authentication may not rely on "readily available biographical information", defined to include the SSN or its last four digits, mother's maiden name, home address and date of birth, or on account information (64.2003). Passwords must be set up without such prompts, and back-up methods for forgotten passwords are subject to the same limit (64.2010(e)). Carriers must notify customers immediately when a password, back-up answer, online account or address of record is created or changed. The notice goes to the existing contact details and must not reveal the new information (64.2010(f)).

Business customers with a dedicated account representative and a contract that addresses CPNI protection may agree a different authentication regime (64.2010(g)).

SIM changes and port-outs

The 2023 rules require wireless providers to use secure methods "reasonably designed to confirm the customer's identity" before executing a SIM change or a port-out. Those methods may not rely on biographical information, account information, recent payment information or call detail information. Providers must review their methods at least annually, and staff handling inbound contacts must not see CPNI until the customer is authenticated (88 FR 85794). The definition of SIM covers both physical and virtual cards, so eSIM transfers are in scope.

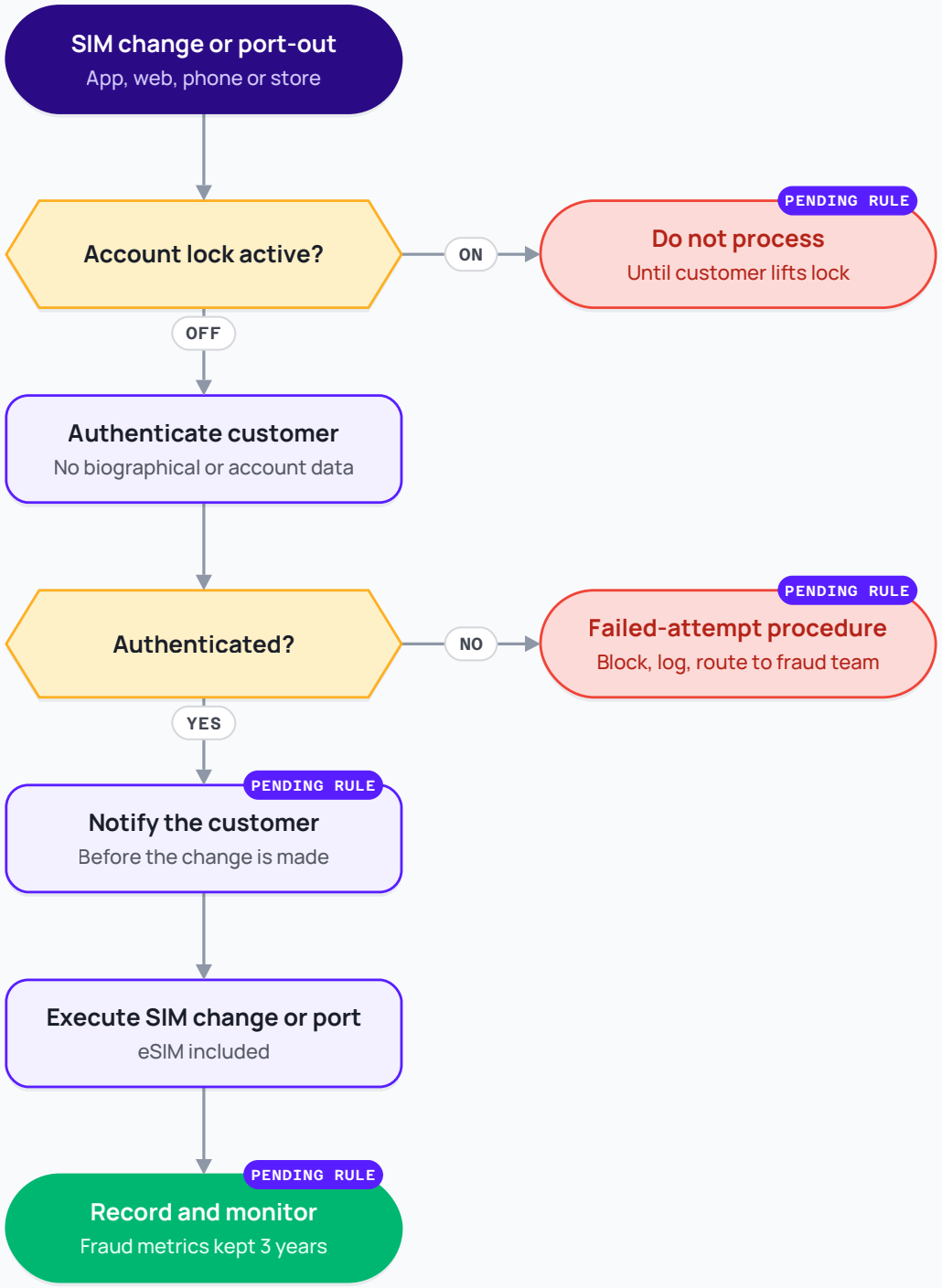

Figure 1. SIM change and port-out handling under the FCC's 2023 rules (adopted; compliance not yet required as of October 2026).

Activating a line

No federal rule lists the identity data a mobile carrier must collect before activating a SIM or eSIM, and there is no national subscriber registration requirement. For voice service, the general know-your-customer duty applies to new and renewing customers. In its Telnyx

enforcement action, the FCC said this duty does not allow providers to accept customer information at face value (FCC 25-10).

Lifeline enrolment

Applicants give their full name, residential address, date of birth and the last four digits of their SSN (or a Tribal identification number) and certify eligibility under penalty of perjury (54.410(d)). If the database or the National Verifier fails to confirm the applicant's identity or that they are alive, the carrier may not enrol them or claim support unless the applicant produces documents (54.404(b)(12)). USAC runs a third-party identity verification check. When it fails, applicants upload copies of unexpired documents such as a driver's licence, passport, permanent resident card or W-2 (USAC, Resolve Application Errors).

5 Digital channels: what's different

> **Bottom line:** the rules are largely channel-neutral, but the CPNI rules prescribe different identity checks for phone, online and in-store access, and Lifeline enrolment runs through different controls online and through field representatives.

Requirement	In person / in store	Online / remote	Difference
Identity check before releasing CPNI	Valid photo ID matching the account	Non-biographical authentication, then a password	`Differs`
Call details over the phone	Not applicable	Password, or send to address or number of record	`Differs`
Account change alerts	Immediate notice to existing contact	Immediate notice to existing contact	`Same`
SIM change and port-out authentication (once required)	Secure method, no biographical data	Secure method, no biographical data	`Same`
Voice know-your-customer	Affirmative, effective measures	Affirmative, effective measures	`Same`

Lifeline enrolment	Registered enrolment representative with a unique ID	National Verifier portal or API with automated identity check	`Differs`
CPNI breach notification	Law enforcement first, then customers	Law enforcement first, then customers	`Same`

Online account access

Before allowing online access to CPNI, a carrier must authenticate the customer without biographical or account information. After that, access is by a password that was itself set up without such prompts (64.2010©). In a store, presenting a valid photo ID that matches the account information is sufficient (64.2010(d)). For a digital-only carrier, the practical consequence is that a one-time code sent to the phone number of record, a document and selfie check, or a similar non-biographical method has to stand in for the counter ID check.

Remote SIM and eSIM changes

The 2023 rules treat every channel alike: the same authentication standard applies whether the request arrives through an app, a call centre or a store. Once in force, providers must also publish their account protection measures on their website and in their app (88 FR 85794). `Adopted, compliance not yet required`

Lifeline in the field and online

Enrolment representatives must register with USAC, giving identifying information such as name, date of birth and the last four SSN digits. They must use their own unique identifier for every database access and enrolment, and carriers may not pay them commission based on enrolments (54.406). Online applicants go through the National Verifier's automated checks, with document upload as the fallback.

6 Data protection and biometrics

There is no single federal data protection statute or authority in the United States. For carriers, the sector-specific regime is CPNI. Carriers must train staff on when CPNI may be used and keep records of disclosures to third parties for at least one year. An officer must file an annual compliance certificate with the FCC by 1 March (47 CFR 64.2009). The FCC treats customer location data collected by a carrier as CPNI (FCC 24-40), which matters for any onboarding step that captures device location.

Breaches of CPNI must be reported electronically to the Secret Service and the FBI within seven business days of a reasonable determination of the breach. Customers may be told only after that, and breach records must be kept for two years (64.2011). The FCC adopted a broader breach rule in 2024, but its changes to this section remain delayed indefinitely (89 FR 9968). `Adopted, effective date not yet set`

FCC rules do not address biometrics. Selfie, liveness and voice biometrics used in onboarding fall under state biometric privacy laws such as those in Illinois, Texas and Washington, which differ in consent, notice and retention requirements. Lifeline eligibility documents must be kept for as long as the subscriber receives service and for at least the three preceding full calendar years (54.417).

7 Sector-specific obligations

SIM-swap and port-out protections waiting to take effect

Beyond authentication, the 2023 rules require providers to:

- maintain procedures for failed authentication attempts;
- notify the customer immediately when a SIM change or port-out request is received, before carrying it out;
- offer free account locks that block SIM changes and port-outs until the customer lifts them;
- run an easy process for reporting and fixing fraudulent changes, and give victims documentation on request;
- train staff on fraud attempts;
- keep three years of SIM change statistics, including successful fraudulent changes and time to remediate (88 FR 85794).

The order delayed the paperwork-related parts until approval by the Office of Management and Budget. The FCC's Wireline Competition Bureau then waived the rest, so that all the rules start together once a compliance date is published in the Federal Register (DA 24-649, para. 2). The FCC's 2026 regulatory agenda lists the next action as undetermined (Unified Agenda 2026).

Voice providers: customers, upstream providers and caller ID

Originating providers must know their customers and exercise due diligence (64.1200(n)(4)). They must also take reasonable steps against upstream providers that carry high volumes of illegal traffic (64.1200(n)(5)) and respond to traceback requests within 24

business hours (64.1200(n)(1)). A downstream provider may block traffic from a provider that fails to stop new and renewing customers from originating illegal calls (64.1200(k)(4)). Providers may use third parties to sign calls under the caller ID authentication framework (STIR/SHAKEN). The provider remains responsible for the attestation decision, and calls must be signed with its own certificate (90 FR 40241).

Lifeline duplicate and re-certification checks

Carriers must query the National Lifeline Accountability Database to block duplicate support at the same address. They must transmit subscriber identity data, update changes within ten business days and re-certify subscribers annually where the National Verifier does not do so (54.404(b), 54.410(f)).

8 Risk indicators and red flags

ACCOUNT TAKEOVER AND NETWORK ABUSE INDICATORS

- **Biographical answers only**: a caller who can give SSN digits or date of birth but not the account password.
- **Change then move**: a password or address change followed by a SIM change or port-out request.
- **Repeated failed authentication** on SIM change requests from the same caller or session.
- **Virtual or shared addresses**: a registered agent, virtual office or address unrelated to the business, a red flag named in the FCC's May 2026 proposal.
- **Thin commercial presence**: a newly created website or email address, or no registration in the claimed state of incorporation.
- **Untraceable payment** for high-volume voice service, such as cryptocurrency.
- **Traffic mismatch**: a domestic business customer whose calls originate from foreign IP addresses.

The address, presence, payment and traffic indicators come from the FCC's know-your-customer proposal (91 FR 30596). CISA advises account holders to add a carrier PIN and multi-factor authentication to counter SIM swapping, and to move away from SMS as a second factor (CISA, Mobile Communications Best Practice Guidance, December 2024).

9 Enforcement and penalties

FCC forfeitures are calculated per violation, with each day of a continuing violation counted separately, up to a cap per act or failure. For common carriers the maximum is $251,322 per violation or per day, up to $2,513,215 for a single continuing violation (47 CFR 1.80(b)). These figures reflect the January 2025 inflation adjustment (90 FR 3710); the FCC made no adjustment for 2026 (91 FR 39613). The FCC sets base amounts and adjusts them up or down for factors such as egregiousness, harm, prior violations, good faith and ability to pay.

In April 2024 the FCC fined the largest wireless carriers for failing to protect customer location data. The AT&T order assessed $57,265,625 (FCC 24-40). On 4 June 2026 the Supreme Court held that issuing forfeiture orders without a jury does not violate the Seventh Amendment. It reasoned that the orders do not finally settle liability, because a carrier that does not pay is entitled to a new trial in any Department of Justice collection suit (FCC v. AT&T, Inc., No. 25-406).

On know-your-customer duties, Lingo Telecom agreed in August 2024 to pay a $1,000,000 civil penalty and adopt a compliance plan over caller ID attestations for spoofed calls (DA 24-790). In February 2025 the FCC proposed a $4,492,500 penalty against Telnyx for failing to vet customers before they originated calls (FCC 25-10).

10 Recent changes and what to watch

- **9 Sep 2026** `Proposed, reply comments close 9 Nov 2026` Stricter screening, removal and re-entry rules for the Robocall Mitigation Database (91 FR 57454). A deficient filing could cut a provider off from carriers.
- **9 Jul 2026** `Proposed` Baseline know-your-upstream-provider checks and codified caller ID attestation levels (91 FR 42602). These would extend vetting from customers to wholesale partners.
- **4 Jun 2026** `Decided` Supreme Court upholds the FCC's forfeiture process without a jury (No. 25-406). FCC fines remain a live risk.
- **26 May 2026** `Proposed, comments closed 27 Jul 2026` Customer identification for new and renewing voice customers: name, physical address, government ID number and alternate phone number, with document verification and penalties per call (91 FR 30596). This would be the first prescriptive telecom customer identification rule.
- **8 May 2026** `Proposed` Tighter know-your-customer duties for resellers and other entities using telephone numbers (91 FR 25312).

- **3 Apr 2026** `Proposed` Lifeline reform, including collection of the full nine-digit SSN and checks of lawful status (91 FR 16871).
- **Pending since 2024** `Adopted, compliance not yet required` SIM-swap and port-out rules, awaiting a compliance date notice in the Federal Register (DA 24-649).

11 What this means for identity verification

Authentication is the core identity task for carriers. Knowledge-based checks built on SSN digits, date of birth or address do not meet the CPNI standard. Remote flows need a factor the customer holds or is: an existing password, a device-bound credential, a document check with face match, or a code sent to an established contact point.

Account-change events (password, address, online account creation) trigger immediate notices to the old contact details. Once the SIM-swap rules apply, SIM change and port-out requests will trigger a notice before execution, a lock check and three years of metrics.

For voice and cloud communications providers, onboarding should already collect and corroborate who the customer is and what they will use the service for. This matters most for high-volume and business accounts. The May 2026 proposal points towards government ID numbers, document copies and periodic re-verification.

Lifeline providers must route enrolment through the National Verifier or the state equivalent, register every field representative, and keep eligibility and identity documents for the life of the subscription plus at least three years. Biometric steps need state-law notice, consent and retention controls that vary by state.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Non-biographical authentication before SIM changes, port-outs and account access, using ID document capture, face match and biometric liveness.
- Remote KYC onboarding for new and renewing voice customers, with document verification including NFC chip reading.
- KYB and beneficial owner verification to corroborate business and high-volume calling customers.
- Phone and email verification plus configurable no-code workflows with an audit trail of every check.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **47 CFR 64.2003, 64.2009, 64.2010, 64.2011 (CPNI rules)**, eCFR, ecfr.gov
- **47 CFR 52.37, Number portability requirements for wireless providers**, eCFR, ecfr.gov
- **47 CFR 64.1200 and 64.6305 (call blocking, know-your-customer, Robocall Mitigation Database)**, eCFR, ecfr.gov
- **47 CFR 54.404, 54.406, 54.410, 54.417 (Lifeline)**, eCFR, ecfr.gov
- **47 CFR 1.80, Forfeiture proceedings**, eCFR, ecfr.gov
- **Protecting Consumers from SIM-Swap and Port-Out Fraud, FCC 23-95**, 88 FR 85794 (8 Dec 2023), federalregister.gov
- **Order, DA 24-649, WC Docket No. 21-341**, Wireline Competition Bureau (5 Jul 2024), fcc.gov
- **Data Breach Reporting Requirements**, 89 FR 9968 (12 Feb 2024), federalregister.gov

- **Enhancing Know-Your-Customer Requirements, FCC 26-27**, 91 FR 30596 (26 May 2026), federalregister.gov
- **Combatting Illegal Robocalls Through FCC Numbering Policies, FCC 26-17**, 91 FR 25312 (8 May 2026), federalregister.gov
- **Enhancing Know-Your-Upstream-Provider Requirements, FCC 26-32**, 91 FR 42602 (9 Jul 2026), federalregister.gov
- **Improving the Effectiveness of the Robocall Mitigation Database, FCC 26-49**, 91 FR 57454 (9 Sep 2026), federalregister.gov
- **Robocall Mitigation Database; effective date notice**, 91 FR 5242 (5 Feb 2026), federalregister.gov
- **Call Authentication Trust Anchor, FCC 24-120**, 90 FR 40241 (19 Aug 2025), federalregister.gov
- **Lifeline and Link Up Reform and Modernization, FCC 26-8**, 91 FR 16871 (3 Apr 2026), federalregister.gov
- **Unified Agenda of Federal Regulatory and Deregulatory Actions 2026** (14 Aug 2026), federalregister.gov
- **Annual Adjustment of Civil Monetary Penalties To Reflect Inflation**, 90 FR 3710 (15 Jan 2025), federalregister.gov
- **Notification of Cancelled Adjustment of Civil Monetary Penalties for Inflation**, 91 FR 39613 (30 Jun 2026), federalregister.gov
- **FCC v. AT&T, Inc., No. 25-406** (decided 4 Jun 2026), supremecourt.gov
- **AT&T Inc., Forfeiture Order, FCC 24-40** (29 Apr 2024), fcc.gov
- **Lingo Telecom, LLC, Order and Consent Decree, DA 24-790** (21 Aug 2024), fcc.gov
- **Telnyx LLC, Notice of Apparent Liability, FCC 25-10** (4 Feb 2025), fcc.gov
- **Resolve Application Errors, National Verifier**, USAC, usac.org
- **Mobile Communications Best Practice Guidance**, CISA (December 2024), pp. 1 to 2, cisa.gov