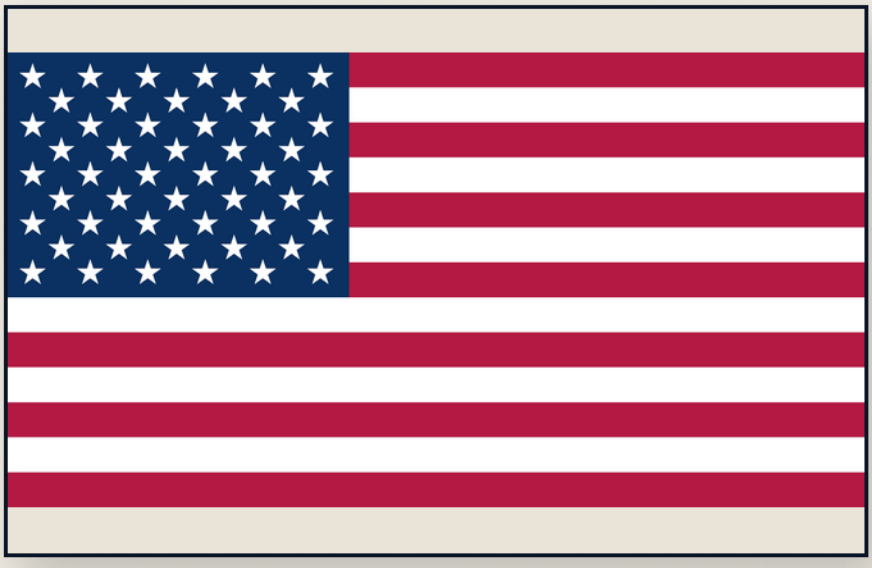
VOVE ID

VOVE COUNTRY CONTROL FILE

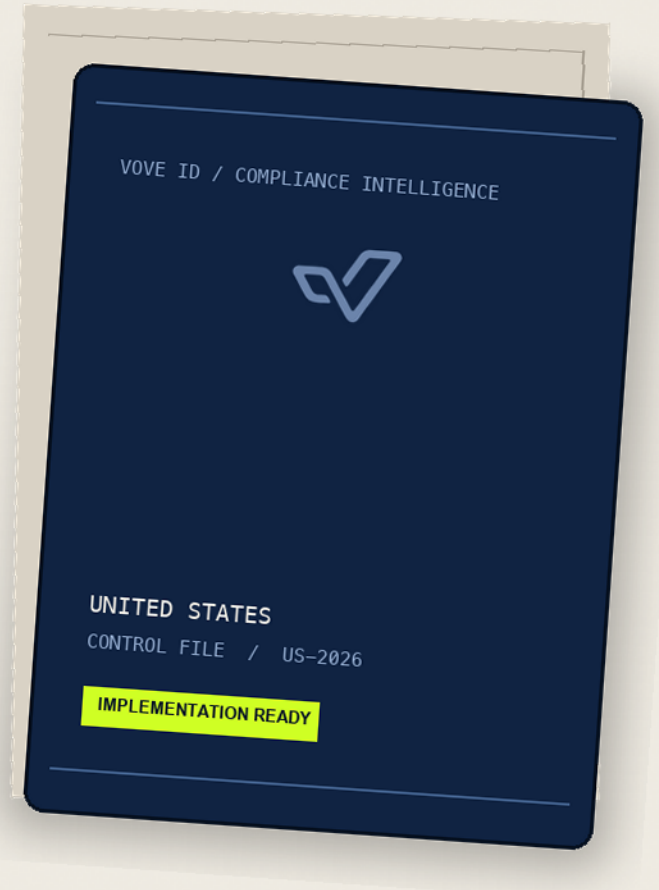
KYC / KYB / AML

2026 EDITION

UNITED STATES



UNITED STATES / US



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

United States KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for banks, fintechs, money services businesses, securities and commodities firms, virtual-currency businesses and other teams entering the United States. It separates federal Bank Secrecy Act and sanctions controls from sector-specific and state obligations; applicability must be resolved before any control is treated as mandatory.

Primary federal AML framework	**Bank Secrecy Act and 31 CFR Chapter X, with sector-specific rules**
Financial intelligence unit	**Financial Crimes Enforcement Network (FinCEN)**
Bank SAR trigger and timing	**$5,000 aggregate threshold; generally 30 days, or 60 days if no suspect is identified**
Currency transaction report	**More than $10,000 in currency aggregated by person and business day; file within 15 days**
Funds-transfer record / travel rule	**$3,000 or more, subject to exclusions and role-specific data requirements**
Covered-institution CDD ownership prong	**Each individual owning 25% or more, plus one control person, subject to exemptions and 2026 relief**
Corporate Transparency Act BOI	**U.S.-created entities and U.S. persons are exempt under the current rule; qualifying foreign registered entities remain in scope**
Core federal AML retention	**Generally 5 years, but the event that starts the clock varies by record**
Money transmission licensing	**FinCEN MSB registration may apply federally; separate state licences or exemptions must be analysed**
OFAC block / reject reporting	**Generally within 10 business days; blocked property also has an annual 30 September report**
Privacy and breach rules	**Sectoral federal rules plus state-by-state privacy, biometric and breach-notification requirements**
FATF public lists	**The United States was not named on the FATF public-list page reviewed 31 July 2026**

Scope and legal framework

The Bank Secrecy Act, codified principally at 31 U.S.C. 5311-5356, and its implementing rules in 31 CFR Chapter X form the core federal AML and reporting framework; USA PATRIOT Act provisions, including customer-identification and information-sharing rules, supplement that framework; OFAC administers U.S. economic and trade sanctions

independently of the BSA; Federal functional regulators and self-regulatory organisations apply sector rules and examination standards; State law separately controls areas including money transmission, virtual-currency licensing, privacy, biometrics and breach notification

FATF context

The United States has been a FATF member since 1990. As at 31 July 2026, it was not named on FATF's current public-list page for jurisdictions subject to increased monitoring or a call for action. FATF's United States country page records the 2016 mutual evaluation and subsequent follow-up; absence from a public list is not a finding that every control is fully effective.

IMPORTANT	This checklist is general regulatory information, not legal advice, a licence determination or a statement that every row applies to every U.S. business. It reflects primary and authoritative material reviewed on 31 July 2026. Confirm entity type, activity, customer, product, charter, federal functional regulator, state nexus, tribal or territorial issues, licensing exemptions, live BSA E-Filing instructions, sanctions programmes, privacy scope and later legal or court developments with qualified U.S. counsel and the competent authorities before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and licensing perimeter

Resolve the legal entity, activity, charter, product, customer location and state nexus first. U.S. AML duties differ materially by sector and federal registration does not replace state authorisation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
BSA obligations in 31 CFR Chapter X are defined by institution type; a bank, broker-dealer, casino and money services business do not share one identical programme or reporting rule set.	Build an entity-activity matrix that maps each product and customer flow to the relevant Chapter X part, federal functional regulator and examination manual.	Signed perimeter memorandum, charter and entity records, activity map, regulator mapping and counsel conclusions.	31 CFR Chapter X; FinCEN, Financial Institutions
A business that meets a money services business definition must register with FinCEN unless an exception applies; initial registration is generally due within 180 days and renewal is every two calendar years.	Classify each money transmission, exchange, cheque, prepaid-access and related service; register on time and calendar biennial renewal.	MSB analysis, Form 107 filing, acknowledgement, agent list, renewal calendar and exemption rationale where used.	31 CFR 1022.380; FinCEN, MSB Registration
FinCEN MSB registration is not a substitute for state money-transmitter or virtual-currency licensing, and requirements vary by state and activity.	Complete a state-by-state licensing and exemption analysis before serving residents or taking regulated activity into a state; track licence conditions and change triggers.	Fifty-state matrix, legal opinions, NMLS records, licences, exemptions, surety bonds and renewal controls.	California Financial Code, Money Transmission Act; NYDFS, Virtual Currency Businesses
The federal investment-adviser AML and SAR rule is not effective in 2026; FinCEN postponed its effective date to 1 January 2028.	Do not mislabel the postponed rule as a current federal duty. Track the rulemaking and separately implement obligations arising from other status, contracts, sanctions or risk policy.	Applicability memo, rule-change register, board decision and implementation roadmap for any future effective rule.	FinCEN final rule postponing IA AML Rule, 31 Dec. 2025

2. AML PROGRAMME, GOVERNANCE AND RISK ASSESSMENT

AML programme, governance and risk assessment

Design the programme for the institution category actually in scope and document why its controls are reasonably designed for the business's products, customers, channels and geographies.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Covered financial institutions must maintain a written, risk-based AML programme containing the elements prescribed for their sector, commonly internal controls, a responsible person, training and independent testing.	Map the applicable programme regulation to owned policies and controls; obtain governing-body approval where required and document independence and authority.	Approved AML programme, responsibility charter, organisation chart, training records, test plan, findings and remediation log.	31 U.S.C. 5318(h); applicable 31 CFR Chapter X sector part
The CDD Rule requires covered institutions to understand the nature and purpose of customer relationships, develop risk profiles, monitor for suspicious activity and update customer information on a risk basis.	Define risk factors, scoring logic, expected-activity capture, event-driven refresh triggers and escalation rules; do not rely solely on fixed periodic review dates.	Risk methodology, customer profile, model governance, alert scenarios, trigger catalogue, review samples and approvals.	31 CFR 1010.210; FinCEN, CDD Final Rule; FFIEC BSA/AML Manual, CDD
An effective programme must address products, services, customers, entities, delivery channels and geographic exposure, including new or materially changed activity.	Run a documented enterprise and product risk assessment before launch and after material change; link residual risks to controls and accepted exceptions.	Enterprise risk assessment, product approval, control inventory, residual-risk decisions and change log.	31 U.S.C. 5318(h); FFIEC BSA/AML Manual, BSA/AML Risk Assessment
Outsourcing a control does not remove the regulated institution's responsibility for compliance and effective oversight.	Perform due diligence before appointment, set measurable contractual requirements, control data and model changes, test performance and maintain exit capability.	Vendor due diligence, contract, service levels, audit rights, monitoring reports, issue register and exit plan.	FFIEC BSA/AML Manual, Developing Conclusions and Finalizing the Exam

3. CUSTOMER IDENTIFICATION AND IDENTITY VERIFICATION

Customer identification and identity verification

Customer Identification Program rules are sector-specific. The bank rule below is a useful control benchmark but must not be copied to an entity governed by a different CIP provision without confirming scope.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Before opening a bank account, the CIP must obtain at least name, date of birth for an individual, address and an identification number, subject to the rule's detailed alternatives and exceptions.	Configure mandatory fields by person and entity type; prevent opening or restrict use when required information is missing under the approved policy.	CIP policy, field rules, onboarding screenshots, test cases, exception approvals and sampled customer files.	31 CFR 1020.220(a)(2)
A bank CIP must contain risk-based procedures to verify identity to the extent reasonable and practicable within a reasonable time after account opening, using documentary, non-documentary or combined methods.	Define acceptable documents, database and device checks, fraud controls, discrepancy handling and a reasonable verification deadline by risk and channel.	Verification matrix, vendor configuration, decision logs, false-positive testing, discrepancy cases and quality assurance results.	31 CFR 1020.220(a)(2)(ii)
The CIP must explain when the institution will not open an account, restrict it, close it or file a SAR when it cannot form a reasonable belief that it knows the customer's true identity.	Implement explicit unresolved-identity states, permitted activity, time limits, escalation ownership, closure and SAR decisioning.	CIP failure procedure, case workflow, restriction rules, closure samples and SAR decision records.	31 CFR 1020.220(a)(2)(iii)
Bank CIP notice must be provided before account opening in a form reasonably designed to inform the customer that identifying information is being requested.	Place approved notice before submission in every assisted and digital channel and retain the deployed version and effective date.	Notice text, channel screenshots, version history, localisation review and deployment record.	31 CFR 1020.220(a)(5)

Legal entities and beneficial ownership

Keep customer due diligence under 31 CFR 1010.230 separate from Corporate Transparency Act reporting. They have different covered parties, tests and current exemptions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Covered institutions identify and verify each individual owning 25 percent or more of a legal-entity customer and one control person, subject to exclusions and exemptions.	Separate ownership and control prongs, test direct and indirect holdings, document exclusions and verify each in-scope person.	Ownership chart, certification, calculations, identity evidence, control-person rationale and exemption.	31 CFR 1010.230(d)-(e); FinCEN, CDD Final Rule
FinCEN's 2026 relief permits covered institutions to limit collection to the first account, when reliability is questioned and as needed through risk-based ongoing CDD.	Use the relief only within its terms, retain the verified record and refresh when facts call its reliability into question.	Relief analysis, policy, first-account marker, trigger logic, refresh cases and audit trail.	FinCEN Ruling FIN-2026-R001; 2026 CDD Rule FAQs
U.S.-created entities and U.S. persons are exempt from CTA BOI reporting; qualifying foreign-formed entities registered in the U.S. remain potentially in scope.	Classify formation and registration, document exemptions and keep CTA status separate from financial-institution CDD.	Formation and registration records, CTA memo, exemption proof and CDD-to-CTA reconciliation.	31 CFR 1010.380 as amended by 2025 interim final rule; FinCEN IFR Q&A;
A qualifying foreign company registered on or after 26 March 2025 generally has 30 days from the earlier of actual or public registration notice to file initial BOI; U.S. persons are not reported.	Calendar each deadline, collect only reportable BOI, file through FinCEN and monitor final-rule changes.	Deadline calculation, filing and receipt, supporting records, update monitoring and rule watch.	FinCEN, BOI Interim Final Rule Questions and Answers

Higher-risk customers, PEPs and enhanced due diligence

Use risk-based enhanced diligence. U.S. rules do not impose a single general domestic PEP-screening mandate, but specific foreign private-banking and correspondent-account rules can apply.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The CDD Rule does not create a unique general requirement to screen for or apply specific procedures to customers solely because they may be politically exposed persons.	Treat PEP information as a risk factor within CDD rather than an automatic prohibition; document the risk rationale, source of wealth or funds work and approval proportionate to the case.	PEP policy, risk factors, screening configuration, enhanced review, approvals and periodic quality testing.	Joint Statement on BSA Due Diligence Requirements for Customers Who May Be Considered PEPs, 2020
Covered U.S. financial institutions that maintain qualifying private-banking accounts for non-U.S. persons must perform enhanced scrutiny where a senior foreign political figure is involved.	Detect private-banking accounts and beneficial interests in scope; establish source-of-funds, purpose, expected activity and corruption-proceeds controls before and during the relationship.	Account classification, ownership analysis, source-of-wealth and funds evidence, senior approval, monitoring and reviews.	31 CFR 1010.620
Correspondent accounts for specified foreign financial institutions require due diligence and, for higher-risk categories, enhanced due diligence under the conditions in the rule.	Inventory foreign correspondent accounts, classify the foreign institution and jurisdiction, assess ownership and shell-bank exposure, and apply the required enhanced measures.	Correspondent inventory, foreign-bank questionnaire, ownership and licence checks, risk assessment and monitoring results.	31 CFR 1010.610; 31 CFR 1010.630
Customer information must be updated through risk-based ongoing monitoring when events reveal material changes or call existing information into question.	Trigger review for ownership, control, product, geography, sanctions, adverse activity and unexplained behaviour changes; record why the profile remains reliable or was revised.	Trigger catalogue, event logs, refreshed files, investigator rationale, approvals and overdue-review reporting.	FinCEN, CDD Final Rule; 2026 CDD Rule FAQs; FFIEC BSA/AML Manual, CDD

Monitoring, suspicious activity and information sharing

SAR thresholds and obligations depend on institution type. The bank rule below must be replaced with the applicable sector rule for MSBs, broker-dealers, casinos and other covered businesses.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A bank generally files a SAR for a transaction conducted or attempted by, at or through it involving at least $5,000 in aggregate when it knows, suspects or has reason to suspect one of the regulatory bases.	Map scenarios to the exact bank or other sector SAR rule, aggregate related activity, investigate promptly and document both filing and non-filing decisions.	Scenario inventory, alert and case data, aggregation tests, decision rationale, approvals and filed SAR receipt.	31 CFR 1020.320(a); use applicable sector rule
A bank SAR is generally due within 30 calendar days after initial detection of facts that may constitute a basis for filing, extended to 60 days only when no suspect is identified; urgent ongoing threats require immediate contact with appropriate law enforcement in addition to filing.	Start and evidence the regulatory clock at initial detection, distinguish research from impermissible delay, escalate deadline risk, and maintain an emergency contact procedure.	Clock logic, case timestamps, deadline dashboard, escalation records, law-enforcement contact log and filing confirmation.	31 CFR 1020.320(b)
SARs and information revealing their existence are confidential, with disclosure limited by the applicable regulation.	Restrict SAR access, redact customer-facing material, train staff against tipping off, control subpoenas and external requests, and log permitted disclosures.	Access-control list, training, disclosure procedure, audit logs, legal holds and tested response playbook.	31 CFR 1020.320(e); applicable sector SAR rule
Section 314(a) requests and voluntary 314(b) information sharing operate under defined scope, confidentiality and procedural protections; 314(b) participation requires a current notice to FinCEN.	Separate compulsory 314(a) search workflow from voluntary 314(b) sharing, validate counterparties and notices, secure transmissions and document use limitations.	314 procedures, current certification or notice, request log, search proof, response record and access controls.	31 CFR 1010.520; 31 CFR 1010.540; FinCEN Section 314 resources

Currency, funds transfers and cash reporting

Build separate decision paths for financial-institution CTRs, funds-transfer records and non-financial trade-or-business cash reports. They are not interchangeable with SARs.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A financial institution files a CTR for each deposit, withdrawal, exchange or other payment or transfer involving more than $10,000 in currency, aggregated for the same person during one business day when the institution has the required knowledge.	Aggregate across branches, channels and accounts; identify conductors and beneficiaries; apply exemptions only when documented and current.	Aggregation logic, CTR file and acknowledgement, identity record, exemption status, tests and exception report.	31 CFR 1010.311; 31 CFR 1010.313; FinCEN CTR FAQs
A CTR is generally filed within 15 calendar days after the reportable transaction date.	Calculate and monitor the deadline from transaction date, reconcile reportable activity to accepted filings and remediate rejects promptly.	Filing calendar, transaction-to-filing reconciliation, BSA E-Filing acknowledgement and reject handling.	31 CFR 1010.306(a)(1); FinCEN CTR FAQs
For transmittals of funds of $3,000 or more, covered roles must collect, retain and transmit specified information, subject to exclusions and the precise role-based requirements.	Determine whether the business is an originator's, intermediary or beneficiary's institution; configure the required data, preservation and transmission for domestic and cross-border flows.	Funds-flow map, message-field rules, transfer samples, exception logic, retention proof and quality tests.	31 CFR 1010.410(e)-(f); FinCEN Funds Travel Regulations FAQs
A trade or business that receives more than $10,000 in cash in one or related transactions generally files Form 8300 within 15 days and provides the required annual written statement to each named person by 31 January.	Detect cash and related transactions outside financial-institution CTR scope, file electronically when required, provide statements and retain records for five years.	Form 8300 assessment, filing and receipt, aggregation workpaper, customer statement and retention log.	26 U.S.C. 6050I; 31 U.S.C. 5331; IRS, Form 8300 guidance

8. SANCTIONS AND PROHIBITED ACTIVITY

Sanctions and prohibited activity

OFAC sanctions are separate from the BSA and can apply without a monetary threshold. Screening alone is insufficient without ownership, blocking, reporting and programme controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
U.S. persons must comply with applicable OFAC sanctions, including U.S.-organised entities and their foreign branches; some programmes also extend to foreign subsidiaries or non-U.S. persons in specified circumstances.	Map persons, entities, branches, products, currencies, locations and counterparties to each applicable sanctions programme and licence.	Sanctions applicability map, programme inventory, licences, legal interpretations and geographic controls.	OFAC FAQ 11; applicable sanctions programme regulations
Property owned 50 percent or more in the aggregate, directly or indirectly, by one or more blocked persons is itself blocked even when the entity is not named on OFAC's list.	Collect and calculate relevant ownership chains, aggregate blocked interests, assess control-related risk and escalate uncertainty before releasing property.	Ownership chart, calculations, screening result, legal escalation, disposition decision and audit trail.	OFAC, Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked
Initial reports of blocked or rejected transactions are generally due to OFAC within 10 business days; holders of blocked property file an annual report by 30 September.	Freeze or reject as the programme requires, preserve funds, notify OFAC through the current channel, reconcile blocked property and calendar annual reporting.	Block or reject decision, account restriction, report and acknowledgement, blocked-property ledger and annual filing.	31 CFR 501.603-604; OFAC Reporting FAQ
OFAC expects a risk-based sanctions compliance programme; its framework describes management commitment, risk assessment, internal controls, testing or auditing and training as essential components.	Implement the five components, tune screening for names, ownership, geography, IP and transaction context, and independently test end-to-end effectiveness.	Sanctions programme, risk assessment, screening configuration, alert decisions, test report, training and remediation.	OFAC, A Framework for OFAC Compliance Commitments

Records, audit trail and regulator access

Retention periods often last five years, but different records use different start events. Preserve provenance and retrieval as well as the document itself.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Bank CIP identifying information is retained for five years after the account is closed or becomes dormant; descriptions of verification documents, methods, results and discrepancy resolution are retained for five years after the record is made.	Configure separate retention clocks for identifying data and verification records and test closure, dormancy and record-creation events.	Retention schedule, data map, clock logic, deletion holds, retrieval test and sampled records.	31 CFR 1020.220(a)(3)
A bank retains each SAR and supporting documentation for five years from filing and provides supporting documentation to FinCEN or appropriate law enforcement on request.	Bind supporting evidence to the filing, preserve confidentiality, control authorised requests and prove complete retrieval within the response procedure.	SAR archive, supporting-document index, request log, access audit and retrieval test.	31 CFR 1020.320(d)
Unless a more specific rule provides otherwise, records required under 31 CFR Chapter X are generally retained for five years and kept accessible as specified by the rule.	Map every BSA record to its governing provision, trigger event, format, location, owner, legal hold and destruction approval.	Regulatory retention schedule, data inventory, immutable logs, legal-hold procedure and destruction certificates.	31 CFR 1010.430
MSBs must maintain the registration form and specified supporting and agent-list records for five years and make them available as required.	Keep the registration package, owner or controlling-person records and agent list current, retrievable and linked to renewal and material changes.	Registration archive, agent list, update log, renewal file and retrieval test.	31 CFR 1022.380; FinCEN, MSB Registration

Privacy, biometrics, security and breach response

There is no single general U.S. privacy rule or regulator for every business. Determine sector, state, data type, residency and threshold before selecting notices, rights, security and breach deadlines.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
FTC-jurisdiction financial institutions maintain a written security programme; specified events involving at least 500 consumers' unencrypted information require FTC notice no later than 30 days after discovery.	Confirm scope, appoint a qualified individual, assess risk, implement the prescribed safeguards, oversee providers and apply the 500-consumer notice test.	Scope memo, security programme, qualified-individual report, risk assessment, tests, vendor oversight and notice decision.	16 CFR Part 314; FTC, Safeguards Rule guidance
Covered SEC institutions maintain incident-response policies and generally notify affected individuals as soon as practicable, no later than 30 days after awareness of unauthorised access or use, subject to the rule's investigation-based exception.	Confirm scope, assess customer-information incidents, document any exception and oversee service-provider notice duties.	Scope memo, response programme, investigation, notice, exception rationale and vendor contract.	SEC Regulation S-P amendments, Release No. 34-100155 (2024)
A banking organisation notifies its primary federal regulator no later than 36 hours after determining that a qualifying computer-security incident occurred.	Define the incident test and decision authority, maintain regulator contacts and preserve each determination and notice timestamp.	Incident taxonomy, decision log, regulator notice, acknowledgement, contacts and exercise results.	12 CFR 53.3, 225.302 and 304.23; federal banking-agency notification rule
State privacy, biometric and breach laws apply independently; examples include California's CCPA and breach rules and Illinois BIPA's biometric-data controls.	Map state scope by person, data and threshold; implement the required notices, consent, rights, retention, security and breach workflows.	State matrix, notices, biometric consent, retention schedule, rights log, breach analysis and filings.	California Consumer Privacy Act and regulations; California Civ. Code 1798.82; Illinois 740 ILCS 14

11. PRODUCT OVERLAYS AND REGULATORY CHANGE CONTROL

Product overlays and regulatory change control

Apply product-specific overlays without importing vacated, postponed or proposed requirements into the current-law checklist.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A person engaged as a business in accepting and transmitting convertible virtual currency, or buying or selling it, may be a FinCEN money transmitter unless an exemption applies; a person using it solely to purchase goods or services is not an MSB on that basis.	Document each custody, exchange, transmission, hosted-wallet, kiosk and payment flow against FinCEN's function-based CVC analysis and state virtual-currency rules.	CVC flow diagrams, legal classification, MSB registration, state licences, exemptions and transaction-monitoring design.	FinCEN FIN-2013-G001; FinCEN CVC Business Models Guidance, 2019
Virtual-currency transactions are subject to the same OFAC compliance obligations as transactions involving traditional currency.	Screen wallet and counterparty data, blockchain exposure, geolocation and ownership; apply blocking or rejection and reporting according to the relevant programme.	Blockchain-risk policy, analytics configuration, address and party screening, case files, block or reject reports and testing.	OFAC FAQ 560; OFAC Sanctions Compliance Guidance for the Virtual Currency Industry
The federal Residential Real Estate Rule currently has no legal effect while the March 2026 vacatur order remains in force; reporting persons are not presently required to file Real Estate Reports and FinCEN's appeal is pending.	Do not present Real Estate Reports as currently mandatory. Monitor the appeal and FinCEN guidance, preserve launch readiness and apply other existing BSA, sanctions or state duties that independently cover the activity.	Court-status watch, FinCEN update log, applicability memo, dormant control plan and reactivation checklist.	FinCEN Residential Real Estate FAQs, issued 18 May 2026
Material legal, court, product, channel, vendor, model and geographic changes require reassessment before the affected control or customer flow is released.	Operate a dated regulatory inventory and change process with accountable owners, source snapshots, impact assessment, implementation testing and approval.	Regulatory inventory, change tickets, source archive, impact assessment, test results, approvals and next-review date.	31 U.S.C. 5318(h); risk-based programme and supervisory expectations

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

Bank Secrecy Act
U.S. Government Publishing Office · Official statutory compilation
Open official source

31 CFR Chapter X - Financial Crimes Enforcement Network
Electronic Code of Federal Regulations · Primary regulation
Open official source

Customer Identification Program for banks
Electronic Code of Federal Regulations · Primary regulation
Open official source

Customer Due Diligence requirements for legal entity customers
Electronic Code of Federal Regulations · Primary regulation
Open official source

CDD Final Rule overview and 2026 exceptive relief
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

CDD Rule consolidated FAQs updated May 2026
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Suspicious Activity Reports by banks
Electronic Code of Federal Regulations · Primary regulation
Open official source

Records relating to funds transfers and transmittals
Electronic Code of Federal Regulations · Primary regulation
Open official source

General BSA record retention rule
Electronic Code of Federal Regulations · Primary regulation
Open official source

Due diligence for foreign correspondent accounts
Electronic Code of Federal Regulations · Primary regulation
Open official source

Due diligence for private-banking accounts
Electronic Code of Federal Regulations · Primary regulation
Open official source

Section 314(a) information requests
Electronic Code of Federal Regulations · Primary regulation
Open official source

Section 314(b) voluntary information sharing
Electronic Code of Federal Regulations · Primary regulation
Open official source

Currency Transaction Report FAQs
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Funds Travel Regulations FAQs
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Money Services Business registration
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Convertible virtual currency guidance FIN-2013-G001
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Convertible virtual currency business models guidance
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

BOI interim final rule questions and answers
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Investment Adviser AML Rule effective date postponed to 2028
Financial Crimes Enforcement Network · Official regulator publication
Open official source

Residential Real Estate Rule current status FAQs
Financial Crimes Enforcement Network · Official regulator guidance
Open official source

Joint PEP due-diligence statement
Federal banking agencies, FinCEN and State Bank Regulators · Official interagency statement
Open official source

FFIEC BSA/AML Manual - Customer Due Diligence
Federal Financial Institutions Examination Council · Official examination guidance
Open official source

Form 8300 cash-reporting guidance
Internal Revenue Service · Official regulator guidance
Open official source

OFAC compliance framework
Office of Foreign Assets Control · Official regulator framework
Open official source

OFAC 50 Percent Rule guidance
Office of Foreign Assets Control · Official regulator guidance
Open official source

OFAC FAQ 11 - persons required to comply
Office of Foreign Assets Control · Official regulator guidance
Open official source

OFAC reporting requirements FAQs
Office of Foreign Assets Control · Official regulator guidance
Open official source

OFAC virtual-currency FAQ 560
Office of Foreign Assets Control · Official regulator guidance
Open official source

FTC Safeguards Rule guidance
Federal Trade Commission · Official regulator guidance
Open official source

SEC Regulation S-P amendments
U.S. Securities and Exchange Commission · Official regulator publication
Open official source

Computer-security incident notification rule
Federal Deposit Insurance Corporation · Official interagency rule guidance
Open official source

California Consumer Privacy Act regulations
California Privacy Protection Agency · Primary and official state material
Open official source

California data-breach reporting guidance
California Department of Justice · Official state guidance
Open official source

Illinois Biometric Information Privacy Act
Supreme Court of Illinois · Official judicial explanation of state legislation
Open official source

California money-transmitter laws and regulations
California Department of Financial Protection and Innovation · Official state material
Open official source

New York virtual-currency business licensing
New York State Department of Financial Services · Official state guidance
Open official source

FATF United States country page
Financial Action Task Force · Official international assessment
Open official source

FATF black and grey lists
Financial Action Task Force · Official current-status source
Open official source

Document control

Version 1.1 / Published 31 July 2026 / Last reviewed 31 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice, a licence determination or a statement that every row applies to every U.S. business. It reflects primary and authoritative material reviewed on 31 July 2026. Confirm entity type, activity, customer, product, charter, federal functional regulator, state nexus, tribal or territorial issues, licensing exemptions, live BSA E-Filing instructions, sanctions programmes, privacy scope and later legal or court developments with qualified U.S. counsel and the competent authorities before launch.