Identomat

COMPLIANCE GUIDE

# Banking & Digital Banking Compliance in the United States

COUNTRY United States

INDUSTRY Banking & Digital Banking

LAST UPDATED 16 October 2026

KEY REGULATORS Financial Crimes Enforcement Network · Office of the Comptroller of the Currency · Federal Deposit Insurance Corporation

## Key takeaways

- To take deposits you need a charter, from the federal banking regulator or a state, plus federal deposit insurance. A fintech without a charter usually reaches customers through a partner bank, and that bank stays fully responsible for identity checks done on its behalf.
- Every new account needs four facts before it is opened: name, date of birth, address and an identification number (a Social Security or other taxpayer number for U.S. persons). The bank must then verify identity within a reasonable time, using documents, database checks or both.
- Opening accounts fully online is allowed. The bank's written procedures must cover customers who never come to a branch, and examiners treat accounts opened without face-to-face contact as potentially higher risk, so expect closer monitoring of new digital accounts.
- State-issued mobile driver's licences and other government digital IDs can now count as government-issued ID for account opening (federal guidance of September 2026), and banks may optionally get a customer's taxpayer number from a trusted third-party source instead of asking the customer.
- Several big changes are still proposals, not law: a rewrite of anti-money laundering programme rules and new guidance on managing fintech and vendor partners. Anti-money laundering rules for investment advisers are adopted but apply only from 1 January 2028.

---

The United States is open to digital banking, but there is no separate licence for an online bank: a digital-only bank holds the same charter and deposit insurance as a branch-based one and follows the same identity rules. Most neobanks operate through a chartered partner bank rather than holding a charter of their own.

The principal authorities are the Financial Crimes Enforcement Network, which writes the anti-money laundering rules, and the federal banking agencies that charter, insure and examine banks: the Office of the Comptroller of the Currency, the Federal Reserve and the Federal Deposit Insurance Corporation, with the National Credit Union Administration for credit unions and state departments for state-chartered banks.

The biggest obstacle for a new entrant is the charter and deposit insurance process itself. For a fintech using a partner bank, it is meeting the bank's customer identification programme and monitoring standards, since the bank answers to its examiners for every account the fintech opens.

CONTENTS


1 Who regulates this sector
2 Licensing and authorisation
3 AML, KYC and customer due diligence
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

Banking supervision in the United States is split between federal and state authorities, and between the agency that writes anti-money laundering rules and the agencies that examine banks against them. A bank always has one primary federal regulator, determined by its charter and Federal Reserve membership.

| Authority | Remit | Level | Official site |
|---|---|---|---|
| FinCEN (U.S. Treasury) | Administers the Bank Secrecy Act; writes customer identification, due diligence and reporting rules; civil penalties | Federal | fincen.gov |
| Office of the Comptroller of the Currency (OCC) | Charters and supervises national banks and federal savings associations | Federal | occ.gov |
| Federal Reserve Board | Supervises state member banks and bank holding companies | Federal | federalreserve.gov |
| Federal Deposit Insurance Corporation (FDIC) | Grants deposit insurance; supervises state non-member banks | Federal | fdic.gov |
| National Credit Union Administration (NCUA) | Charters federal credit unions; insures credit union deposits | Federal | ncua.gov |

| | | | |
|---|---|---|---|
| Federal Financial Institutions Examination Council (FFIEC) | Interagency body that publishes the BSA/AML Examination Manual and shared guidance; not itself a supervisor | Federal (coordinating) | ffiec.gov |
| Office of Foreign Assets Control (OFAC) | Economic sanctions programmes and enforcement | Federal | ofac.treasury.gov |
| Consumer Financial Protection Bureau (CFPB) | Federal consumer financial law for larger banks and certain non-banks | Federal | consumerfinance.gov |
| SEC and FINRA | Securities regulator and the self-regulatory organisation for broker-dealers | Federal / self-regulatory | sec.gov, finra.org |
| State banking departments (for example New York DFS, California DFPI) | Charter and supervise state banks alongside the FDIC or Federal Reserve | State | dfs.ny.gov, dfpi.ca.gov |

## 2 Licensing and authorisation

Anyone wishing to establish a national bank or federal savings association must apply to the OCC and obtain its prior approval (12 CFR 5.20). A state bank is chartered by its state banking department instead. In either case, a proposed bank applies separately to the FDIC for deposit insurance under section 5 of the Federal Deposit Insurance Act (12 CFR 303, Subpart B). The process for a new (de novo) bank is long, and the conditions attached to approval often include business plan, capital and compliance commitments specific to the applicant.

There is no separate online or digital banking licence: a digital-only bank holds an ordinary charter. A business that only markets deposit accounts or cards through a partner bank does not need a bank charter, but money transmission and lending activities of its own may need state licences.

The OCC amended its chartering rule with effect from 1 April 2026 to confirm that national banks limited to trust company operations may also carry on non-fiduciary activities (91 FR

9977). This affects firms, including technology and digital asset companies, that seek a national trust charter rather than a full-service bank charter.

## 3 AML, KYC and customer due diligence

Banks are financial institutions under the Bank Secrecy Act (BSA) and must maintain a written anti-money laundering programme. FinCEN's rules for banks sit in 31 CFR Part 1020, alongside each banking agency's parallel rule.

### Customer identification programme

A written programme, approved by the board, covering data collection, verification, recordkeeping, government-list checks and customer notice (31 CFR 1020.220).

### Ongoing due diligence

Risk-based procedures to understand the nature and purpose of each relationship, build a customer risk profile, monitor and, on a risk basis, update customer information.

### Beneficial ownership

For legal entity customers: each individual owning 25 percent or more of the equity, plus one individual with significant control (31 CFR 1010.230).

### Records

Identifying data kept five years after the account closes; verification records five years after they are made; other BSA records five years (31 CFR 1010.430).

### Beneficial ownership relief `Optional relief`

Since 13 February 2026, a FinCEN order (FIN-2026-R001) lets covered financial institutions identify and verify a legal entity's beneficial owners only when the entity first opens an account, when facts call earlier information into question, or as their risk-based procedures require, rather than at every new account. The relief is discretionary: a bank that wants to rely on it must say so in its own procedures, and may keep collecting at every opening.

### Reporting thresholds

Suspicious activity reports (SARs) follow the banking agencies' tiered rules, shown here from the OCC's version (12 CFR 21.11) and mirrored in FinCEN's 31 CFR 1020.320:

| Trigger | Threshold |
| --- | --- |

| | |
|---|---|
| Insider abuse (directors, officers, employees, agents) | Any amount |
| Suspected federal crime where a suspect can be identified | $5,000 or more |
| Suspected federal crime, no identifiable suspect | $25,000 or more |
| Potential money laundering, structuring or BSA evasion | $5,000 or more |
| Filing deadline | 30 calendar days from initial detection; up to 60 days if no suspect is yet identified |
| Currency transaction report | Cash transactions of more than $10,000 (31 CFR 1010.311) |
| Funds transfer recordkeeping and travel rule | Transmittals of $3,000 or more (31 CFR 1010.410(e)-(f)) |

Banks must also search their records when FinCEN relays a law enforcement request (31 CFR 1010.520), and may share information with other financial institutions under the voluntary safe harbour in 31 CFR 1010.540.

## 4 Identity verification and onboarding

Before opening an account, a bank must obtain at least the customer's name, date of birth (for individuals), a residential or business street address, and an identification number: a taxpayer identification number for U.S. persons, or for non-U.S. persons a taxpayer number, passport number and country of issuance, alien identification card number, or the number of another government-issued photo document evidencing nationality or residence (31 CFR 1020.220(a)(2)(i)). Verification may follow within a reasonable time after opening; the programme must state what the customer can do with the account meanwhile, and when the bank will close it or file a SAR if verification fails.

### Documentary and non-documentary verification

Documentary verification typically means an unexpired government-issued photo ID such as a driver's licence or passport; for entities, documents such as certified articles of incorporation or a business licence. The FFIEC manual encourages reviewing more than one

document because of counterfeit risk. Non-documentary methods include comparing customer data with a consumer reporting agency, public database or other source, contacting the customer, checking references and obtaining financial statements. The rule does not prescribe biometrics, selfie matching or liveness detection; these are permitted tools within a bank's risk-based procedures rather than legal requirements.

### Digital credentials and taxpayer numbers

FAQs issued on 8 September 2026 by FinCEN with the staffs of the Federal Reserve, FDIC, NCUA and OCC state that an unexpired state-issued mobile driver's licence, or another government-issued verifiable digital credential, qualifies as government-issued identification if the bank can extract the data and its programme allows it. Credentials issued by non-government parties may be used as a non-documentary method only if the issuer authenticates as strongly as the bank itself would. A June 2025 exemption order from the OCC, FDIC and NCUA, with FinCEN's concurrence, lets banks they supervise obtain taxpayer identification numbers from a third-party source rather than from the customer, provided the number is obtained before opening; use of the exemption is optional. The Federal Reserve issued a parallel order for its banks.

### Reliance and third parties

A bank may rely on another financial institution's identification only if reliance is reasonable, the other institution has its own BSA programme and a federal functional regulator, and it certifies annually by contract (31 CFR 1020.220(a)(6)). A fintech partner or identity vendor is not covered by that safe harbour: it acts as the bank's agent, and the FFIEC manual states that the bank remains ultimately responsible for compliance with the identification rule.

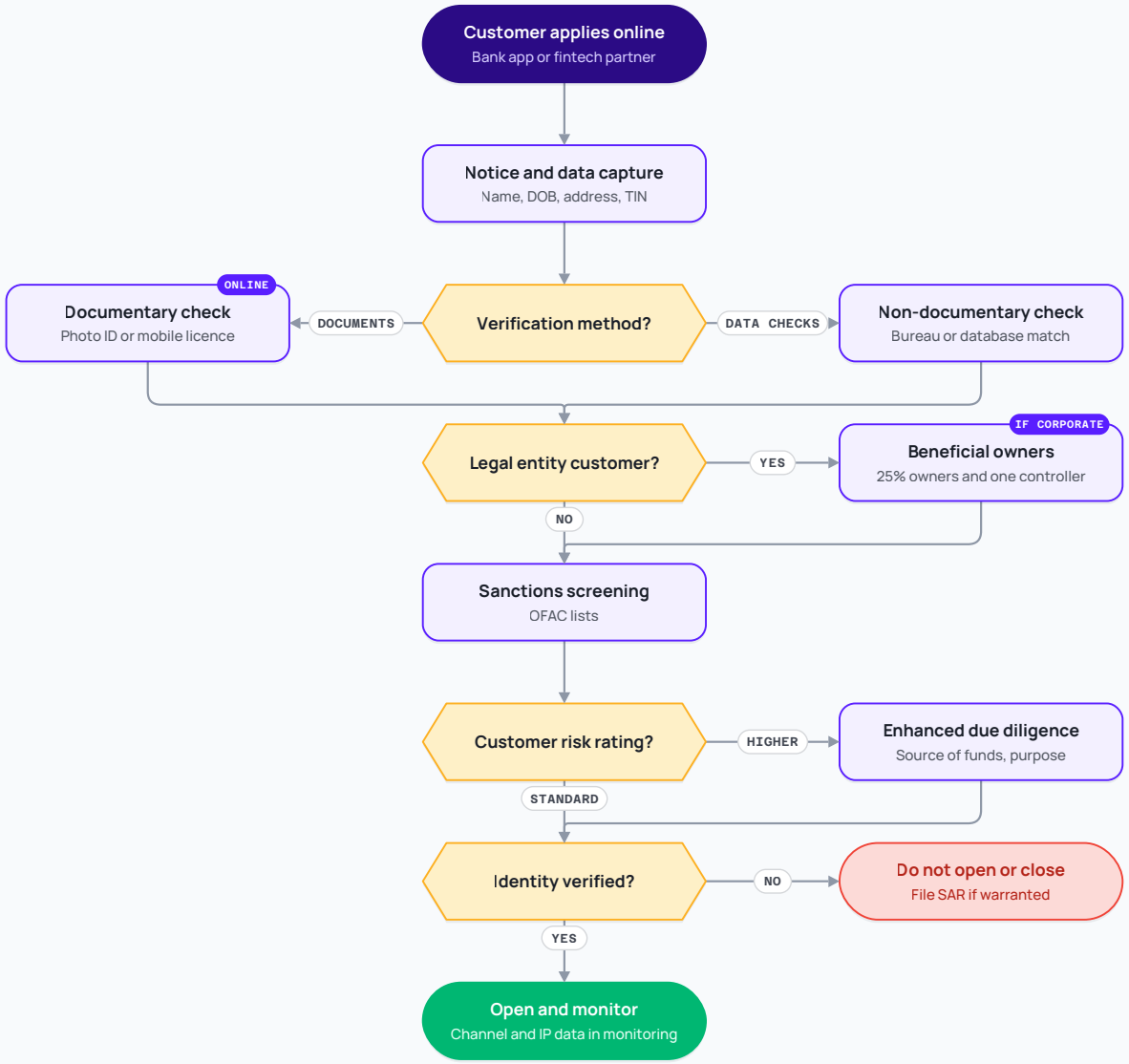



Figure 1. Remote retail and business account opening at a U.S. bank or through its fintech partner.

## 5 Digital channels: what's different

**Bottom line:** the identification rule is channel-neutral in what it requires, but a bank opening accounts online must have non-documentary procedures for customers who never appear in person, and examiners treat those accounts as potentially higher risk.

| Requirement | In person / branch | Online / remote | Difference |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Permission to open accounts** | Permitted | Permitted; procedures must address customers not present | Differs |
| **Data collected before opening** | Name, DOB, address, ID number | Same four elements | Same |
| **Verification approach** | Usually inspection of a photo ID | Non-documentary methods required where no documents are seen | Differs |
| **Government digital credentials** | Mobile licence may count as ID | Mobile licence may count as ID | Same |
| **Risk treatment** | Risk-based | Potentially higher risk; channel is a monitoring factor | Differs |
| **Taxpayer number source** | Customer or third party (optional order) | Customer or third party (optional order) | Same |
| **Access authentication** | Branch identification | Risk-assessed; MFA where single-factor is inadequate | Differs |
| **Responsibility when a third party onboards** | Bank remains responsible | Bank remains responsible | Same |

### Non-face-to-face accounts are a risk factor

The FFIEC BSA/AML Examination Manual's electronic banking section tells management to treat online account opening as a potentially higher-risk area: identity is harder to verify, the customer may be outside the bank's market, and the account may front for an unknown third party. It expects banks to include how an account was opened in deciding the level of monitoring, to use reports such as IP address changes and linked accounts sharing addresses, phones, emails or taxpayer numbers, and to set policies on when a customer must open an account face to face. This is supervisory guidance, not a regulation, but it is what examiners test.

### Authentication after onboarding

The FFIEC's 2021 guidance on authentication and access, published by the Federal Reserve as SR 21-14, states that single-factor authentication, even with layered security, has proved inadequate for high-risk transactions and users, and that multifactor

authentication or controls of equivalent strength should follow where a bank's risk assessment shows the need. It applies whether the bank or a third party provides the digital banking platform.

### Fintech partnerships and banking as a service

The 2023 Interagency Guidance on Third-Party Relationships states that using a third party does not diminish a bank's responsibility to comply with law as if it performed the activity itself. A September 2026 proposal would replace it with a more tailored, risk-based text `Proposed, comments close 16 Nov 2026`; the bank's ultimate responsibility is unchanged in the proposal.

## 6 Data protection and biometrics

There is no single federal data protection statute or authority. For banks, customer information security is governed by the Interagency Guidelines Establishing Information Security Standards, which implement the Gramm-Leach-Bliley Act and, as the FFIEC's 2021 authentication guidance summarises, require banks to safeguard the information of consumers with whom they have a continuing relationship. That includes identity documents and verification results collected at onboarding. The identification rule requires a description of documents relied on rather than copies; banks that keep images must apply the BSA's five-year retention rule to them.

Federal banking law does not regulate biometric data as a category. Selfie matching, liveness checks and face templates are instead governed by state law: several states, including Illinois, Texas and Washington, have biometric privacy statutes, and comprehensive state privacy laws such as California's add further duties. Consent, notice, retention and destruction duties therefore depend on where customers live, and a nationwide digital bank should design its biometric flow for the strictest state it serves.

## 7 Sector-specific obligations

### Correspondent and private banking

Covered institutions need risk-based, and where necessary enhanced, due diligence for correspondent accounts held for foreign financial institutions (31 CFR 1010.610). For private banking accounts, they must identify nominal and beneficial owners, determine whether any is a senior foreign political figure, and establish source of funds and expected

use (31 CFR 1010.620). FinCEN can also impose special measures cutting off named foreign institutions, and has proposed or finalised several since 2025.

### Securities and investment firms

Identity rules outside banking follow the same model under separate parts of FinCEN's rules: customer identification programmes for broker-dealers (31 CFR 1023.220), mutual funds (31 CFR 1024.220) and futures commission merchants and introducing brokers (31 CFR 1026.220). Broker-dealers must also maintain an AML programme meeting their regulator's and self-regulatory organisation's requirements (31 CFR 1023.210). Registered investment advisers have no AML programme or SAR obligation yet: FinCEN delayed its 2024 adviser rule to 1 January 2028 (91 FR 36) `Adopted, effective 1 Jan 2028`, and a 2024 joint SEC and FinCEN proposal for adviser identification programmes remains a proposal `Proposed, not adopted`.

### Supervision without reputation risk

A final OCC and FDIC rule effective 9 June 2026 removes reputation risk from their supervision and bars them from pressing banks to close or refuse accounts because of a customer's political, religious or other protected views or lawful but disfavoured business (91 FR 18279). The Federal Reserve has proposed a similar rule `Proposed`. Account decisions still have to rest on documented illicit-finance and other financial risk.

## 8 Risk indicators and red flags

DIGITAL BANKING INDICATORS FROM FFIEC AND FINCEN SOURCES

- **Unverifiable remote applicant**: identity checks fail or stall while the account is already in use.
- **Linked accounts**: several accounts sharing an address, phone number, email or taxpayer number.
- **IP and location anomalies**: frequent IP address changes or access from outside the bank's market.
- **High velocity**: funds moving in and out of a new online account quickly.
- **Many cards per account**: an unusual number of debit cards tied to one account.
- **Front company**: an entity account apparently used for an unknown third party.
- **Priority typologies**: activity linked to Chinese money laundering networks, southwest border illicit finance and trade-based laundering, the focus of FinCEN's October 2026 action.

## 9 Enforcement and penalties

FinCEN civil penalties are set per violation and inflation-adjusted, last on 17 January 2025 (31 CFR 1010.821). For penalties assessed on or after that date: a willful BSA violation carries $71,545 to $286,184 under the general provision (31 U.S.C. 5321(a)(1)); a negligent violation up to $1,430, and a pattern of negligent activity up to $111,308; and violations of the correspondent and private banking due diligence rules or special measures up to $1,776,364. Each banking agency can separately impose civil money penalties and cease-and-desist orders, OFAC penalises sanctions breaches, and willful violations can be prosecuted criminally.

On 13 October 2026 FinCEN assessed a $1.2 billion penalty against Bank of America, N.A., which admitted willfully failing to maintain an adequate AML programme, conduct correspondent due diligence and file SARs (FinCEN). The OCC concurrently assessed a $750 million civil money penalty, its largest against a bank, credited against FinCEN's amount, finding the bank failed to remediate under a December 2024 cease-and-desist order (OCC NR 2026-89). OFAC settled related sanctions matters for $11.6 million.

## 10 Recent changes and what to watch

- **13 Oct 2026**: FinCEN and OCC penalties against Bank of America `Final`. Shows examiners will escalate when a bank fails to deliver on a remediation order.
- **15 Sep 2026**: Proposed interagency third-party risk management guidance `Proposed, comments close 16 Nov 2026`. Would replace the 2023 guidance that governs bank-fintech partnerships.
- **8 Sep 2026**: FAQs on mobile driver's licences and verifiable digital credentials under the identification rule `Guidance in effect`. Opens a documentary route for fully digital onboarding.
- **9 Jun 2026**: OCC and FDIC reputation risk rule `In force`. Supervisors may no longer cite reputation risk.
- **Apr to Jul 2026**: AML/CFT programme reform proposals from FinCEN, the OCC, FDIC and NCUA, and the Federal Reserve `Proposed, comments closed 9 Jun and 8 Sep 2026`. Would refocus programmes on effectiveness and higher risks; current programme rules apply until a final rule.
- **13 Feb 2026**: Beneficial ownership exceptive relief `Optional relief`. No need to re-verify owners at every new account if procedures say so.
- **Aug 2025**: CFPB reconsideration of the personal financial data rights (open banking) rule `Under reconsideration`. Affects how banks share data with fintech apps that customers authorise.

## 11 What this means for identity verification

Remote onboarding design for a U.S. bank or its partners should capture the four required data elements before the account opens and record which method verified each customer, because the rule requires a description of documents relied on and of non-documentary methods and their results. Combining document checks with database matching gives the bank a fallback for customers whose documents cannot be read or trusted, which the rule requires for customers not present in person.

Accepting mobile driver's licences is now supported by federal guidance, but only where the bank can read the credential's data; third-party digital credentials need evidence that the issuer authenticates at the bank's own standard. Biometric matching and liveness are not federal requirements, so their use should be justified by the risk assessment and built around state biometric privacy laws. Monitoring should carry onboarding signals forward: channel, device and IP data, and links between accounts. For legal entities, owners must be

verified at first opening and again when information becomes doubtful. Where a fintech or vendor performs any of these steps, the contract, testing and records must let the bank show examiners that the work meets its own programme.

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:

- Remote customer identification with ID document capture and verification, including mobile driver's licence and NFC chip reading, face match and biometric liveness.
- KYB and beneficial owner verification for legal entity customers at first account opening and when ownership information changes.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring afterwards.
- A no-code workflow builder to combine documentary and non-documentary checks, with an audit trail of the methods and results for each customer.

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

- **31 CFR 1020.220, Customer identification program requirements for banks**, eCFR, ecfr.gov
- **31 CFR 1010.230, Beneficial ownership requirements for legal entity customers**, eCFR, ecfr.gov
- **31 CFR 1020.320, Reports by banks of suspicious transactions**, eCFR, ecfr.gov
- **12 CFR 21.11, Suspicious Activity Report (OCC)**, eCFR, ecfr.gov

- **31 CFR 1010.311, Filing obligations for reports of transactions in currency**, eCFR, ecfr.gov
- **31 CFR 1010.410, Records to be made and retained by financial institutions**, eCFR, ecfr.gov
- **31 CFR 1010.430, Nature of records and retention period**, eCFR, ecfr.gov
- **31 CFR 1010.520 and 1010.540, Information sharing**, eCFR, ecfr.gov
- **31 CFR 1010.610 and 1010.620, Correspondent and private banking due diligence**, eCFR, ecfr.gov
- **31 CFR 1010.821, Penalty adjustment and table** (amounts for penalties assessed on or after 17 January 2025), eCFR, ecfr.gov
- **31 CFR 1023.210, 1023.220, 1024.220, 1026.220, Securities and futures AML and CIP rules**, eCFR, ecfr.gov
- **12 CFR 5.20, Organizing a national bank or Federal savings association**, eCFR, ecfr.gov
- **12 CFR 303, Subpart B, Deposit insurance**, eCFR, ecfr.gov
- **FAQs Regarding Treatment of Verifiable Digital Credentials Under the CIP Rule**, FinCEN and agencies, 8 September 2026, fincen.gov
- **Exemption Order Related to TIN Collection and CIP Requirements (OCC, FDIC, NCUA)**, 27 June 2025, fincen.gov; Federal Reserve order, fincen.gov
- **FIN-2026-R001, Exceptive Relief from Requirement to Identify and Verify Beneficial Owners at Each Account Opening**, 13 February 2026, fincen.gov
- **FFIEC BSA/AML Examination Manual, Customer Identification Program**, bsaaml.ffiec.gov
- **FFIEC BSA/AML Examination Manual, Electronic Banking**, bsaaml.ffiec.gov
- **Authentication and Access to Financial Institution Services and Systems**, FFIEC, 11 August 2021 (SR 21-14), federalreserve.gov
- **Interagency Guidance on Third-Party Relationships: Risk Management**, 88 FR 37920 (9 June 2023), federalregister.gov
- **Proposed Third-Party Risk Management Guidance**, 91 FR 58536 (15 September 2026), federalregister.gov
- **Anti-Money Laundering and Countering the Financing of Terrorism Programs** (proposed), FinCEN 91 FR 18704; OCC, FDIC, NCUA 91 FR 18304; Federal Reserve 91 FR 42363, federalregister.gov
- **Prohibition on the Use of Reputation Risk by Regulators**, 91 FR 18279 (10 April 2026), federalregister.gov
- **National Bank Chartering**, 91 FR 9977 (2 March 2026), federalregister.gov
- **Delaying the Effective Date of the Investment Adviser AML/CFT Rule**, 91 FR 36 (2 January 2026), federalregister.gov
- **Personal Financial Data Rights Reconsideration**, 90 FR 40986 (22 August 2025), federalregister.gov
- **FinCEN Assesses $1.2 Billion Penalty against Bank of America**, 13 October 2026, fincen.gov
- **OCC News Release 2026-89**, 13 October 2026, occ.gov