Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in the United States

COUNTRY United States

INDUSTRY Fintech & Digital Payments

LAST UPDATED 16 October 2026

KEY REGULATORS Financial Crimes Enforcement Network · State financial regulators (e.g. New York DFS, California DFPI) · Consumer Financial Protection Bureau

Key takeaways

- A US payment, wallet or remittance app that moves customer money needs two things: a federal registration with the Financial Crimes Enforcement Network (FinCEN, the Treasury's anti-money laundering authority) and a money transmitter licence in each state where its customers are, unless it operates through a licensed partner bank.
- Money transmitters are covered by the federal anti-money laundering rules at any transaction size; there is no small-business floor for moving money.
- Online, the federal rules do not prescribe how to verify a customer. For transfers of $3,000 or more, a remote provider must record the sender's name, address and tax number and how the transfer was paid for, while an in-person provider must also inspect an identity document.
- A state licence follows the customer, not the office: a provider with no physical presence in New York or California still needs a licence there if it serves people located in those states.
- Rules are moving: a proposed rewrite of anti-money laundering programme rules (not yet law) would name remote onboarding as a risk factor firms must assess, and the federal stablecoin law applies from 18 January 2027.

The United States is open to non-bank payment providers, including digital-only ones, but entry is layered. Federal law sets the anti-money laundering, sanctions and consumer-protection baseline, while licensing to move money sits with each state. There is no single national payments licence.

The principal authorities are FinCEN for anti-money laundering rules, the state financial regulators (with New York and California among the most active) for licensing, and the Consumer Financial Protection Bureau (CFPB) and Federal Trade Commission (FTC) for consumer protection and data security.

The biggest obstacle for a new entrant is the state-by-state licensing build, which is why many apps launch on a sponsor bank's charter first. That route shortens time to market but does not shift the bank's legal responsibility, so the bank will impose its own identity and monitoring standards on the app.

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

Regulator	Remit for fintech and payments	Level	Official site
Financial Crimes Enforcement Network (FinCEN)	Money services business registration, anti-money laundering programmes, suspicious activity and recordkeeping rules, civil penalties	Federal	fincen.gov
Internal Revenue Service (IRS)	Examines money services businesses for Bank Secrecy Act compliance under authority delegated by FinCEN	Federal	irs.gov
State financial regulators (for example New York DFS, California DFPI)	Money transmitter licensing, examination and enforcement, mostly managed through the Nationwide Multistate Licensing System (NMLS)	State	dfs.ny.gov, dfpi.ca.gov
Consumer Financial Protection Bureau (CFPB)	Electronic Fund Transfer Act and Regulation E, enforcement of federal consumer financial law against non-banks	Federal	consumerfinance.gov
Federal Trade Commission (FTC)	Gramm-Leach-Bliley Safeguards Rule for non-bank financial institutions, including breach reporting	Federal	ftc.gov

Office of Foreign Assets Control (OFAC)	Economic sanctions that apply to every US person, including payment providers	Federal	ofac.treasury.gov
OCC, Federal Reserve Board, FDIC	Supervise sponsor banks in bank-fintech partnerships; payment stablecoin issuer licensing under the GENIUS Act	Federal	occ.gov, federalreserve.gov, fdic.gov

The Conference of State Bank Supervisors (CSBS) coordinates state regulators and publishes model legislation, but it is not itself a regulator. State attorneys general and state privacy regulators also act against payment firms; their rules are summarised only where they bear on onboarding.

2 Licensing and authorisation

Federal: register with FinCEN

FinCEN treats a money services business (MSB) as a financial institution. A money transmitter is an MSB regardless of the amount of money it transmits, while currency dealers, cheque cashers and issuers or sellers of money orders, travellers' cheques or stored value are MSBs only above an activity threshold of more than $1,000 per person per day, applied separately to each activity (FinCEN, MSB definition and registration). Banks and firms registered with and regulated by the SEC or CFTC are excluded.

Each MSB must register on FinCEN Form 107 within 180 days after it is established, renew every two calendar years, and re-register after a change of control, a transfer of more than 10 percent of voting power or equity, or an increase of more than 50 percent in its agents. It must keep a list of its agents, and a foreign-located MSB doing business in the United States must appoint a US agent for service of process (31 CFR 1022.380). Registration is not a licence: FinCEN does not approve business models.

State: a licence where the customer is

Licensing to move money is state law, state by state. New York requires a licence under Article 13-B of the Banking Law and manages applications through NMLS (NY DFS, Money Transmitters). The Department's industry letter of 31 March 2011 concluded that transmitters doing business with people located in New York need a licence even with no office or agent in the state. California's Money Transmission Act defines "in this state" to include transactions with, to or from persons located in California, and the DFPI has applied

it to out-of-state providers (DFPI opinion, Money transmission in this state). These two states are illustrative, not a survey.

The CSBS Money Transmission Modernization Act is a model law that sets common net worth, surety bond and permissible investment standards. It binds only where a state has enacted it, in full or in part, so firms still need to check each state's own statute.

Operating without authorisation

Failure to register carries a civil penalty for each day the violation continues, and operating an unregistered or unlicensed money transmitting business is a federal crime under 18 U.S.C. 1960, punishable by up to five years' imprisonment (FinCEN, MSB registration penalties).

3 AML, KYC and customer due diligence

MSBs are obliged entities under the Bank Secrecy Act. Each must keep a written anti-money laundering programme, commensurate with the risks of its location, size and services, that includes policies and controls for verifying customer identification, filing reports and keeping records; a designated compliance person; training; and an independent review (31 CFR 1022.210). An agent and its principal may agree who drafts the controls, but each remains solely responsible for implementing them.

Unlike banks, MSBs have no standalone customer identification programme rule, and they are not among the "covered financial institutions" whose programme rules carry the customer due diligence and beneficial ownership requirements; FinCEN's April 2026 proposal lists those as banks, broker-dealers, mutual funds, futures firms and credit card system operators (91 FR 18704). Identity obligations for MSBs come instead from the programme rule and from transaction-level rules.

Obligation	Threshold or trigger	Source
Suspicious activity report (SAR)	$2,000 or more, filed within 30 calendar days of detection; $5,000 for issuers reviewing money order or travellers' cheque clearance records	31 CFR 1022.320
Funds transfer records and Travel Rule data	$3,000 or more; name, address and other data must travel with the order	31 CFR 1010.410(e)-(f)

Cash purchases of money orders and similar instruments	$3,000 to $10,000 in currency; identity verified by document	31 CFR 1010.415
Prepaid access	Name, date of birth, address and ID number for prepaid programme users; sellers also above $10,000 in a day	31 CFR 1022.210(d)(1)(iv)
Currency transaction reports	Cash transactions, as cross-referenced to the general rule	31 CFR 1022.311
Record retention	Five years	31 CFR 1010.430(d)

SARs and any information that would reveal them are confidential and may not be disclosed to the customer. Geographic targeting orders can add temporary, local thresholds; the order covering MSBs along the southwest border requires reports and identity verification for currency transactions of $1,000 to $10,000 until 1 March 2027 `In force, not applied where a court has enjoined it` (FinCEN, 4 September 2026).

4 Identity verification and onboarding

Federal rules for MSBs do not list accepted documents for account opening or prescribe biometric or liveness checks. The programme rule requires reasonably designed procedures to verify customer identification, so the method is a risk-based choice that examiners and partner banks will test. The concrete federal identity elements appear at transaction level:

In-person transmittals

For a $3,000 order from someone who is not an established customer, verify identity before accepting it by examining a document, preferably with name, address and photograph, and record the document type and number plus a taxpayer identification number (TIN) or, if none, an alien or passport number (1010.410(e)(2)(i), (e)(5)).

Remote transmittals

For the same order not made in person, record the name, address and TIN (or alien or passport number) and a copy or record of the method of payment, such as the card or cheque used (1010.410(e)(2)(ii)).

Synthetic identities, built by combining a real Social Security number (SSN) with invented details, are a known weakness of non-documentary checks. The Social Security Administration's electronic Consent Based SSN Verification service lets permitted financial institutions and their service providers confirm whether a name, date of birth and SSN match its records. It needs the person's written consent, which may be an electronic signature, and returns only "yes" or "no"; it does not verify identity on its own (SSA, eCBSV).

Reliance is limited. A sponsor bank remains responsible for compliance with financial crimes laws for activities performed through a fintech partner, and an MSB's agent agreement does not transfer the principal's obligations.

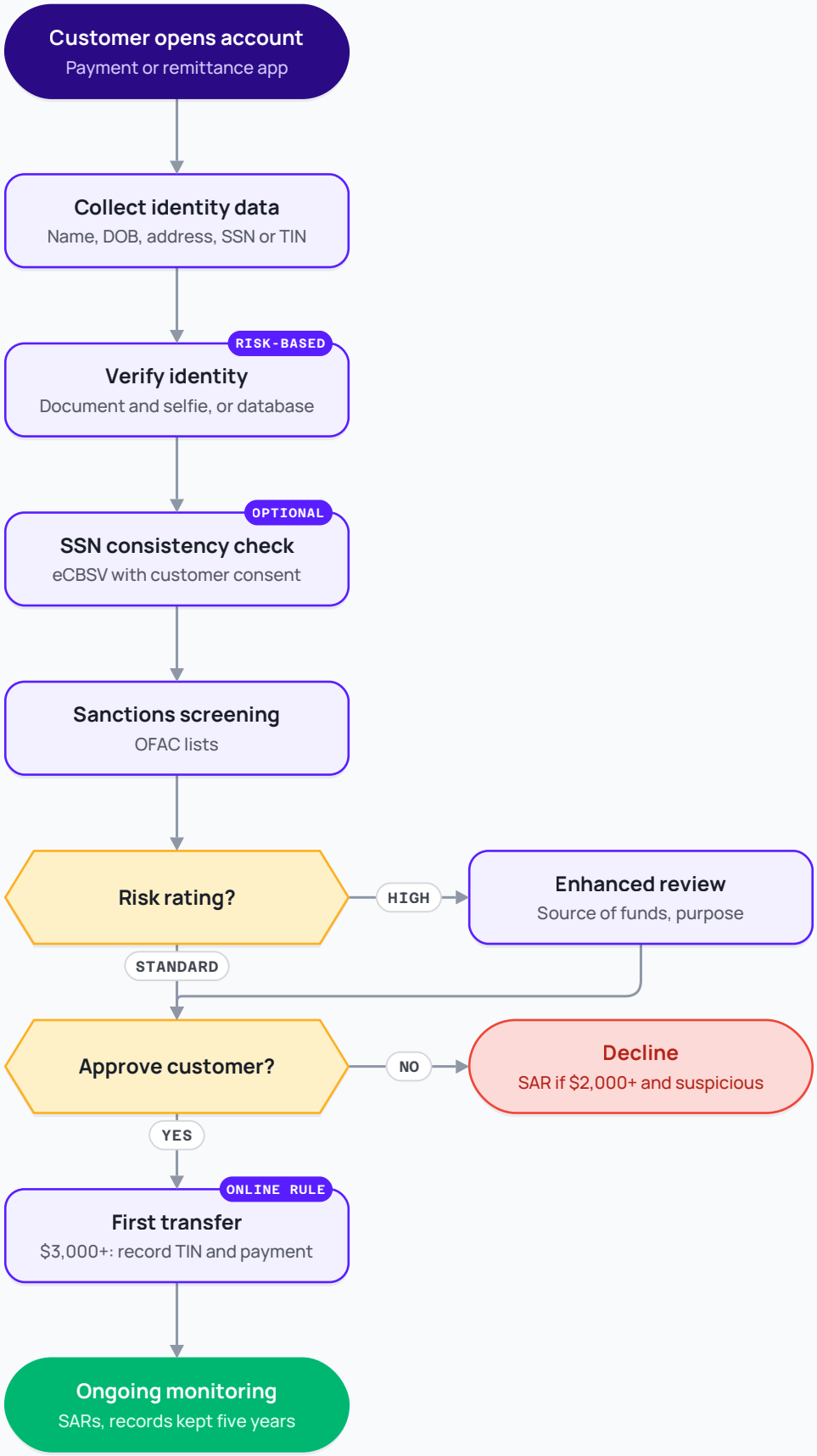


Figure 1. Remote customer onboarding for a US payment or remittance app (illustrative).

5 Digital channels: what's different

Bottom line: the federal anti-money laundering rules are largely channel-neutral, but going online widens the state licensing footprint to every state where customers are located, and replaces the federal document check for larger transfers with a data-and-payment-trail record.

Requirement	In person / agent location	Online / remote	Difference
Where a state licence is needed	States where the provider or its agents serve customers	Every state where customers are located, even with no office	Differs
FinCEN registration	Required at any volume	Required at any volume	Same
Identity on $3,000+ transmittal (new customer)	Examine ID document before accepting	Record name, address, TIN and payment method	Differs
Paying out to a non-customer recipient	Verify identity of the person collecting	Keep copy of the payment instrument and recipient details	Differs
Anti-money laundering programme	Written, risk-based	Written, risk-based	Same
Suspicious activity reporting	$2,000, 30 days	$2,000, 30 days	Same
Unauthorised transfer liability (Regulation E)	Tiered consumer liability	Tiered consumer liability	Same
Breach reporting to the FTC	500 or more consumers, 30 days	500 or more consumers, 30 days	Same

Licensing follows the customer

New York's 2011 position and California's definition of "in this state" both turn on where the customer is located, not where the server or office sits. An app available nationwide therefore faces the full multistate licensing build from day one unless it operates under a bank's charter or as a bank's agent.

No federal remote-verification standard

Federal MSB rules neither require nor prohibit document-and-selfie checks, database verification or biometrics. For larger remote transmittals the rule instead requires a TIN and a record of how the transfer was funded (31 CFR 1010.410(e)(2)(ii)). Sponsor banks and state examiners typically expect more, so the practical standard is set by the risk assessment and the partner contract.

Remote onboarding as a named risk factor

FinCEN's proposed programme rule would require every MSB to run risk assessment processes covering its "distribution channels", which FinCEN defines to include remote or other non-face-to-face account opening, and it lists IP addresses, device logins and geolocation as information firms may use `Proposed, comments closed 9 Jun 2026` (91 FR 18704).

6 Data protection and biometrics

There is no single federal data protection statute or authority in the United States. For non-bank payment providers the main federal rule is the FTC's Safeguards Rule under the Gramm-Leach-Bliley Act, which requires an information security programme for customer information. Since 13 May 2024 it also requires notice to the FTC, through a form on its website, of any unauthorised acquisition of unencrypted customer information involving at least 500 consumers, as soon as possible and no later than 30 days after discovery (88 FR 77499). Unauthorised access is presumed to be acquisition unless the firm has reliable evidence to the contrary, and the FTC may publish the reports.

Selfie, face-match and liveness data collected at onboarding is not addressed by federal MSB rules, but several states regulate biometric identifiers directly, and state consumer privacy laws add notice, retention and deletion duties. Identity records that Bank Secrecy Act rules require must still be kept for five years, so retention schedules need to separate mandatory records from optional biometric data.

7 Sector-specific obligations

Bank partnerships and banking-as-a-service

The OCC, Federal Reserve and FDIC's 2023 interagency guidance states that a bank's use of third parties, including fintech companies, does not diminish its responsibility to comply

with laws addressing financial crimes and consumer protection as if it performed the activity itself (88 FR 37920). The guidance expects due diligence on the fintech's licences, ownership and OFAC exposure, contract rights to audit and require remediation, and regulator access to the fintech's records. It is supervisory guidance without the force of law, but sponsor banks write it into their programme agreements.

Consumer protection for transfers

Regulation E caps a consumer's liability for unauthorised electronic fund transfers at the lesser of $50 or the amount taken if a lost or stolen access device is reported within two business days, and at $500 if later, with further exposure if a statement error is not reported within 60 days (12 CFR 1005.6). Weak onboarding and account-takeover controls therefore become direct losses. The CFPB rule that would have placed the largest non-bank payment apps under its supervision was disapproved by Congress `Disapproved, no force or effect` (Pub. L. 119-11, 9 May 2025); the CFPB's enforcement authority over non-banks is unaffected.

Payment stablecoins

Under the GENIUS Act, only permitted issuers may issue payment stablecoins in the United States once the Act takes effect on 18 January 2027, and from 18 July 2028 digital asset service providers may not offer or sell to US persons a payment stablecoin from an unpermitted issuer `Adopted, effective 18 Jan 2027` (91 FR 61688). FinCEN has proposed carving permitted issuers out of the MSB definition and giving them their own programme rules `Proposed` (FinCEN, 10 April 2026). Wallet and payment apps that distribute stablecoins should map which issuers they support before the 2028 date.

8 Risk indicators and red flags

FinCEN's January 2024 analysis of identity-related suspicious activity groups identity abuse into impersonation, compromise of credentials and circumvention of verification (FinCEN Financial Trend Analysis). Indicators relevant to payment apps include:

PAYMENT AND REMITTANCE TYPOLOGIES

- **Synthetic identity**: an SSN that does not match the name and date of birth, or a thin file with no history.
- **Impersonation at onboarding**: document images, selfies or device data reused across several accounts.
- **Account takeover**: login from a new device followed quickly by changed contact details and a large transfer out.
- **Threshold avoidance**: repeated transfers just under $3,000, or cash just under local order thresholds.
- **Funnel accounts**: many unrelated senders paying one recipient who moves funds abroad.
- **Agent anomalies**: an agent whose volume jumps or whose customers share identifiers.
- **Sanctioned networks**: payments touching entities named in FinCEN special measures or OFAC designations.

9 Enforcement and penalties

FinCEN's civil penalties are set per violation and, for continuing violations, per day. Amounts below apply to penalties assessed on or after 17 January 2025 (31 CFR 1010.821):

Violation	Statutory amount	Adjusted maximum
Wilful Bank Secrecy Act violation (31 U.S.C. 5321(a)(1))	$25,000 to $100,000	$71,545 to $286,184
Negligent violation	$500	$1,430
Pattern of negligent activity	$50,000	$111,308
Failure to register as a money transmitting business (per day)	$5,000	$10,556
Funds transfer recordkeeping violations	$10,000	$26,262

In December 2025 FinCEN assessed $3.5 million against Paxful, an online peer-to-peer platform, which admitted failing to register as an MSB, to maintain an effective programme and to file SARs (FinCEN, 9 December 2025). In February 2025 it imposed $37 million on Brink's Global Services USA for operating as an unregistered money transmitter without an adequate programme (FinCEN, Brink's). State regulators add their own licensing penalties.

10 Recent changes and what to watch

- **6 October 2026** `Proposal withdrawn` FinCEN withdrew its 2020 proposal on unhosted crypto wallet reporting for banks and MSBs; no new wallet reporting duty applies.
- **5 October 2026** `Proposed` FinCEN proposed prohibiting transmittals of funds involving the A7 network's sub-agents; remittance providers should prepare screening.
- **30 September 2026** `Adopted, effective 18 Jan 2027` Treasury's interim rule on state stablecoin certifications confirms the GENIUS Act start date.
- **4 September 2026** `In force, partly enjoined` Southwest border geographic targeting order for MSBs runs to 1 March 2027.
- **10 April 2026** `Proposed, comments closed 9 Jun 2026` FinCEN's programme rule rewrite would require documented risk assessments, including of remote channels, and a US-based compliance officer.
- **9 May 2025** `Disapproved` CFPB larger-participant supervision of payment apps nullified by Pub. L. 119-11.

11 What this means for identity verification

Collect SSN or another TIN at onboarding rather than at the first large transfer: remote transmittals of $3,000 or more need it, and collecting it once avoids friction later. Because federal rules set no remote method, document the chosen method (document and selfie, database or both) in the risk assessment and align it with the sponsor bank's standard. Consent-based SSN verification is a useful synthetic-identity control and needs a consent step in the flow. Keep the payment-method record for remote transfers, store required identity records for five years, and keep biometric data on a separate, state-law-driven retention schedule. Re-verify on account recovery, device change and payout-detail changes, the moments account takeover exploits. Build licensing logic by customer location, since the state of residence determines the licence and the state's examiner.

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 KYC onboarding with ID document capture and verification (including NFC), face match and biometric liveness, configurable to each sponsor bank's standard.
- Collection of SSN or TIN, address and contact data at sign-up, with phone and email verification, so records for $3,000+ transfers are ready before the first payment.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and on an ongoing basis, plus transaction monitoring to support SAR decisions.
- KYB and beneficial owner verification for business customers, merchants and agents.
- A no-code workflow builder to route customers by risk and state, with an audit trail for examiners and partner banks.

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 Part 1022, Rules for Money Services Businesses** (1022.210, 1022.311, 1022.320, 1022.380), eCFR, current as of 9 October 2026, ecfr.gov
- **31 CFR Part 1010 Subpart D, Records Required To Be Maintained** (1010.410, 1010.415, 1010.430), eCFR, current as of 13 October 2026, ecfr.gov
- **31 CFR 1010.821, Penalty adjustment and table**, eCFR, ecfr.gov
- **Money Services Business (MSB) Registration and definition**, FinCEN, fincen.gov

- **Anti-Money Laundering and Countering the Financing of Terrorism Programs**, proposed rule, 91 FR 18704, 10 April 2026, federalregister.gov
- **Permitted Payment Stablecoin Issuer AML/CFT and Sanctions Compliance Program Requirements**, proposed rule, 10 April 2026, federalregister.gov
- **Forms and Procedures for Review of State Certifications by the Stablecoin Certification Review Committee**, interim final rule, 91 FR 61688, 30 September 2026, federalregister.gov
- **Geographic Targeting Order on Certain Money Services Businesses Along the Southwest Border**, FinCEN, 4 September 2026, federalregister.gov
- **Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets; Withdrawal**, FinCEN, 6 October 2026, federalregister.gov
- **Recently published documents (including the A7 network special measure proposal, 5 October 2026)**, Federal Register, FinCEN agency page, federalregister.gov
- **Standards for Safeguarding Customer Information**, final rule, 88 FR 77499, 13 November 2023 (16 CFR 314.2(m), 314.4(j)), federalregister.gov
- **12 CFR 1005.6, Liability of consumer for unauthorized transfers** (Regulation E), eCFR, ecfr.gov
- **Public Law 119-11**, joint resolution disapproving the CFPB rule on larger participants in general-use digital consumer payment applications, 9 May 2025, congress.gov
- **Interagency Guidance on Third-Party Relationships: Risk Management**, 88 FR 37920, 9 June 2023, govinfo.gov
- **Money Transmitters**, New York State Department of Financial Services, dfs.ny.gov; **Industry letter: Money Transmitters with No Physical Presence in New York**, 31 March 2011, dfs.ny.gov
- **Money Transmitters** and **Opinion: Money transmission in this state**, California DFPI, dfpi.ca.gov, dfpi.ca.gov
- **CSBS Money Transmission Modernization Act** (model law description), CSBS, csbs.org
- **Social Security Begins New Electronic Social Security Number Verification Service**, SSA press release, 29 October 2020, ssa.gov
- **Identity-Related Suspicious Activity: 2021 Threats and Trends**, FinCEN Financial Trend Analysis, January 2024, fincen.gov
- **FinCEN Assesses $3.5 Million Penalty Against Paxful**, 9 December 2025, fincen.gov; **FinCEN Announces $37,000,000 Civil Money Penalty Against Brink's Global Services USA**, 2025, fincen.gov