ProSight™

Quarterly Regulatory Update

Materials April 1, 2026, through June 30, 2026

Presented by: Melissa Blaser

ProSight Compliance Peer Discussions

ProSight™

About

- Follow-up to our Quarterly Regulatory Updates (QRU) webinars
- Open forum for Compliance Professionals led by ProSight's in-house compliance experts
- In each session you can:
  - Engage in strategic discussion on industry challenges
  - Exchange ideas and insights with peers
  - Expand your network of industry colleagues
  - And more!

Schedule

Held two weeks after each QRU webinar

Next session: August 6 | 1:00 – 1:45 PM CST

Register

Email contentandproduction@prosightfa.org with “**Compliance**” in the subject line

Watch for an invitation in your inbox

Suggest Discussion Topics

Email contentandproduction@prosightfa.org with “**Topic Suggestion**” in the subject line

Agenda to follow

Presenter

Melissa Blaser, Partner

CPA, CRCM, CAMS, CFSA, CFIRS

815.484.5652

mblaser@wipfli.com

Wipfli Articles

- How to maintain stablecoin compliance under the GENUIS Act – Wipfli
- Financial services complaints management: A short guide | Wipfli
- Regulation B amendments impact small business lending data collection rules – Wipfli
- P2P payments in 2026: Trends, risks and compliance expectations | Wipfli
- Streamlining BOI verification with FinCEN exceptive relief | Wipfli
- State Do Not Call lists: What you need to know
- Updated California data privacy laws expose fintech companies to costly compliance risks
- What companies get wrong about TCPA and B2B marketing

Wipfli Articles

- What businesses get wrong about TCPA lawsuits and settlements
- New executive order opens the door for fintechs
- Small business lending data collection rules are changing
- TCPA compliance checklist: Measure your compliance posture
- TCPA revocation of consent rules are reshaping litigation risk
- The FCC one-to-one consent rule was overturned. TCPA consent requirements still matter.
- Financial services complaint management: How to handle compliance for customer or client complaints

BSA

FinCENs Proposal AML and CFT Programs (04-10-26)

ProSight™

- **SUMMARY:** Pursuant to the Department of the Treasury (Treasury) and FinCEN’s efforts to modernize the Bank Secrecy Act (BSA) and to implement provisions of the Anti-Money Laundering Act of 2020 (AML Act), FinCEN is proposing a rule to fundamentally reform the requirements for financial institutions’ anti-money laundering and countering the financing of terrorism (AML/CFT) programs. Among other changes, this proposed rule aims to ensure that financial institutions establish and maintain effective AML/CFT programs that better achieve the purposes of the BSA and lead to more effective outcomes for financial institutions as well as law enforcement and national security agencies.
- FinCEN is also proposing measures to modernize and reform Federal supervision of AML/CFT programs by enhancing FinCEN’s role in AML/CFT supervision and enforcement in coordination with Federal banking regulators. In addition, FinCEN is proposing regulatory amendments to promote clarity and consistency across FinCEN’s program rules for different types of financial institutions.
- **DATES:** Comments must be received by June 9, 2026.

FinCENs Proposal AML and CFT Programs (04-10-26)

- (a) In general. A bank has an effective AML/CFT program and complies with the requirements of 31 U.S.C. 5318(h)(1) and this section if the bank:
- (1) Establishes an AML/CFT program in accordance with paragraph (b) of this section; and
- (2) Maintains an AML/CFT program by implementing the AML/CFT program in accordance with paragraph (c) of this section.
- (b) Program establishment. A bank establishes an AML/CFT program in accordance with this paragraph (b) if the bank:
- (1) Establishes a risk-based set of internal policies, procedures, and controls that is reasonably designed to ensure compliance with the Bank Secrecy Act and this chapter and to:
- (i) Identify, assess, and document the bank's money laundering, terrorist financing, and other illicit finance activity risks through risk assessment processes that:
- (A) Evaluate the money laundering, terrorist financing, and other illicit finance activity risks of the bank's business activities, including its products, services, distribution channels, customers, and geographic locations;
- (B) Review and, as appropriate, incorporate the AML/CFT priorities; and
- (C) Are updated promptly upon any change that the bank knows or has reason to know significantly changes the bank's money laundering, terrorist financing, and other illicit finance activity risks;

FinCENs Proposal AML and CFT Programs (04-10-26)

- (ii) Mitigate the bank's money laundering, terrorist financing, and other illicit finance activity risks consistent with the risk assessment processes required under paragraph (b)(1)(i) of this section, including by directing more attention and resources toward higher-risk customers and activities, consistent with the risk profile of the bank, rather than toward lower-risk customers and activities; and
- (iii) Conduct ongoing customer due diligence, including to:
- (A) Understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- (B) Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information (including information regarding the beneficial owners of legal entity customers, as defined in § 1010.230 of this chapter);
- (2) Establishes independent AML/CFT program testing to be conducted by bank personnel or by an outside party;
- (3) Designates an individual, who is:
- (i) Located in the United States;
- (ii) Accessible to, and subject to oversight and supervision by, FinCEN and its designee; and
- (iii) Responsible for establishing and implementing the AML/CFT program and coordinating and monitoring day to-day compliance; and
- (4) Establishes an ongoing employee training program.

FinCENs Proposal AML and CFT Programs (04-10-26)

- (c) Program implementation. A bank implements an AML/CFT program in accordance with this paragraph (c) if the bank implements, in all material respects, the AML/CFT program required under paragraph (b) of this section.
- <u>(d) Written AML/CFT program and approval. A bank's AML/CFT program must be written, and it must be approved by the bank's board of directors, an equivalent governing body within the bank, or appropriate senior management. The bank must make a copy of its AML/CFT program available to FinCEN or its designee upon request.</u>

FinCENs Proposal AML and CFT Programs (04-10-26)

- (1) In general. A bank required to have an AML/CFT program under 31 U.S.C. 5318(h), 12 U.S.C. 1818(s), or 12 U.S.C. 1786(q)(1) must implement a written Customer Identification Program (CIP) appropriate for the bank's size and type of business that, at a minimum, includes each of the requirements of paragraphs (a)(1) through (5) of this section. The CIP must be a part of the AML/CFT program.
- <u>(6) * * *</u>
- <u>(iii) The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML/CFT program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.</u>

FinCENs Proposal AML and CFT Programs (04-10-26)

- (b) FinCEN enforcement and supervision policy—(1) In general. Except with respect to a significant or systemic failure to implement the AML/CFT program in accordance with § 1020.210(c), a bank that has established an AML/CFT program in accordance with § 1020.210(b) will not be subject to:
- (i) An AML/CFT enforcement action related to the requirements of 31 U.S.C. 5318(h)(1) § 1020.210 by FinCEN; or
- (ii) A significant AML/CFT supervisory action related to the requirements of 31 U.S.C. 5318(h)(1) or § 1020.210 by FinCEN or by a Federal Financial Institutions Regulatory Agency when acting pursuant to authority delegated under this chapter.
- (2) Notice requirement. To provide the Director, FinCEN an opportunity to provide a view under paragraph (c)(1) of this section, a Federal Financial Institutions Regulatory Agency when acting pursuant to authority delegated under this chapter will:
- (i) Send written notice to the Director, FinCEN of its intent to take that action at least 30 days before taking the action (unless a shorter period of time is necessary, in the sole discretion of the Federal Financial Institutions Regulatory Agency, to remedy, prevent, or respond to an unsafe or unsound practice or condition), accompanied by the relevant AML/CFT information underlying the proposed action, including the relevant portions of the draft report or enforcement action, the relevant examination workpapers supporting the proposed action, and the relevant AML/CFT information submitted by the bank to the Federal Financial Institutions Regulatory Agency, other than information over which the bank may claim privilege under Federal or State law; and

FinCENs Proposal AML and CFT Programs (04-10-26)

- (ii) Respond to the extent reasonably practicable to requests for additional information from the Director, FinCEN regarding the proposed action.
- (d) FinCEN considerations. In determining whether to take an AML/CFT enforcement action or significant AML/CFT supervisory action, or when reviewing a proposed action by a Federal Financial Institutions Regulatory Agency the Director, FinCEN shall consider:
- (1) The factors under 31 U.S.C. 5318(h)(2)(B), as applicable to actions concerning the AML/CFT program requirements under § 1020.210;
- (2) The extent (if any) to which the bank, where appropriate in light of its size, complexity, and risk profile, has advanced the AML/CFT priorities by providing highly useful information to law enforcement authorities or national security officials, conducting proactive analytics, or performing other innovative activities producing demonstrable outputs evincing the effectiveness of the bank's AML/CFT program (including effective use of artificial intelligence, federated learning, and other advanced monitoring tools); and
- (3) Any other factor the Director, FinCEN deems appropriate, including the bank's size, complexity, and risk profile, and, as relevant, where the bank's low-risk customers or limited business activities naturally limits the extent to which the bank can meaningfully contribute to AML/CFT priorities.

Agencies AML and CFT Proposal (04-10-26)

- The Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) (collectively, ‘‘the Agencies’’ or ‘‘Agency’’ when referencing the singular) are inviting comment on a proposed rule that would require banks to establish and maintain effective anti money laundering and countering the financing of terrorism (AML/CFT) programs reasonably designed to identify, assess, and mitigate risks of illicit finance. The amendments are intended to align with changes that are being concurrently proposed by the Financial Crimes Enforcement Network (FinCEN) to implement provisions of the Anti-Money Laundering Act of 2020 (AML Act).

Agencies AML and CFT Proposal (04-10-26)

ProSight™

- (b) AML/CFT program in general. Each national bank or Federal savings association must establish and maintain an effective AML/CFT program. A national bank or Federal savings association complies with this requirement if it:
- (1) Establishes an AML/CFT program in accordance with paragraph (c) of this section; and
- (2) Maintains an AML/CFT program by implementing the AML/CFT program in accordance with paragraph (d) of this section.
- (c) AML/CFT program establishment. A national bank or Federal savings association establishes an AML/CFT program in accordance with this paragraph if it:
- (1) Establishes a risk-based set of internal policies, procedures, and controls that is reasonably designed to ensure compliance with the Bank Secrecy Act and the implementing regulations at 31 CFR chapter X and to:
- (i) Identify, assess, and document the national bank's or Federal savings association's money laundering, terrorist financing, and other illicit finance activity risks through risk assessment processes that:
- (A) Evaluate the money laundering, terrorist financing, and other illicit finance activity risks of the national bank's or Federal savings association's business activities, including its products, services, distribution channels, customers, and geographic locations;

Agencies AML and CFT Proposal (04-10-26)

ProSight™

- (B) Review and, as appropriate, incorporate the AML/CFT priorities as that term is defined in 31 CFR 1010.100; and
- (C) Are updated promptly upon any change that the national bank or Federal savings association knows or has reason to know significantly changes the national bank's or Federal savings association's money laundering, terrorist financing, and other illicit finance activity risks;
- (ii) Mitigate the national bank's or Federal savings association's money laundering, terrorist financing, and other illicit finance activity risks consistent with the risk assessment processes required under paragraph (c)(1)(i) of this section, including by directing more attention and resources toward higher-risk customers and activities, consistent with the risk profile of the national bank or Federal savings association, rather than toward lower-risk customers and activities; and
- (iii) Conduct ongoing customer due diligence, including to:
- (A) Understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- (B) Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information (including information regarding the beneficial owners of legal entity customers, as defined in 31 CFR 1010.230);

Agencies AML and CFT Proposal (04-10-26)

- (2) Establishes independent AML/CFT program testing to be conducted by bank or savings-association personnel or by an outside party;
- (3) Designates an individual, who is (i) located in the United States; (ii) accessible to, and subject to oversight and supervision by, FinCEN and the OCC; and (iii) responsible for establishing and implementing the AML/CFT program and coordinating and monitoring day-to-day compliance; and
- (4) Establishes an ongoing employee training program.
- (d) AML/CFT program implementation. A national bank or Federal savings association implements an AML/CFT program in accordance with this paragraph if the national bank or Federal savings association implements, in all material respects, the AML/CFT program required under paragraph (c) of this section.
- (e) Written AML/CFT program and approval. A national bank's or Federal savings association's AML/CFT program must be written, and it must be approved by the national bank's or Federal savings association's board of directors, an equivalent governing body within the national bank or Federal savings association, or appropriate senior management within the national bank or Federal savings association.
- (f) Customer identification program. Each national bank or Federal savings association shall implement a customer identification program in accordance with 31 CFR 1020.220.

Agencies AML and CFT Proposal (04-10-26)

- (g) Enforcement and supervision policy.
- (1) In general. Except with respect to a significant or systemic failure to implement the AML/CFT program in accordance with paragraph (d) of this section, a national bank or Federal savings association that has established an AML/CFT program in accordance with paragraph (c) of this section will not be subject to an AML/CFT enforcement action or to a significant AML/CFT supervisory action related to the requirements of 12 U.S.C. 1818(s), 31 U.S.C. 5318(h)(1), this section, or 31 CFR 1020.210.
- (h) FinCEN consultation.
- (1) Consultation and consideration requirement. Before initiating an AML/CFT enforcement action or a significant AML/CFT supervisory action, the OCC will provide the FinCEN Director an opportunity to review the action and consider any input offered by the FinCEN Director on the action, which may include any view as to the effectiveness of the national bank's or Federal savings association's AML/CFT program.
- (2) Notice requirement. To provide the FinCEN Director an opportunity to provide a view under paragraph (h)(1) of this section, the OCC will:

Agencies AML and CFT Proposal (04-10-26)

- (i) Send written notice to the FinCEN Director of its intent to take that action at least 30 days before taking the action (unless a shorter period of time is necessary, in the sole discretion of the Comptroller of the Currency, to remedy, prevent, or respond to an unsafe or unsound practice or condition), accompanied by the relevant AML/CFT information underlying the proposed action, including the relevant portions of the draft report or enforcement action, the relevant examination workpapers supporting the proposed action, and the relevant AML/CFT information submitted by the national bank or Federal savings association to the OCC, other than information over which the national bank or Federal savings association may claim privilege under Federal or State law; and
- (ii) Respond to the extent reasonably practicable to requests for additional information from the FinCEN Director regarding the proposed action.
- (i) Disclosure of supervisory information to FinCEN.

Agencies AML and CFT Proposal (04-10-26)

- **[OPTION 1 FOR PARAGRAPH (i)(1):]**
- (1) Notwithstanding 12 CFR part 4, the OCC permits a national bank or Federal savings associations, on behalf of OCC, to disclose to the FinCEN Director, and permits the FinCEN Director to use, any information relating to an existing or potential AML/CFT enforcement action or significant AML/ CFT supervisory action to which the national bank or Federal savings association has access.
- **[OPTION 2 FOR PARAGRAPH (i)(1):]**
- (1) Notwithstanding 12 CFR part 4, the OCC permits a national bank or Federal savings association, on behalf of the OCC, to disclose to the FinCEN Director, and permits the FinCEN Director to use, any information relating to an existing or potential AML/CFT enforcement action or significant AML/ CFT supervisory action to which the national bank or Federal savings association has access upon the contemporaneous disclosure of such information to the OCC.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) are jointly issuing this proposed rule to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act). Specifically, it implements the GENIUS Act's directive to treat permitted payment stablecoin issuers (PPSIs) as financial institutions for purposes of the Bank Secrecy Act, proposes anti-money laundering obligations for PPSIs, and proposes certain specific obligations required by the GENIUS Act for PPSIs. It also implements the GENIUS Act's directive to require PPSIs to maintain effective sanctions compliance programs.
- As MSBs, stablecoin issuers are currently subject to a range of BSA obligations. MSBs; are required to, for instance: (i) establish written AML programs; (ii) file currency transaction reports (CTRs) and SARs; and (iii) maintain certain records, including those relating to certain transmittals of funds. MSBs are subject to examination for BSA compliance by the Internal Revenue Service (IRS) under a delegation of authority by FinCEN.
- As required by the GENIUS Act, FinCEN is proposing certain obligations that differ in some material respects from current obligations that stablecoin issuers are subject to as MSBs, as well as some PPSI-specific obligations required by the GENIUS Act. However, in many respects, FinCEN expects that the proposed requirements for PPSIs would be comparable to stablecoin issuers' existing requirements as MSBs.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- FinCEN is proposing to amend the definition of "money services business," 31 CFR 1010.100(ff), to add PPSIs to the list of financial institutions that the term "money services business" shall not include. The amendment makes clear that PPSIs are subject to obligations as a PPSI and not as a money services business.
- The GENIUS Act directs that PPSIs be subject to "maintenance of an effective anti-money laundering program, which shall include appropriate risk assessments and designation of an officer to supervise the program." Effective AML/CFT programs safeguard national security and generate significant public benefits by preventing the flow of illicit funds in the financial system and by assisting law enforcement and national security agencies with the identification and prosecution of persons attempting to launder money and undertake other illicit activity through the financial system.
- Under proposed § 1033.210 PPSIs would have an effective AML/CFT program and comply with the requirements of 31 U.S.C. 5318(h)(1) and § 1033.210 if the PPSI: (1) establishes an AML/CFT program in accordance with paragraph (b) of § 1033.210; and (2) maintains an AML/CFT program by implementing the AML/CFT program in accordance with paragraph (c) of § 1033.210. As part of the program, and consistent with the mandate in the GENIUS Act, PPSIs would be required to conduct ongoing customer due diligence

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- A PPSI would be required to establish a risk-based set of internal policies, procedures, and controls that are reasonably designed to ensure compliance with the BSA and 31 CFR chapter X. The risk-based internal policies, procedures, and controls must also be reasonably designed to: (1) identify, assess, and document the PPSI's ML/TF risks through risk assessment processes that evaluate the risks of the PPSI's business activities, review and, as appropriate, incorporate the AML/CFT Priorities, and are updated promptly upon any change that the PPSI knows or has reason to know significant changes in the PPSI's ML/TF risks; (2) mitigate the PPSI's ML/TF risks, consistent with the PPSI's risk assessment processes; and, (3) conduct ongoing customer due diligence.
- The proposed rule would also require a PPSI to establish an ongoing employee training program and independent AML/CFT program testing as part of its AML/CFT program.
- Finally, the proposed rule would require a PPSI to designate an individual responsible for establishing and implementing the AML/CFT program and coordinating and monitoring day-to-day compliance; that individual would be required to be located in the United States and accessible to, and subject to oversight and supervision by, FinCEN and its designee, including the appropriate primary Federal payment stablecoin regulator. That individual also could not have been convicted of a felony offense involving certain kinds of activity, as required by the GENIUS Act.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- FinCEN is proposing in § 1033.210(b)(1)(i) that, as part of a PPSI's risk-based set of internal policies, procedures, and controls, the PPSI establish and maintain risk assessment processes to: (1) evaluate the ML/TF risks of the PPSI's business activities, including products, services, distribution channels, customers, and geographic locations; (2) review and, as appropriate, incorporate the AML/CFT Priorities; and (3) be updated promptly upon any change that the PPSI knows or has reason to know significantly changes the PPSI's ML/TF risks. This provision implements the GENIUS Act's directive that PPSI AML/CFT programs include appropriate risk assessments.
- FinCEN is proposing to require PPSIs to collect beneficial ownership information about legal entity customers, which is critical for a PPSI to effectively carry out its due diligence obligations as provided in the GENIUS Act. This proposed obligation is effectuated through FinCEN's proposed AML/CFT program obligation, its proposed amendment to § 1010.605(e)(1), and its proposed amendment to § 1010.230(b)(2) and (c) Collecting information on legal entity customers helps a financial institution assess and mitigate risk, as well as the ability of law enforcement to identify assets and accounts connected with illicit activity. FinCEN is not contemplating application of CDD to secondary market activity. Accordingly, FinCEN is not extending the collection of beneficial ownership information to secondary market activity.
- The GENIUS Act requires that PPSIs have "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations." The GENIUS Act also requires that PPSIs "issue payment stablecoins only if the issuer has the technological capability to comply, and will comply, with the terms of any lawful order.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- FinCEN proposes applying the CTR reporting provisions to PPSIs through proposed §§ 1033.310 through 1033.315, which would cross reference corresponding provisions in §§ 1010.310 through 1010.315.
- FinCEN recognizes that, presently, stablecoin issuers rarely transact in physical transfers of currency. FinCEN nevertheless considers it prudent to allow for the possibility that this could change, with PPSI activity expanding to encompass retail, brick-and-mortar locations where currency could be used, or even kiosks that resemble automated teller machines (ATMs).
- The GENIUS Act explicitly requires PPSIs to be subject to BSA requirements relating to “monitoring and reporting of any suspicious transaction relevant to a possible violation of law or regulation.”
- Proposed § 1033.320(c) would provide that PPSIs must maintain copies of filed SARs and the underlying related documentation for a period of five years from the date of filing. Supporting documentation would need to be made available to FinCEN, any Federal, State, or local law enforcement agency; or any Federal regulatory authority that examines the PPSI for compliance with the BSA under the proposed rule, upon request of that agency or authority.
- Consistent with BSA provisions regarding SAR confidentiality proposed § 1033.320(d) would provide that a SAR and any information that would reveal the existence of a SAR are confidential and shall not be disclosed except as authorized in § 1033.320(d)(1)(ii).

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

ProSight™

- The proposal would require PPSIs to comply with the recordkeeping obligations outlined in § 1010.410(a) through (c). The recordkeeping obligations would require PPSIs to create and retain certain records for extensions of credit in excess of $10,000 and certain records of cross-border transfers of currency, monetary instruments, funds, checks, investment securities, and credit worth more than $10,000. Section 1010.410(d) would require also a PPSI to maintain records related to any order issued under § 1010.370(a) for up to five years.
- The proposal would also require PPSIs to comply with the Recordkeeping Rule and Travel Rule, which are complementary obligations codified in §§ 1010.410(e) and 1010.410(f), respectfully. The Recordkeeping Rule requires financial institutions to collect and retain records for funds transfers and transmittals of funds in amounts of $3,000 or more.
- FinCEN is not proposing to substantively change the Recordkeeping Rule and Travel Rule requirements via this rulemaking other than clearly imposing those requirements on PPSIs, consistent with the GENIUS Act, and ensuring it is clear that transmittal orders involving payment stablecoins are covered by the Recordkeeping Rule and Travel Rule.
- The GENIUS Act generally directs that PPSIs be treated as financial institutions under the BSA and be subject to “all laws” relating to “prevention of money laundering. Although the GENIUS Act does not explicitly direct FinCEN to apply its provisions relating to information sharing to PPSIs, information sharing authorities are established components of the BSA, which, among other purposes, seek to “prevent laundering of money.”

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- Proposed § 1033.540 would cross-reference § 1010.540 and permit PPSIs to, upon providing notice to FinCEN, transmit, receive, or otherwise share information with other financial institutions or associations of financial institutions in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.
- The GENIUS Act mandated that a PPSI maintain “appropriate enhanced due diligence, and the BSA directs that financial institutions establish appropriate enhanced due diligence for correspondent accounts and private banking accounts.
- As financial institutions, FinCEN is proposing that PPSIs be required to comply with special measures issued pursuant to sections 311, 9714(a), and 2313a to maintain the options available under these sections to protect the U.S. financial system from certain illicit finance threats.
- Based on that experience, OFAC is now proposing requiring PPSIs adopt a sanctions compliance program including the five key elements in line with the 2019 Compliance Framework: (1) Senior Management and Organizational Commitment; (2) Risk Assessment; (3) Internal Controls; (4) Testing and Auditing; and (5) Training.
- Specifically, by mandating the five elements as a minimum for an effective sanctions compliance program, the proposed rule intentionally sets a necessary floor for an effective sanctions compliance program while leaving space for PPSIs to take additional or refined compliance measures that account for the specific circumstances of individual PPSIs.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- Proposed § 502.201(b)(1) would require a PPSI's senior management to review and approve a PPSI's sanctions compliance program and to support the sanctions compliance program's effective implementation, including by ensuring the sanctions compliance program, at a minimum: (i) applies to all payment stablecoin-related activity; (ii) has sufficient resources, including necessary investments in human capital, expertise, and information technology, to carry out the requirement that PPSIs conduct risk assessments, maintain internal controls, conduct testing and auditing, and maintain a risk-based sanctions compliance training program, as described in the proposed § 502.201(b)(2) through (b)(5) (see sections VII.B.2 through VII.B.5 below); (iii) is fully integrated into the PPSI's ongoing stablecoin-related operations; (iv) routinely provides risk updates, including test results, to senior management and other appropriate personnel within the PPSI; and (v) provides sufficient authority and autonomy to the compliance function to manage effectively U.S. sanctions risk for the entire PPSI.
- Third, senior management would be required to ensure the sanctions compliance program is fully integrated into a PPSI's ongoing stablecoin-related operations.
- Fourth, senior management would be required to ensure senior management, and other appropriate personnel, routinely receive risk updates, including test results, from the sanctions compliance program.
- Finally, while routine updates to senior management are essential, under the proposed rule, senior management would also be required to ensure that the sanctions compliance program has sufficient authority and autonomy to function and conduct timely and effective operations. The proposed rule would require that a PPSI's sanctions compliance program be empowered to work independently to take appropriate actions to address and mitigate sanctions risks for the entire organization, which is critical to the integrity of the PPSI's compliance functions.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- Proposed § 502.201(b)(2) would require a PPSI conduct sanctions-related risk assessments by: (i) conducting holistic assessments of U.S. sanctions risks at appropriate intervals; (ii) using the risk assessments to inform the PPSI's operation of its sanctions compliance program, including revising internal controls and training as appropriate; and (iii) revising risk assessments as appropriate to account for any identified U.S. sanctions violations or deficiencies, new products, services, mergers, or acquisitions, and any other factors that may affect a PPSI's risk profile.
- Proposed § 502.201(b)(3) would require a PPSI to establish and maintain a system of risk-based internal controls—including technical capabilities and written policies and procedures—applicable to all payment stablecoin-related activity, whether on the primary or secondary market, that identifies, blocks, and/or rejects transactions that may violate or would violate U.S. sanctions and retains relevant records in accordance with OFAC regulations. OFAC assesses that a dynamic internal controls system that adapts to new regulatory and risk-related developments is critical to fulfilling key obligations imposed under the GENIUS Act.
- Second, the written policies and procedures requirement of proposed § 502.201(b)(3) prescribes that the risk-based internal controls established by the PPSI are documented in writing and are clearly communicated to all relevant personnel and stakeholders (e.g., clients, business partners, counterparties). OFAC is proposing written policies and procedures because they ensure that compliance measures (like screening the SDN List) are applied consistently across an entire organization, preventing fragmented, decentralized, or ad-hoc practices that can lead to sanctions violations.

FinCEN and OFAC Proposal GENIUS Act (04-10-26)

- Proposed § 502.201(b)(4) would require that a PPSI establish and maintain an independent testing or audit function, accountable to senior management, with sufficient resources, expertise, and authority to identify U.S. sanctions compliance-related weaknesses and deficiencies. In addition, each PPSI would also have to ensure that qualified personnel routinely perform comprehensive, independent, and objective testing or auditing of the effectiveness of the sanctions compliance program and its functions.
- Proposed § 502.201(b)(5) would require a PPSI establish and maintain a risk-based compliance training program that is: (i) performed at least annually and with a frequency appropriate to the PPSI's risk assessments and risk profile; (ii) provided to all relevant personnel and stakeholders; (iii) appropriately tailored to each trainee's role and responsibilities; (iv) modified to reflect risk assessments findings and identified deficiencies in the sanctions compliance program, including testing and audit findings; and (v) designed to include easily accessible resources and materials for all relevant personnel and stakeholders.
- The proposed penalties are consistent with those prescribed in the GENIUS Act, which provides for a civil penalty of not more than $100,000 for each day during which a PPSI materially violates any regulation issued under the GENIUS Act and an additional penalty of not more than $100,000 per day during which a PPSI knowingly violates any regulation issued under the GENIUS Act. Additionally, the penalties are consistent with those permitted under IEEPA, which allows for the imposition of civil penalties of the greater of $377,700 or twice the amount of the underlying transaction for each violation as well as the Trading with the Enemy Act (TWEA), the sanctions authority that underpins OFAC's Cuba sanctions program, which allows OFAC to impose penalties of up to $111,308 for each violation.

FDIC Proposes BSA and OFAC rules for PPSIs (06-05-26)

- **SUMMARY:** The Federal Deposit Insurance Corporation (FDIC) proposes to issue regulations pursuant to the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) that would implement appropriate Bank Secrecy Act (BSA) and sanctions compliance standards applicable to FDIC-supervised permitted payment stablecoin issuers.
- **DATES:** Comments must be received by the FDIC no later than August 4, 2026.
- **PART 350—PAYMENT STABLECOIN**
- (d) Bank Secrecy Act and economic sanctions compliance requirements and standards. To ensure compliance with Bank Secrecy Act and economic sanctions requirements, each permitted payment stablecoin issuer shall comply with the Bank Secrecy Act, sections 4(a)(5) and 4(a)(6)(B) of the GENIUS Act (12 U.S.C. 5903(a)(5) and (6)(B)), and applicable regulations at 31 CFR chapter V and 31 CFR chapter X, including any Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) program, economic sanctions compliance program, and reporting requirements.

FDIC Proposes BSA and OFAC rules for PPSIs (06-05-26)

- **Enforcement Policy.**
- (a) *In General*. Except with respect to a significant or systemic failure to implement an effective AML/CFT program in accordance with applicable regulations at 31 CFR Chapter X, an FDIC-supervised permitted payment stablecoin issuer that has established an effective AML/CFT program in accordance with applicable regulations at 31 CFR Chapter X will not be subject to an AML/CFT enforcement action or to a significant AML/CFT supervisory action related to the requirements of 31 U.S.C. 5318(h)(1), this section, or applicable regulations at 31 CFR Chapter X.
- *(b) Program establishment violations.* Nothing in this subpart C may be construed to restrict an AML/CFT enforcement action or a significant AML/CFT supervisory action with respect to any failure to establish an effective AML/CFT program in accordance with applicable regulations at 31 Chapter X.
- (*c) Criminal Enforcement Unaffected.* Nothing in this subpart may be construed to affect criminal enforcement liability under the Bank Secrecy Act.

FDIC Proposes BSA and OFAC rules for PPSIs (06-05-26)

- **§ 350.202 FinCEN consultation.**
- (a) *Consultation and consideration requirement.* Before initiating an AML/CFT enforcement action or a significant AML/CFT supervisory action, the FDIC will provide the Director, FinCEN an opportunity to review the action and the FDIC will consider any input offered by the Director, FinCEN on the action, which may include any view as to the effectiveness of the permitted payment stablecoin issuer's AML/CFT program.
- (b) *Notice requirement.* To provide the Director, FinCEN an opportunity to provide a view under § 350.202(a), the FDIC will:
- (1) Send written notice to the Director, FinCEN of its intent to take an action at least 30 days before taking the action (unless a shorter period of time is necessary, in the sole discretion of the FDIC, to remedy, prevent, or respond to an unsafe or unsound practice or condition), accompanied by the relevant AML/CFT information underlying the proposed action, including the relevant portions of the draft report or enforcement action, the relevant examination workpapers supporting the proposed action, and the relevant AML/CFT information submitted by permitted payment stablecoin issuer to the FDIC, other than information over which the permitted payment stablecoin issuer may claim privilege under Federal or State law; and
- (2) Respond to the extent reasonably practicable to requests for additional information from the Director, FinCEN regarding the proposed action.

FDIC Proposes BSA and OFAC rules for PPSIs (06-05-26)

ProSight™

- **§ 350.203 Disclosure of Supervisory Information to FinCEN.**
- **[OPTION 1 FOR PARAGRAPH (§ 350.203):]**
- The FDIC permits a permitted payment stablecoin issuer subject to FDIC jurisdiction, on behalf of FDIC, to disclose to the Director, FinCEN, and permits the Director, FinCEN to use any information of the permitted payment stablecoin issuer relating to an existing or potential AML/CFT enforcement action or significant AML/CFT supervisory action to which the permitted payment stablecoin issuer has access.
- **[OPTION 2 FOR PARAGRAPH (§ 350.203):]**
- (a) The FDIC permits a permitted payment stablecoin issuer subject to FDIC jurisdiction, on behalf of the FDIC, to disclose to the Director, FinCEN, and permits the Director, FinCEN to use any information relating to an existing or potential AML/CFT enforcement action or significant AML/CFT supervisory action to which the permitted payment stablecoin issuer has access upon the contemporaneous disclosure of such information to the FDIC.
- (b) A permitted payment stablecoin issuer's disclosure of information to the Director, FinCEN under § 350.203 does not waive, invalidate, destroy, or otherwise affect any privilege or protection available under Federal or State law, including the attorney-client privilege, the work-product doctrine, the bank-examination privilege, or any other confidentiality or evidentiary privilege.
- (c) Any disclosure made by a permitted payment stablecoin issuer under § 350.203 is made on behalf of the FDIC pursuant to the FDIC's authorization under 12 U.S.C. 1821(t).

OCC Proposes BSA and OFAC rules for PPSIs (06-22-26)

- **SUMMARY:** The Office of the Comptroller of the Currency (OCC), in coordination with the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC), proposes to issue regulations to implement the Guiding and Establishing National Innovation for U.S. Stablecoins Act's requirement to issue regulations implementing appropriate Bank Secrecy Act (BSA) and sanctions compliance standards for permitted payment stablecoin issuers subject to the OCC's jurisdiction.
- *(b) Disclosure of supervisory information to FinCEN.*
- **[OPTION 1 FOR PARAGRAPH (b)(1):]**
- (1) Notwithstanding the other requirements of this part, the OCC permits a permitted payment stablecoin issuer, on behalf of OCC, to disclose to the FinCEN Director, and permits the FinCEN Director to use, any information relating to an existing or potential AML/CFT enforcement action or significant AML/CFT supervisory action to which the permitted payment stablecoin issuer has access.
- **[OPTION 2 FOR PARAGRAPH (b)(1):]**
- (1) Notwithstanding the other requirements of this part, the OCC permits a permitted payment stablecoin issuer, on behalf of the OCC, to disclose to the FinCEN Director, and permits the FinCEN Director to use, any information relating to an existing or potential AML/CFT enforcement action or significant AML/CFT supervisory action to which the permitted payment stablecoin issuer has access upon the contemporaneous disclosure of such information to the OCC.

OCC Proposes BSA and OFAC rules for PPSIs (06-22-26)

- (2) A permitted payment stablecoin issuer's disclosure of information to the FinCEN Director under paragraph (b)(1) of this section does not waive, invalidate, destroy, or otherwise affect any privilege or protection available under Federal or State law, including the attorney-client privilege, the work-product doctrine, the bank-examination privilege, or any other confidentiality or evidentiary privilege.
- (3) Any disclosure made by a permitted payment stablecoin issuer under paragraph (b)(1) of this section is made on behalf of the OCC pursuant to the OCC's authorization under 12 U.S.C. 1821(t).
- (c) AML/CFT and sanctions compliance. To ensure compliance with Bank Secrecy Act and sanctions requirements, each permitted payment stablecoin issuer must comply with the Bank Secrecy Act, sections 4(a)(5) and 4(a)(6)(B) of the GENIUS Act (12 U.S.C. 5901 et seq.), and applicable regulations at 31 CFR chapters V and X, including any AML/CFT program, sanctions program, and reporting requirements.
- **19.261 FinCEN consultation.**
- (a) *Consultation and consideration requirement.* Before initiating an AML/CFT enforcement action or a significant AML/CFT supervisory action against a permitted payment stablecoin issuer, the OCC will provide the FinCEN Director an opportunity to review the action and consider any input offered by the FinCEN Director on the action, which may include any view as to the effectiveness of the permitted payment stablecoin issuer's AML/CFT program.

OCC Proposes BSA and OFAC rules for PPSIs (06-22-26)

- (b) *Notice requirement.* To provide the FinCEN Director an opportunity to provide a view under paragraph (a)(1) of this section, the OCC will:
- (i) Send written notice to the FinCEN Director of its intent to take that action at least 30 days before taking the action (unless a shorter period of time is necessary, in the sole discretion of the Comptroller of the Currency, to remedy, prevent, or respond to an unsafe or unsound practice or condition), accompanied by the relevant AML/CFT information underlying the proposed action, including the relevant portions of the draft report or enforcement action, the relevant examination workpapers supporting the proposed action, and the relevant AML/CFT information submitted by the permitted payment stablecoin issuer to the OCC, other than information over which the permitted payment stablecoin issuer may claim privilege under Federal or State law; and
- (ii) Respond to the extent reasonably practicable to requests for additional information from the FinCEN Director regarding the proposed action.
- **§ 19.262 Enforcement and supervision policy.**
- (a) *In general.* Except with respect to a significant or systemic failure to implement an effective AML/CFT program in accordance with applicable regulations at 31 CFR chapter X, a permitted payment stablecoin issuer that has established an effective AML/CFT program in accordance with applicable regulations at 31 CFR Chapter X will not be subject to an AML/CFT enforcement action or to a significant AML/CFT supervisory action.
- *(b) Program establishment violations.* Nothing in this section may be construed to restrict an AML/CFT enforcement action or a significant AML/CFT supervisory action with respect to any failure to establish an effective AML/CFT program.
- (c) *Criminal Enforcement Unaffected*. Nothing in this subpart may be construed to affect criminal enforcement under applicable law.

GENIUS Act CIP proposal (06-22-26)

- The Financial Crimes Enforcement Network (FinCEN), together with the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) are jointly issuing this proposed rule to implement certain provisions of the Guiding and Establishing National and Innovation for U.S. Stablecoins Act (GENIUS Act). Specifically, this rulemaking implements the GENIUS Act's directives to treat permitted payment stablecoin issuers as financial institutions under the Bank Secrecy Act and to require issuers to maintain an effective customer identification program.
- Comments must be received by August 21, 2026.
- Stablecoin issuers are presently subject to BSA obligations as financial institutions and, more specifically, as money transmitters under FinCEN's regulations, which are a type of money services business (MSB).
- The GENIUS Act also directs the Secretary of the Treasury and each primary Federal payment stablecoin regulator-the OCC, Board, FDIC, and NCUA-to issue regulations through appropriate notice and comment rulemaking and to coordinate, as appropriate, to carry out the Act. FinCEN and the Agencies are issuing a single, joint rule, ensuring consistent and uniform application of CIP requirements to all PPSIs subject to each Agency's jurisdiction.

GENIUS Act CIP proposal (06-22-26)

- (2) *Identity verification procedures*. The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the permitted payment stablecoin issuer to form a reasonable belief that it knows the true identity of each customer. The procedures must be based on the permitted payment stablecoin issuer's assessment of the relevant risks, including those presented by the various types of accounts maintained by the permitted payment stablecoin issuer, the various methods of opening accounts provided by the permitted payment stablecoin issuer, the various types of identifying information available and the permitted payment stablecoin issuer's size, location, and customer base. At a minimum, these procedures must contain the elements described in this paragraph (a)(2).
- (i) *Customer information required* -(A) *In general*. The CIP must contain procedures for opening an account that specify the identifying information that (printed page 37271) will be obtained with respect to each customer. Except as permitted by paragraph (a)(2)(i)(B) of this section, the permitted payment stablecoin issuer must obtain, at a minimum, the following information from the customer prior to opening an account:
- (1) Name;
- (2) Date of birth, for an individual; or date of formation, for a person that is not an individual;
- (3) Address, which shall be:
- (i) For an individual, a residential or business street address;
- (ii) For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, of the residential or business street address of a next of kin or of another contact individual; or
- (iii) For a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and

GENIUS Act CIP proposal (06-22-26)

- (4) Identification number, which shall be:
- (i) For a U.S. person, a taxpayer identification number; or
- (ii) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard; or
- (iii) For a non-U.S. person that is not an individual and that does not have an identification number, the permitted payment stablecoin issuer must request alternative government-issued documentation certifying the existence of the person.
- (B) *Exception for persons applying for a taxpayer identification number*. Instead of obtaining a taxpayer identification number from a customer prior to opening an account, the CIP may include procedures for opening an account for a person that has applied for, but has not received, a taxpayer identification number. In this case, the CIP must include procedures to confirm that the application was filed before the person opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.
- (ii) *Customer verification*. The CIP must contain procedures for verifying the identity of each customer, using information obtained in accordance with paragraph (a)(2)(i) of this section, within a reasonable time before or after the customer's account is opened. The procedures must describe when the permitted payment stablecoin issuer will use documents, non-documentary methods, or a combination of both methods, as described in this paragraph (a) (2)(ii).

GENIUS Act CIP proposal (06-22-26)

- (A) *Verification through documents*. For a permitted payment stablecoin issuer relying on documents, the CIP must contain procedures that set forth the documents the permitted payment stablecoin issuer will use. These documents may include:
- (1) For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- (2) For a person other than an individual (such as a corporation, partnership, or trust), documents and any amendments thereto showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.
- (B) *Verification through non-documentary methods*. For a permitted payment stablecoin issuer relying on non-documentary methods, the CIP must contain procedures that set forth the non-documentary methods the permitted payment stablecoin issuer will use.
- (1) These methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided with respect to the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; or obtaining a financial statement.
- (2) The permitted payment stablecoin issuer's non-documentary procedures must address situations where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the permitted payment stablecoin issuer is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without meeting in person; and the permitted payment stablecoin issuer is otherwise presented with circumstances that increase the risk that the permitted payment stablecoin issuer will be unable to verify the true identity of a customer through documents.

GENIUS Act CIP proposal (06-22-26)

- (C) *Additional verification for certain customers.* The CIP must address situations where, based on the permitted payment stablecoin issuer's risk assessment of a new account opened by a customer that is not an individual, the permitted payment stablecoin issuer will obtain information about individuals with authority or control over such account in order to verify the customer's identity. This verification method applies only when the permitted payment stablecoin issuer cannot verify the true identity of a customer that is not an individual using the verification methods described in paragraphs (a)(2)(ii)(A) and (B) of this section.
- (iii) *Lack of verification*. The CIP must include procedures for responding to circumstances in which the permitted payment stablecoin issuer cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:
- (A) When the permitted payment stablecoin issuer should not open an account;
- (B) The terms under which a customer may use an account while the permitted payment stablecoin issuer attempts to verify the customer's identity;
- (C) When the permitted payment stablecoin issuer should close an account after attempts to verify a customer's identity fail; and
- (D) When the permitted payment stablecoin issuer should file a Suspicious Activity Report in accordance with applicable law and regulation.

GENIUS Act CIP proposal (06-22-26)

- (i) *Required records*. At a minimum, the record must include:
- (A) All identifying information about a customer obtained under paragraph (a)(2) (i) of this section;
- (B) A description of any document that was relied on under paragraph (a)(2)(ii) (A) of this section, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date;
- (C) A description of the methods and results of any measures undertaken to verify the identity of a customer under paragraphs (a)(2)(ii)(B) and (C) of this section; and
- (D) A description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained.
- (ii) *Retention of records*. The permitted payment stablecoin issuer must retain the records made under paragraph (a)(3)(i)(A) of this section for five years after the date the account is closed and the records made under (printed page 37272) paragraphs (a)(3)(i)(B) through (D) of this section for five years after the record is made.
- (4) *Comparison with Government lists*. The CIP must include reasonable procedures for determining whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal Government agency and designated as such by Treasury in consultation with the primary Federal payment stablecoin regulators. The procedures must require the permitted payment stablecoin issuer to make such a determination within a reasonable period of time after the account is opened, or earlier if required by another Federal law or regulation or Federal directive issued in connection with the applicable list. The procedures must also require the permitted payment stablecoin issuer to follow all Federal directives issued in connection with such lists.

GENIUS Act CIP proposal (06-22-26)

- (5) Notice -(i) *Customer notice*. The CIP must include procedures for providing customers with adequate notice that the permitted payment stablecoin issuer is requesting information to verify their identities.
- (ii) *Adequate notice*. Notice is adequate if the permitted payment stablecoin issuer generally describes the identification requirements of this section and provides such notice in a manner reasonably designed to ensure that a prospective customer is able to view the notice, or is otherwise given notice, before opening an account. For example, depending upon the manner in which the account is opened, a permitted payment stablecoin issuer may post a notice on its website, include the notice in its account applications, or use any other form of oral or written notice.

FinCEN-WCHT-Notice (05-11-26)

- **Suspicious Activity Report (SAR) Filing Request:**
- FinCEN requests that financial institutions reference this Notice in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term “FIN-2026-HTWORLDCUP” and select SAR Field 38(h) (human trafficking).
- The U.S. Department of the Treasury’s (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to urge financial institutions to be vigilant in detecting, identifying, and reporting suspicious activity connected to human trafficking associated with the 2026 Fédération Internationale de Football Association (FIFA) World Cup. While human trafficking is an ever-present threat in the United States, major events such as the 2026 FIFA World Cup can create a concentrated demand for licit and illicit services, including commercial sex acts and involuntary servitude, resulting in increased vulnerability for human trafficking. Individuals visiting or residing near World Cup host cities may be vulnerable to trafficking by perpetrators seeking to exploit increased economic activity surrounding such events.
- The United States, along with Canada and Mexico, will host the 2026 FIFA World Cup from June 11 to July 19, 2026, in Atlanta, Boston, Dallas, Houston, Kansas City, Los Angeles, Miami, New York/New Jersey, Philadelphia, the San Francisco Bay Area, and Seattle; as well as Toronto and Vancouver in Canada; and Guadalajara, Mexico City, and Monterrey in Mexico.

FinCEN-WCHT-Notice (05-11-26)

- FinCEN recommends increased vigilance by financial institutions located in and around host city locations associated with the 2026 FIFA World Cup. It is also critical that customer-facing financial institution staff are aware of behavioral indicators that may indicate human trafficking, as victims of human trafficking may have no contact with people outside of their traffickers other than when visiting financial institutions.
- Human trafficking and TCOs are two of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities. Treasury's 2026 U.S. National Money Laundering Risk Assessment also notes human trafficking is estimated to be a multi-billion dollar industry that generates substantial illicit proceeds for TCOs and associated networks, creating risks in the U.S. financial system.
- FinCEN strongly encourages financial institutions to notify law enforcement of suspected human trafficking-related activity via the National Human Trafficking Hotline, in addition to filing SARs regarding human trafficking activity related to the 2026 FIFA World Cup as soon as possible regardless of threshold. FinCEN also encourages information sharing among financial institutions to identify, report, and prevent human trafficking-related activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering related to human trafficking.

FinCEN-WCHT-Notice (05-11-26)

- Major events such as the 2026 FIFA World Cup create opportunities for traffickers to take advantage of the inundation of tourists, increased hotel bookings, and the subsequent increase in demand for licit and illicit services There is no specific profile for a trafficked victim, as traffickers are willing to exploit anyone who can earn them illicit profits, but certain groups may be at an increased risk of being trafficked.
- Victims of trafficking may be compelled by force, fraud, or coercion to engage in commercial sex acts. Sex trafficking may exist within varied settings, including in public on city streets and at truck stops, as well as within illicit massage businesses, escort services, residential brothels, strip clubs, hostess clubs, hotels, and motels. Sex traffickers may recruit victims and advertise opportunities to engage in commercial sex acts online through websites, social media, or other digital platforms. According to law enforcement, victims may be forced to travel frequently to meet clients for commercial sex acts within short timeframes, and the victims or their traffickers may have unusually large travel-related transactions. Victims often receive payment for commercial sex acts in cash but may also receive payments via peer-to-peer (P2P) transfers, credit card transactions, and digital assets. Law enforcement and BSA data also identified a trend of prepaid access cards being used to pay for commercial sex acts beginning in 2020. According to law enforcement, victims are often instructed to deposit cash received in exchange for commercial sex acts into easily accessible automated teller machines (ATMs) and then transfer these funds to another account. In cases where victims are paid through P2P transfers, the victims are typically instructed by their traffickers to quickly transfer these funds via P2P to another account.

FinCEN-WCHT-Notice (05-11-26)

- Victims may be lured into employment by recruiters or misled to believe that they are obtaining lawful employment for their labor or services These victims may be exploited for their labor through the use of force, fraud, or coercion. victim’s wages may be withheld entirely or partially by their traffickers, indicated by an absence or deviation of expected payroll expenses, or wages may be transferred from the victim’s account to their traffickers. Victims of trafficking may also have minimal or no transactions associated with maintaining essential needs, given the trafficker financial control over the victim.

1. A customer in or around a city hosting a major event has unusually large local travel expenses (e.g., multiple hotel rooms, taxi or ridesharing fares, train tickets) in a relatively short period of time, especially expenses occurring during late night and early morning hours, for no business or apparent lawful purpose.
2. A customer’s account has few or no transactions indicative of obtaining or maintaining essential needs (e.g., housing, personal products and nourishment, travel) and may only receive credits from multiple third parties or a direct deposit or paycheck that is immediately transferred to a singular individual or business account.
3. A customer’s account has an unusually high number of transactions involving essential needs (e.g., multiple payments for housing or lodging, bulk purchases of personal products and goods for nourishment, travel-related expenses) or bulk purchases of prepaid access cards for no business or apparent lawful purpose.

FinCEN-WCHT-Notice (05-11-26)

4. A customer's business account does not exhibit normal or expected payroll expenditures for any readily discernible reason. For example, the customer's business transactions indicate that payroll is nonexistent or extremely low compared to businesses in the same industry with similar profiles.
5. A customer deposits funds into an account at a location other than where the customer resides and the funds are quickly withdrawn, typically in a separate location from the deposits, for no business or apparent lawful purpose.
6. A customer frequently deposits or withdraws cash at ATMs, especially ATMs located at gas stations, particularly if the transactions occur between 10:00pm and 5:00am. The customer may quickly transfer deposited funds via P2P transfers to a separate account for no business or apparent lawful purpose.
7. A customer regularly receives multiple P2P transfers from accounts with which the customer has no previous transactional relationships and for which there is no business or apparent lawful purpose. Payment memos may indicate or contain vague references disguising payment for commercial sex (e.g., "link," "services," "donation," "personal care," "wellness," "advertisements," etc.). These funds are then further sent via P2P, in whole or in part, to another account.
8. A customer receives frequent P2P transfers from multiple accounts and seems to be consolidating funds received by others via P2P transfers for no business or apparent lawful purpose. This activity may be indicative of the movement of funds related to sex trafficking.
9. A customer sends three rapid, sequential P2P transfers to three separate accounts for no business or apparent lawful purpose. Such payments may indicate illicit massage business payments, where a customer is expected to make three payments, specifically a door fee, a service fee, and a tip for services provided.

FinCEN-WCHT-Notice (05-11-26)

10. The phone number associated with a customer's account is listed as a contact method in online commercial sex advertisements. This could be potentially indicative of either a victim's or a trafficker's account.

- Financial institutions filing Suspicious Activity Reports (SARs) on human trafficking associated with the 2026 FIFA World Cup should reference this Notice in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2026-HTWORLDCUP" and select SAR field 38(h) (human trafficking).
- If you believe you may have information about a trafficking situation:
  - Call the National Human Trafficking Hotline toll-free hotline at 1-888-373-7888: Anti-Trafficking Hotline Advocates are available 24/7 to take reports of potential human trafficking.
  - Text the National Human Trafficking Hotline at 233733.
  - Chat the National Human Trafficking Hotline via humantraffickinghotline.org/chat.
  - Submit a tip online through the anonymous online reporting form. However, please note that if the situation is urgent or occurred within the last 24 hours the hotline encourages you to call, text, or chat.

FinCEN Alert IRGC (05-11-26)

- The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to assist financial institutions in identifying actors suspected of funding and facilitating procurement networks supporting the Islamic Revolutionary Guard Corps (IRGC) and mitigating those risks through the filing of suspicious activity reports (SARs). The IRGC was created after the Iranian Revolution as a parallel organization to Iran's regular armed forces that reports directly to Iran's Supreme Leader and is charged with defending the Iranian regime. The IRGC includes ground, naval, and air forces, along with the Basij internal security militia, and the IRGC-Qods Force (IRGC-QF).
- As described in FinCEN's 2025 Iran Advisory, the IRGC relies on complex financial facilitation networks comprised of exchange houses, front companies, financial facilitators, and other service providers operating across multiple jurisdictions to obscure beneficial ownership, disguise the origin of funds, and enable movement of proceeds linked to sanctions evasion and other illicit activity. In addition, recent analysis of Bank Secrecy Act (BSA) data indicates that the IRGC relies on networks of shell companies and financial facilitators to launder digital asset proceeds through layered corporate structures and cross-border transactions.
- This Alert reminds financial institutions of their BSA reporting obligations and encourages vigilance against sanctions evasion, terrorist financing, and other illicit activity that may be connected with the IRGC.

FinCEN Alert IRGC (05-11-26)

- Iran as well as the IRGC are subject to comprehensive U.S. sanctions, including a prohibition on opening or maintaining correspondent accounts in the United States for, or on behalf of, Iranian financial institutions pursuant to Section 311 of the USA PATRIOT Act pursuant to a finding that the jurisdiction of Iran is a primary money laundering concern. Furthermore, FinCEN notes that the Financial Action Task Force (FATF) has long identified Iran as a high-risk jurisdiction, and recently re-iterated the need for countries to apply effective countermeasures, including calling on all jurisdictions to prohibit Iranian digital asset service providers from establishing or maintaining a presence in their countries or establishing relationships with their digital asset service providers, along with limiting digital asset transactions with Iran.
- The IRGC and other Iranian actors rely on multi-jurisdictional “shadow banking” network so comprised of exchange houses, trading companies, and front companies to sell oil and other commodities abroad, launder the proceeds, and then procure weapons and other materiel on the international market.
- U.S. financial institutions may indirectly detect Iran-linked rahbar companies and exchange houses when processing U.S. dollar-denominated payments for foreign correspondents. Indicators include recently incorporated entities transacting in unusually large sums, rapid movement of funds, transactions between companies in disparate lines of business, and large, round dollar payments. Treasury also continues to encourage U.S. financial institutions to exercise heightened vigilance with respect to certain correspondent relationships and to carefully consider whether it may be appropriate to require certain respondents to apply strengthened controls, such as targeted monitoring, heightened due diligence, or additional training.

FinCEN Alert IRGC (05-11-26)

- According to industry reporting, the volume of Iranian digital assets activity has reached billions of dollars per year. Iranian government entities, including the IRGC, conduct sanctions evasion as part of this activity In addition, according to press reporting, Iran has stated its intent to use digital assets to collect illegal payments from oil tankers attempting to freely navigate passage through the Strait of Hormuz.
- Because digital assets can be quickly transferred internationally without intermediary financial institutions, digital assets enable Iranian facilitators to circumvent the traditional financial system. Like other illicit actors, Iranian facilitators are likely to use stablecoins for this purpose, due to stablecoins' relative liquidity, ease of settlement, and exchange rate stability Iran is also adapting its abuse of stablecoins in its continued efforts to evade sanctions. According to FinCEN analysis, Iran's use of stablecoins includes minting and moving between large volume stablecoin issuers as well as the creation of proprietary stablecoins, such as USDZ, the stablecoin associated with OFAC-designated stablecoin issuer Zedxion.
- U.S. financial institutions with exposure to digital assets should consider reviewing blockchain ledgers for activity attributed to Iran-based DASPs, including indirect connections to such activity. Institutions should also be aware that the international digital assets industry is highly dynamic; new digital assets businesses may incorporate or operate in Iran with little notice or footprint, making it especially important to assess the risks of recently established digital asset businesses. Further, unregistered peer-to-peer (P2P) exchangers and unregistered foreign-located MSBs may offer digital asset-related services in Iran. Financial institutions should be aware that these unregistered digital asset exchangers typically rely on the liquidity provided by larger DASPs to process transactions.

FinCEN Alert IRGC (05-11-26)

- **Oil Smuggling-Related Red Flags**

1. Shipping Companies with Iranian Counterparties. Transactions involving a petroleum or shipping company reveal that it does business with counterparties that have ties to Iran or transport goods using “shadow fleet” vessels that have ties to Iran or that maritime databases indicate have made stops at Iranian ports.
   - *Financial institutions may consider ensuring their correspondent account holders conduct due diligence on their customers for prior connections to Iran or Iranian counterparties.*
2. Irregularities in Shipping Documentation that may be Intended to Hide Activities Involving Iran. A customer makes oil-related transactions and wire transfers involving vessels that have been previously linked to suspicious financial activities or that include documentation, such as bills of lading or shipping invoices, with no consignees, that appear to be falsified, or that omit key information, to obfuscate the Iranian nexus.
   - *Financial institutions may consider requiring a review of shipping documentation to identify falsified or missing information where practical.*
3. Efforts to Disguise Vessel Information and Ownership. Documentation associated with a customer’s oil-related transactions references vessels that, according to maritime databases, have undergone recent or multiple name or flag changes, or transfer of ownership or operation to another person following OFAC’s designation of its owner or operator, but the designated owner or operator appears to maintain an interest in the vessel.
   - *Financial institutions may consider requiring due diligence on vessels to determine whether they have undergone recent name, flag, or ownership changes, including transfer from sanctioned persons.*

FinCEN Alert IRGC (05-11-26)

4. Efforts to Disguise Oil Origins. Documentation associated with a customer's oil-related transactions references "Malaysian blend" oil, particularly if the vessel is bound for China by way of Southeast Asia and if maritime databases indicate that the vessel displayed Automatic Information System (AIS) irregularities during its voyage or reveal evidence of a ship-to-ship transfer in geographic areas of concern or without commercial need.
   - *Financial institutions may consider requiring heightened due diligence on any transactions referencing "Malaysian blend" oil, particularly if the transactions show other indications of oil smuggling.*

- **Shadow Banking and Front Company Abuse-Related Red Flags**

5. Unclear Sources of Funds. A customer receives wire transfers or deposits that do not contain any information about the source of funds, contain incomplete information about the source of funds, or do not match the customer's line of business, and they involve entities in a high-risk jurisdiction for Iranian illicit finance-related activity.
   - *Financial institutions may consider reviewing relationships with clients that show a pattern of opaque business dealings in jurisdictions at high risk for IRGC abuse.*
6. Use of Company Types and Jurisdictions at High-Risk for IRGC Abuse. A general trading company with opaque ownership registered in a commercial free trade zone in the UAE or other location and whose trading counterparties are companies mostly located in jurisdictions such as Singapore and Hong Kong has bank accounts at multiple financial institutions in locations such as China, Hong Kong, Oman, or the UAE.
   - *Financial institutions may consider conducting heightened due diligence on company types that are at high risk for IRGC abuse.*

FinCEN Alert IRGC (05-11-26)

7. Likely Front Companies that Exhibit Transaction Patterns Typical of IRGC Shadow Banking. A company registered in Hong Kong that banks using a Chinese non-resident account has little to no web presence, is co-located with numerous other similar companies, or is recently incorporated yet transmitting large, round dollar payments with no adequate explanation for the source of funds, or makes numerous payments in large figures to UAE general trading companies or commercial free trade zone-based intermediaries with no clear business purpose.
    - *Financial institutions should consider conducting heightened due diligence on recently formed companies transacting in unusually high amounts that exhibit payment patterns typical of Iranian shadow banking.*
8. Unusual Use of Exchange Houses. A customer makes transactions that move through multiple exchange houses and/or trading companies, adding additional fees and costs as the transactions progress, where the fees, number of transactions, or pattern of transactions do not reflect standard and customary commercial practices.
    - *Financial institutions may consider conducting heightened due diligence on customers that make frequent or unusual use of exchange houses in jurisdictions at high risk for IRGC activity.*

- **Digital Assets-Related Red Flags**

9. Unusual Digital Asset Payments by Petroleum, Shipping, Trading, or Trust Companies. A company engaged in a line of business with potential exposure to Iranian oil smuggling deviates from normal business practices to send or receive payments using digital assets.
    - *Financial institutions may consider conducting heightened due diligence for companies using digital assets to effect significant payments in cases where the underlying transaction could be related to Iranian oil.*

FinCEN Alert IRGC (05-11-26)

ProSight™

10. Stablecoin Payments with an Unclear Source of Funds. A customer in a high-risk jurisdiction for Iranian illicit finance-related activities receives a stablecoin payment that does not match the customer's line of business and fails to provide information about the source of funds or provides documentation indicating a potential link to Iranian illicit finance.
    - *Financial institutions may consider requesting documentation from customers regarding the source of digital asset payments that involve entities in a high-risk jurisdiction for Iranian illicit finance related activity.*
11. Unusual Stablecoin Account Activity. A customer of a stablecoin issuer, particularly a foreign entity such as an overseas purported trust company, opens an account and subsequently engages in mint activity requiring multiple rate/limit increases in a short period of time, or otherwise transacts in a manner that does not appear consistent with its reported business profile.
    - *Financial institutions may consider requesting documentation from customers regarding the source of stablecoin payments that involve entities in a high-risk jurisdiction for Iranian illicit finance related activity.*
12. Payments to or from an Iran-located DASP. Blockchain analysis indicates that a customer account transacted directly or indirectly with a digital asset address attributed to an Iranian entity.
    - Financial institutions may consider using blockchain analytics to identify digital asset transactions that may be connected to a known Iranian entity.

FinCEN Alert IRGC (05-11-26)

13. Iran-related Cyber Indicators. Authentication and account activity indicates that a user may be conducting digital asset transactions from Iran. For example, activity logs may show connections from Iranian IP addresses, or sharing IP addresses or common devices with users previously identified as having an Iranian nexus, authentication using an Iranian email service or Iranian telephone number, or use of a device with time zone, language, and other setting consistent with a location in Iran. Connection through a virtual private network (VPN), residential proxy network, or Tor exit node—when combined with other evidence of a location in Iran—may indicate an attempt by an Iranian user to circumvent geofencing. In reporting such activity, financial institutions may also be able to provide associated technical details such as IP addresses with time stamps, device identifiers, and indicators of compromise that can provide helpful information to authorities.
    - *Financial institutions may consider screening cyber indicators such as IP addresses for evidence that an account has been accessed from Iran or by an Iranian entity.*
14. P2P Exchangers, Foreign-Located MSBs, and Nested DASPs. Account activity indicates that a customer may operate as an unregistered P2P exchanger, foreign-located MSB, or nested DASP that provides services in Iran. For example, a customer of a DASP who is located in a high-risk jurisdiction for Iranian illicit finance-related activity appears to be using liquidity provided by the DASP to execute large numbers of offsetting transactions.
    - *Financial institutions may consider heightened monitoring of customer accounts for activity associated with potential operation of an unregistered P2P exchanger, foreign-located MSB, or nested DASP for customers with possible exposure to Iranian counterparts.*

FinCEN Alert IRGC (05-11-26)

- FinCEN requests that financial institutions reference this Alert by including the key term “FIN-2026-Alert002” in SAR field 2 (Filing Institutions Note to FinCEN) and the narrative, and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization).

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

- The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN), jointly with the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and National Credit Union Administration, (collectively, the Agencies), is issuing this Advisory in coordination with the Internal Revenue Service (IRS) to advise financial institutions—in particular, banks—to be vigilant against fraud schemes and other suspicious or potentially criminal activities involving the unlawful employment of illegal aliens and the associated risks to the integrity of the U.S. financial system. Through these schemes, employers can gain an unfair advantage over legitimate U.S. businesses; depress wages; facilitate identity theft of people who are authorized to work in the United States, including American citizens; and steal millions of dollars in Federal and state payroll tax revenue meant for government benefit programs.
- In certain instances, the access to financial services and unlawfully obtained wages can be leveraged to facilitate the financing of transnational criminal organizations (TCOs)—several of which have been designated as Foreign Terrorist Organizations (FTOs)—and their global criminal enterprises, including drug trafficking, human trafficking, and other illegal activity in the United States.
- This joint Advisory aligns with FinCEN's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities of Fraud, Terrorist Financing, Drug Trafficking Organization (DTO) Activity, TCO Activity, and Human Trafficking and Human Smuggling, and is issued as part of Treasury's continued effort to prevent the exploitation of the U.S. financial system by illegal aliens in the United States.

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

- The Immigration Reform and Control Act (IRCA) of 1986 prohibits U.S. persons and entities from knowingly hiring, or recruiting or referring for a fee, unlawful aliens for employment. Under IRCA and its implementing regulations, employers are required to verify and document the identity and employment eligibility of their employees through the Employment Eligibility Verification Form I-9 (Form I-9).
- According to ICE, many employers across the agriculture, construction, domestic service, hospitality, and other industries (hereafter "complicit employers") are knowingly—or through willful negligence—facilitating the hiring, concealment, and in some cases, exploitation of unlawful alien labor in their workforce to reduce labor costs and gain an unfair advantage over competitors. A key feature of these schemes is the use of identity theft and payroll fraud to conceal violations of IRCA and other U.S. immigration laws.
- According to recent ICE worksite enforcement operations, unlawful aliens illicitly obtain Social Security numbers (SSNs) and other personally identifiable information (PII) of U.S. citizens and lawful permanent residents and submit this information to make the Form I-9s appear legitimate, gain unlawful employment and wages, as well as employer- and government-provided health care benefits in the United States, and, based on FinCEN's analysis of Bank Secrecy Act (BSA) reporting, fraudulently obtain access to financial services and extension of credit for automobile and other types of loans. Victims of these identity theft schemes can face higher taxes, and denial of employer and government provided health care, disability, and tuition benefits as a result of illegal aliens using their stolen identity to earn wages and employment benefits. The fraudulently obtained SSNs and other PII can also be used by illegal aliens to remit unlawfully obtained wages through financial institutions to their home countries. As part of these schemes, complicit employers may also assist illegal aliens in perpetrating identity theft and obtaining fraudulent documentation. In some instances, this may serve as a means to exploit and abuse their unlawful alien workers.

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

ProSight™

- Complicit employers can also conceal their violation of IRCA and the hiring of low wage unlawful alien workers through off-the-books payments These schemes allow complicit employers to further reduce their labor costs by evading Federal payroll taxes—contributing to a significant tax gap in recent years—under the Federal Insurance Contributions Act (FICA) for Social Security and Medicare and the Federal Unemployment Tax Act (FUTA), as well as state-level payroll taxes and premiums for required employment benefits such as workers' compensation insurance. In its simplest form, these schemes involve complicit employers making cash payments or using irregular payment methods to pay unlawful alien workers while maintaining two sets of books for payroll—one to submit fraudulent filings to the IRS and one to track the actual, illegal payments.
- These schemes often start with complicit employers contracting with a complicit labor broker. The labor broker will set up a shell company either directly or through a nominee owner purporting to be involved in the agriculture, construction, domestic service, hospitality, or staffing industries. The shell company will often be an unregistered money services business (MSB) providing off the books payroll or payment processor services for the complicit employers. According to the IRS, these shell companies may have generic names such as ABC Construction or XYZ Logistics that may correlate to the initials of the labor broker's name. Based on FinCEN's analysis of BSA reporting and other available information, complicit labor brokers may also use the shell company to engage in other illicit transactions such as money laundering for DTOs and TCOs. These schemes are often part of a broader, global money laundering network that inserts cash into the U.S. financial system in small amounts, across a large number of cities, and then collects checks from the involved businesses—including shell companies associated with payroll fraud schemes.

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

- The complicit labor broker then directs the complicit employers to write checks payable to the shell company for purported services or products related to their industry (e.g., a construction business sending checks for framing, drywall, stucco, masonry, or painting). The complicit labor brokers can then launder the funds by cashing the checks to the shell companies in structured transactions through banks and MSBs, including check cashiers, or depositing the checks into the shell company's bank account.
- After deducting a four to ten percent fee for the off-the-books payroll services, the complicit labor broker sends payments to the unlawful alien workers on behalf of the complicit employers through (i) cash couriers, (ii) checks, or (iii) peer-to-peer (P2P) platforms. These payments (known as "structuring" and "microstructuring") are often repetitive transactions that are designed to fall below BSA reporting and recordkeeping thresholds, and that may correlate to payroll cycles outside of standard payroll processing systems. Neither the complicit labor broker nor the complicit employers withhold any Federal and state payroll taxes for the unlawful alien workers, and do not pay the employer share of such taxes. Complicit labor brokers may also use the shell company to obtain a minimal workers' compensation policy for a small number of purported employees and "rent" or sell access to the complicit employers that are employing hundreds of unlawful alien workers to allow them to avoid costly premiums by committing insurance fraud. As a result of this off-the-books payroll tax evasion and workers' compensation fraud scheme, the complicit employers undercut legitimate companies hiring lawful workers, steal millions of dollars of payroll taxes, and defraud insurance companies.

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

- FinCEN's regulations define the term Taxpayer Identification Number (TIN) by cross-referencing section 6109 of the Internal Revenue Code of 1986 (the IRC). The IRC and its implementing regulations define ITINs, which are issued to resident and nonresident aliens not eligible for an SSN solely for Federal tax purposes. An ITIN is a nine-digit number beginning with the number "9" and has a range of numbers from "50" to "65," "70" to "88," "90" to "92," and "94" to "99" for the fourth and fifth digits (i.e. 9XX-7X-XXXX). ITINs do not provide evidence of legal status in the United States, authorize recipients to work legally in the United States, or serve as identification outside of the Federal tax system.
- Although ITINs facilitate tax compliance, the Agencies, in accordance with E.O. 14406, note that the use of an ITIN in lieu of an SSN or valid employment authorization document may be identified as a risk factor requiring enhanced due diligence to ensure the account is not being utilized to facilitate the unlawful employment of unlawful aliens. The Agencies are also particularly concerned by the use of an ITIN to obtain credit products or open depository accounts where the applicant lacks verified legal presence and the potential illicit finance risks associated with such activity.
- Consistent with existing BSA obligations, the Agencies encourage banks subject to the jurisdiction of the Agencies to consider the use of an ITIN as part of the bank's application of appropriate risk based procedures for customer due diligence. Specifically, when an ITIN is presented in lieu of an SSN or valid employment authorization document to obtain credit products or open an account, banks are encouraged to assess whether the use of an ITIN may be a relevant risk factor. Banks are further encouraged to conduct this assessment in light of the totality of other factors and information available to the bank to understand the nature and purpose of customer relationships for the purpose of developing customer risk profiles and conduct ongoing monitoring to identify and report suspicious transactions.

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

- FinCEN has identified the following red flags to help financial institutions detect, prevent, and report suspicious activity connected to fraud schemes involving the unlawful employment of unlawful aliens. Many of these red flags build off of FinCEN's 2 023 Payroll Tax Fraud Notice, which remain relevant for this joint Advisory.
- Red flags may include:
- *A customer is an individual that:*

1. Uses an SSN that, upon verification, does not match or is inconsistent with the SSA's records;
2. Opens an account using a non-U.S. passport or ITIN claiming to be self-employed or operating a small business in the agriculture, construction, domestic service, hospitality, or staffing industries and is receiving a significant amount and volume of recurring check deposits from multiple companies before either making a significant and repetitive amount of structured cash withdrawals or issuing low-dollar checks to multiple individuals;
3. Cashes a significant volume of checks drawn on accounts owned by companies in the agriculture, construction, domestic service, hospitality, or staffing industries on a recurring basis at an MSB, including a check cashier;
4. Receives recurring P2P payments from a small, recently established company in the agriculture, construction, domestic service, hospitality, or staffing industries;

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

5. Works in the agriculture, construction, domestic service, hospitality, or staffing industries and opens a bank account with an ITIN with little to no transactional activity besides remittance to foreign jurisdictions;
6. Opens an account for a company in the agriculture, construction, domestic service, hospitality, or staffing industries and is attempting to use a Commercial Mail Receiving Agency instead of a business address;
7. Possesses no known prior involvement in the agriculture, construction, domestic service, hospitality, or staffing industries and provides a non-U.S. passport or ITIN as a form of identification when opening an account for a new company in those industries;
8. Makes statements as the account holder or company representative to bank tellers or check cashers that the purpose of the cash withdrawals, negotiation of checks for cash, or check cashing activity is for payroll and the volume, amount, and frequency of transactions are uncharacteristic for a company in agriculture, construction, domestic service, hospitality, or staffing industries with a small number of employees;

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

- *A customer is a large company in the agriculture, construction, domestic service, hospitality, or staffing industries that:*

9. Has been identified by ICE worksite enforcement news releases and open-source reporting that the customer has a history of worksite compliance violations from ICE;
10. Has significant business operations and transactional activity but with little to no payroll activity commensurate to the customer's profile;
11. Is making Federal and state payroll tax deposits that are significantly less than what would be expected based on their business operations and associated workforce size;
12. Is issuing a significant and repetitive amount of checks to a singular or small number of recently established companies with little to no online presence;
13. Recently acquired a workers' compensation policy for a small number of workers that is not commensurate with their customer profile and transactional activity;

FinCEN Advisory Non-Work Authorized Populations (06-05-26)

ProSight™

- *A customer is a small company in the agriculture, construction, domestic service, hospitality, or staffing industries:*

14. With beneficial owners that have no known prior involvement with, or in, the company or these industries and may have prior fraud convictions;
15. With minimal to no history of tax- or payroll-related payments to the IRS, state and local tax authorities, or a third-party payroll company despite a large volume of deposits from clients;
16. That conducts large or unusual volumes of cash withdrawals or negotiation of checks for cash when accompanied by another involved person(s) or using an armored car service to deliver bulk cash (i.e., conducting informal or off-the-books payroll);
17. That is issuing recurring, large volumes of checks for under $1,000 that are made payable to a significant number of separate individuals who cash the checks; and/or
18. That is a new customer (i.e., less than two years old) with minimal to no online presence and has indicators of being a shell company.

- FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Advisory by including the key term “FINANCIALINTEGRITY-2026-A002” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative.

314b Fact Sheet (06-12-26)

ProSight™

- **Issue Date: June 12, 2026**
- The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this fact sheet in support of Treasury's efforts to promote greater information sharing between and among financial institutions to identify fraud, money laundering, terrorist financing, narcotics trafficking and related crimes, sanctions evasion, and other criminal activity. This fact sheet further clarifies: (1) the permissibility of real-time information sharing under section 314(b) of the USA PATRIOT Act; (2) under what circumstances information, including related to fraud, can be shared; and (3) how information can be shared. This fact sheet expands upon and replaces FinCEN's December 2020 fact sheet.
- Section 314(b) provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, to improve the identification and reporting of activities that may involve money laundering or terrorist activities. Participation in information sharing pursuant to section 314(b) is voluntary. FinCEN strongly encourages financial institutions to participate in the program as information sharing between and among financial institutions can assist financial institutions in managing illicit financing risks and can ultimately provide the government with highly useful information to identify and prevent financial crime.
- Among other things, information sharing pursuant to section 314(b) allows financial institutions to respond to threats—activities a financial institution suspects may involve possible terrorist activity or money laundering, such as fraud and other criminal activity—that are carried out by repeat actors moving across financial institutions to evade detection. The section 314(b) program provides financial institutions with the flexibility and connectivity needed to counter these threats and prevent bad actors from exploiting gaps between institutions.

314b Fact Sheet (06-12-26)

ProSight™

- **What information can be shared pursuant to section 314(b)?**
- Financial institutions and associations of financial institutions may rely on the safe harbor provided by section 314(b) to share information with one another regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering (which, as discussed below, may include information about fraud and other specified unlawful activities (SUAs)).
- "Money laundering" includes knowingly conducting or attempting to conduct a financial transaction with proceeds from SUA that is intended to promote the SUA. Activity constituting "specified unlawful activity" is defined in 18 U.S.C. § 1956, which lists the predicate crimes for money laundering offenses. These SUAs include a range of fraud offenses, including federal statutes used to charge schemes involving fraud against individuals, organizations, or governments. Accordingly, if a financial institution or association of financial institutions suspects that a transaction may involve the proceeds of fraud (or other criminal activity) or be for the purpose of furthering or concealing a fraudulent scheme or other criminal activity, then it may share related information with other financial institutions or associations of financial institutions under section 314(b).
- For example, a financial institution or association of financial institutions may share information on attempts to engage in transactions that the financial institution or association of financial institutions suspects may involve money laundering or terrorist activity. A financial institution or association of financial institutions may also share information about attempts to induce others to engage in transactions, such as in a money mule scheme, where the other conditions of section 314(b) are satisfied.

314b Fact Sheet (06-12-26)

- Sharing may occur between one financial institution or association of financial institutions and another, or financial institutions and associations of financial institutions may share information within a group of participating financial institutions or associations of financial institutions. Regardless of how information is shared, financial institutions and associations of financial institutions must maintain adequate procedures to protect the security and confidentiality of all information shared pursuant to section 314(b) and may only use such information for specified purposes.
- In cases where a financial institution files a SAR that has benefited from section 314(b) information sharing, FinCEN encourages financial institutions to note this in the narrative to allow FinCEN to identify and communicate specific examples of the benefits of the section 314(b) program. As discussed below, financial institutions sharing information pursuant to section 314(b) may work together to file joint SARs.
- **Can a financial institution or association of financial institutions share information related to fraud under section 314(b)?**
- Yes. Fraud offenses are SUAs for money laundering offenses. Accordingly, if a financial institution or association of financial institutions suspects that the information involves a fraud offense (or any other SUA), and the requirements for participation in section 314(b) information sharing are otherwise met, then such information sharing would be covered by the section 314(b) safe harbor. The financial institution or association of financial institutions need not have identified specific proceeds of fraud being laundered to trigger the protections of the section 314(b) safe harbor, which extends to sharing information where a financial institution "suspect[s] possible terrorist or money laundering activities," including fraud activity that may be an SUA for money laundering purposes.

314b Fact Sheet (06-12-26)

- **Can a section 314(b)-registered financial institution or association of financial institutions share information with another section 314(b)-registered financial institution or association of financial institutions, even if the entity sharing the information has no reason to believe the information relates to any specific customer, account, or transaction of the financial institution receiving the information (or, if an association of financial institutions is receiving the information, the association's member financial institutions)?**
- Yes. A financial institution or association of financial institutions may share, under section 314(b), any information that the financial institution or association of financial institutions suspects may involve possible terrorist activity or money laundering. Such information may include information that relates to any specific customer, account, or transaction of the financial institution receiving the information (or, if an association of financial institutions is receiving the information, the association's member financial institutions). Receiving financial institutions or associations of financial institutions may use such information as permitted under 31 C.F.R. § 1010.540(b)(4)(i).
- For example, such information could be shared with and used by the receiving financial institution to strengthen its anti-money laundering and countering the financing of terrorism (AML/CFT) program's capability to identify and, where appropriate, report on money laundering or terrorist activities, including by incorporating the received information into its transaction monitoring system. More generally, the receiving financial institution could use such information to comply with any of its obligations under the BSA and its implementing regulations. Notably, the regulation implementing section 314(b) contemplates that a financial institution receiving information may not have an existing relationship with an individual or entity about which it receives information and expressly permits, among other things, the use of information for the purpose of "[d]etermining whether to establish or maintain an account, or to engage in a transaction."8 Both the sharing party and the receiving party must maintain adequate procedures to protect the information's security and confidentiality as required under 31 C.F.R. § 1010.540(b)(4)(ii).

314b Fact Sheet (06-12-26)

- **What are the benefits of information sharing under section 314(b)?**
- The section 314(b) program helps financial institutions improve detection of money laundering and terrorist financing and generally enhances their AML/CFT programs. For example, financial institutions can use the section 314(b) program to:
- Share information about fraud and consumer scams and other crimes that occur rapidly and are often carried out by repeat actors who move across financial institutions to evade detection.
- Alert other participating financial institutions to customers of whose suspicious activities they may not previously have been aware.
- Alert other participating financial institutions in real time to transactions that may be connected to money laundering or terrorist financing.
- **Do section 314(b) and its implementing regulations specify the method by which information must be shared?**
- No. Provided that information sharing is consistent with the use and security of information requirements contained in 31 C.F.R. § 1010.540(b)(4), neither section 314(b) nor FinCEN’s implementing regulations specify the method by which information must be shared. As discussed above, financial institutions and associations of financial institutions may, for example, share information in writing or verbally, or they may use electronic platforms. Similarly, financial institutions and associations of financial institutions may share information in real time as activity is occurring.

314b Fact Sheet (06-12-26)

- **Can a financial institution or association of financial institutions share information with a foreign financial institution, such as a foreign affiliate or subsidiary?**
- It depends. As applicable to section 314(b), FinCEN's implementing regulations define "financial institution" as any financial institution described in 31 U.S.C. § 5312(a)(2) that is required under 31 C.F.R. Chapter X to establish and maintain an anti-money laundering program or that is treated under 31 C.F.R. Chapter X as having satisfied the requirements of 31 U.S.C. § 5318(h)(1).
- Where a financial institution has received information pursuant to section 314(b), such information may be shared with a foreign financial institution, such as a foreign affiliate or subsidiary, solely for the purposes identified in 31 C.F.R. § 1010.540(b)(4). Such sharing would not be afforded the safe harbor from liability described in 31 C.F.R. § 1010.540(b)(5) unless the receiving institution is a financial institution as defined at 31 C.F.R. § 1010.540(a)(1)(i). Furthermore, financial institutions should consider any relevant obligations arising under other U.S. legal authorities (including, but not limited to, the Right to Financial Privacy Act, the Gramm-Leach-Bliley Act, or state laws) and, as applicable, aspects of or obligations arising under foreign law, all of which are outside the scope of this guidance.

BSA Odds and Ends

- FinCEN updates MN GTO FAQs 4/9/26

  [Minnesota Fraud GTO FAQs]

- FinCEN issued year in review 4/16/26

  [FinCEN Year In Review | FinCEN.gov]

- FinCEN reissues FAQs on beneficial ownership to combine all FAQs and add Exceptive Relief Order 5/6/26

  [CDD Rule Consolidated FAQs]

- Government Accountability Office says Treasury should address gaps in beneficial ownership rules 5/29/26

  [Corporate Transparency: Treasury Should Address Gaps in Ownership Information Resulting from Expanded Exemptions | U.S. GAO]

Loans

Regulation B final rule disparate impact (04-22-26)

- **SUMMARY:** The Consumer Financial Protection Bureau (Bureau or CFPB) is issuing a final rule that amends provisions related to disparate impact, discouragement of applicants or prospective applicants, and special purpose credit programs under Regulation B, the regulation implementing the Equal Credit Opportunity Act (ECOA or Act). The amendments facilitate compliance with ECOA by clarifying the obligations imposed by the statute.
- **DATES:** This final rule is effective July 21, 2026.
- The Bureau now finalizes the rule as proposed. The Bureau's final rule provides that ECOA does not authorize disparate-impact liability (effects test), further defines discouragement, and adds prohibitions and conditions for SPCPs.
- The Bureau received approximately 64,500 comments in response to the proposed rule. A majority of those comments, including individual commenters, consumer advocate commenters, policy group commenters, State Attorneys General commenters, and Members of Congress, opposed the proposed rule. Several commenters stated that the proposed rule is deficient under the Administrative Procedure Act.
- Some commenters argued that the proposed rule is arbitrary and capricious because after fifty years of the current rule, the Bureau did not provide the required explanation for the significant change in the current rule. Furthermore, the 30-day comment period over the Thanksgiving holiday did not provide a meaningful opportunity to comment on a rule of this significance, according to these commenters. These commenters also stated that the Bureau is exceeding its rulemaking authority with this rule, and that the proposed rule conflicts with ECOA. They also asserted that the proposed rule is inconsistent with ECOA's legislative history and case law.

Regulation B final rule disparate impact (04-22-26)

- As a result, the Bureau is deleting language in § 002.6(a) and its accompanying commentary indicating that disparate-impact liability, which is referred to in the rule as the "effects test," may be applicable under ECOA, and adding language stating that the Act does not recognize the "effects test.‘’ The Bureau is also deleting the language in comment 2(p)-4 referring to the "effects test.“
- Current comment 6(a)-2 explains the effects test and states that the Act and regulation may prohibit a creditor practice that is discriminatory in effect because it has a disproportionately negative impact on a prohibited basis, even though the creditor has no intent to discriminate and the practice appears neutral on its face, unless the creditor practice meets a legitimate business need that cannot reasonably be achieved as well by means that are less disparate in their impact. The comment also provides an example. The Bureau is deleting the current text of comment 6(a)-2 for the reasons explained above and adding a new title "Disparate treatment" and new language providing as follows: The Act prohibits practices that discriminate on a prohibited basis regarding any aspect of a credit transaction. The Act does not provide for the prohibition of practices that are facially neutral as to prohibited bases, except to the extent that facially neutral criteria function as proxies for protected characteristics designed or applied with the intention of advantaging or disadvantaging individuals based on protected characteristics.

Regulation B final rule disparate impact (04-22-26)

- Section 1002.2(p)-Definition of Empirically Derived and Other Credit Scoring Systems
- Current comment 2(p)-4 to the definition of empirically derived and other credit scoring system is entitled "Effects test and disparate treatment.“ The comment states that neutral factors used in credit scoring systems could nonetheless be subject to challenge under the effects test and refers to comment 6(a)-2 for a discussion of the effects test. For the reasons discussed above, the Bureau is deleting "effects test" from the title and deleting the sentence discussing the effects test and the reference to comment 6(a)-2.
- The Bureau has determined that the inclusion of the phrase "acts or practices" in comment 4(b)-1 has resulted in§ 1002.4(b) being interpreted overly broadly to apply to business practices that, though they may have some communicative effect, do not reflect the circumvention or evasion of ECOA's prohibition against discrimination that the discouragement provision was designed to address. Such practices include, for example, business decisions about where to locate branch offices, where to advertise, or where to engage with the community through open houses or similar events. In the Bureau's view, such practices do not constitute "oral or written statements“ to applicants or prospective applicants within the meaning of§ 1002.4(b) and do not, in and of themselves, demonstrate prohibited discouragement.

Regulation B final rule disparate impact (04-22-26)

- New § 1002.8(b)(3)-Prohibited Common Characteristics
- The Bureau adopts new§ 1002.B(b)(3), which prohibits an SPCP offered or participated in by a for-profit organization from using the common characteristic of race, color, national origin, or sex, or any combination thereof, as a factor in determining eligibility for the program. For the reasons discussed above, the Bureau has determined that it is no longer necessary (in light of changed circumstances) or appropriate (in light of ECOA's purpose of preventing discrimination) for the SPCP standards in Regulation B to permit such SPCPs to use the common characteristics of race, color, national origin, or sex as eligibility criteria.

Regulation B final rule disparate impact (04-22-26)

- **§ 1002.4 General rules.**
- (b) *Discouragement.* A creditor shall not make any oral or written statement, in advertising or otherwise, directed at applicants or prospective applicants that the creditor knows or should know would cause a reasonable person to believe that the creditor would deny, or would grant on less favorable terms, a credit application by the applicant or prospective applicant because of the applicant or prospective applicant's prohibited basis characteristic(s). For purposes of this paragraph (b), oral or written statements are spoken or written words, or visual images such as symbols, photographs, or videos.
- (a) *General rule concerning use of information*. Except as otherwise provided in the Act and this part, a creditor may consider any information obtained, so long as the information is not used to discriminate against an applicant on a prohibited basis. The Act does not provide that the "effects test" applies for determining whether there is discrimination in violation of the Act.
- (3) *Prohibited common characteristics*. A special purpose credit program described in paragraph (a)(3) of this section shall not use the race, color, national origin, or sex, or any combination thereof, of the applicant, as a common characteristic or factor in determining eligibility for the program.

Regulation B final rule disparate impact (04-22-26)

- (4) Otherwise prohibited bases in for-profit programs. Subject to paragraph (b)(3) of this section, a special purpose credit program described in paragraph (a)(3) of this section may require its participants to share one or more common characteristics that would otherwise be a prohibited basis only if the for-profit organization provides evidence for each participant who receives credit through the program that in the absence of the program the participant would not receive such credit as a result of those specific characteristics.
- 4. *Disparate treatment*. An empirically derived, demonstrably and statistically sound, credit scoring system may include age as a predictive factor (provided that the age of an elderly applicant is not assigned a negative factor or value). Besides age, no other prohibited basis may be used as a variable. Generally, credit scoring systems treat all applicants objectively and thus avoid problems of disparate treatment. In cases where a credit scoring system is used in conjunction with individual discretion, disparate treatment could conceivably occur in the evaluation process.
- For purposes of§ 1002.4(b), encouraging statements directed at one group of consumers cannot discourage other consumers who were not the intended recipients of the statements.

Regulation B final rule disparate impact (04-22-26)

- i. Statements prohibited by § 1002.4(b) include:
- A. A statement that the applicant should not bother to apply, after the applicant states that he is retired.
- B. Statements directed at the general public that express a discriminatory preference or a policy of exclusion against consumers based on one or more prohibited basis characteristics in violation of the Act.
- C. The use of interview scripts that discourage applications on a prohibited basis.
- ii. Statements not prohibited by § 1002.4(b) include:
- A. Statements directed at one group of consumers, encouraging that group of consumers to apply for credit.
- B. Statements in support of local law enforcement.
- C. Statements recommending that, before buying a home in a particular neighborhood, consumers investigate, for example, the neighborhood's schools, its proximity to grocery stores, and its crime statistics.
- D. Statements encouraging consumers to seek out resources to develop their financial literacy.

Regulation B final rule disparate impact (04-22-26)

- 2. *Disparate treatment*. The Act prohibits practices that discriminate on a prohibited basis regarding any aspect of a credit transaction. The Act does not provide for the prohibition of practices that are facially neutral as to prohibited bases, except to the extent that facially neutral criteria function as proxies for protected characteristics designed or applied with the intention of advantaging or disadvantaging individuals based on protected characteristics.

Consumer groups sue CFPB over Regulation B final rule (04-22-26)

- Case No. 1:26-cv-01820
- COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF
- This case challenges a Final Rule issued on April 22, 2026, by the Consumer Financial Protection Bureau ("CFPB") to amend Regulation B, 12 C.F.R. Part 1002, the implementing regulation of the Equal Credit Opportunity Act ("ECOA"). See Final Rule, Equal Credit Opportunity Act (Regulation B), 91 Fed. Reg. 21620-01 (Apr. 22, 2026) ("Final Rule").
- The Final Rule does not reflect reasoned decision-making or an expert, good-faith effort to implement our nation's foundational credit antidiscrimination statute. Quite the opposite: The Final Rule is a drastic turn, without justification, from the CFPB's (and its Federal Reserve Board predecessor's) longstanding interpretation and enforcement of key ECOA provisions. Indeed, the CFPB acknowledges that the amendments are likely to increase credit discrimination, the very thing the statute is designed to prevent.
- The Final Rule is arbitrary and capricious by any measure. To start, the CFPB failed to identify any concrete problem with the current regulatory regime. The CFPB relied on conclusory assertions and speculation, not evidence, to justify its dramatic departure from decades of settled ECOA implementation. The CFPB's approach is at odds with the available evidence: As commenters to the proposed rule made clear, public data and research—much of it from the CFPB itself—show that the Final Rule is ill-conceived and likely to harm covered entities and consumers alike.

Consumer groups sue CFPB over Regulation B final rule (04-22-26)

- The CFPB's purported cost-benefit analysis, which is required under the Dodd- Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"), independently renders the Final Rule arbitrary and capricious. The CFPB's asserted benefits rest on unsupported generalizations and assumptions, while the CFPB gives the back of the hand to the documented costs that the Final Rule will exact on covered entities, consumers, and small businesses. The CFPB's simplistic references to general principles of economic theory, free- floating hypotheses about potential outcomes, and disregard of hard facts are not actual "analysis" and, thus, do not satisfy the requirements of the Dodd-Frank Act.
- The CFPB's rulemaking process was also flawed. The CFPB issued the Notice of Proposed Rulemaking ("NPRM") without undertaking an Initial Regulatory Flexibility Analysis and without convening a Small Business Regulatory Enforcement Fairness Act panel, as required by the Small Business Regulatory Enforcement Fairness Act of 1996. The NPRM provided just thirty-two days for comments, limiting commenters' ability to compile and provide evidence concerning the rule, and the CFPB refused requests to extend the deadline. While that would have been a needlessly compressed comment period under any circumstance, the thirty-two days here encompassed the Thanksgiving holiday and ran parallel to the comment period that the CFPB set for a simultaneous proposal to overhaul implementation of a separate section of ECOA—a proposal in which Plaintiffs and many other commenters also have a significant interest. The CFPB then failed to conduct a Final Regulatory Flexibility Analysis, and, although the Final Rule acknowledged many comments, it failed to respond to significant comments or simply asserted it was not persuaded, without giving a reasoned explanation.

Consumer groups sue CFPB over Regulation B final rule (04-22-26)

- On top of that, Mr. Vought does not have lawful authority to serve as Director of the CFPB and, thus, the CFPB cannot issue rules under his purported authority.
- Plaintiffs accordingly seek to vacate the Final Rule under the Administrative Procedure Act ("APA"), 5 U.S.C. § 706(2), as arbitrary, capricious, not in accordance with law, without observance of procedure required by law, and in excess of statutory authority. The Rule should also be vacated because actions directed by Mr. Vought are ultra vires.

1071 Final Rule (05-01-26)

- **SUMMARY:** The Consumer Financial Protection Bureau (Bureau or CFPB) is revising certain provisions of Regulation B, subpart B, which implements changes to the Equal Credit Opportunity Act made by section 1071 of the Dodd Frank Wall Street Reform and Consumer Protection Act. The Bureau is amending coverage of certain credit transactions and financial institutions; the small business definition; inclusion of certain data points and how others are collected; and the compliance date.
- **DATES:** This final rule is effective on June 30, 2026. The compliance date for the rule is January 1, 2028.
- The Bureau has determined that a potentially long-term data collection regime should start with a focus on core lending products, lenders, small businesses, and data points. The Bureau believes in retrospect that the approach it took in the 2023 final rule-a broad initial coverage of lenders, products, small businesses and data points-was not conducive to the long-term success of the data collection regime under section 1071. The Bureau now finds that a better, longer-term approach to advance the statutory purposes of section 1071 is to commence the collection of data with a narrower scope to ensure its quality, and to limit, as much as possible, any disturbance of the provision of credit to small businesses.

1071 Final Rule (05-01-26)

- *Covered credit transactions.* The Bureau concludes that the initial iterations of data collection under the rule should focus on the core, widely used lending products most likely to be foundational to small businesses' formation and operation. This final rule therefore excludes merchant cash advances (MCAs), agricultural lending, and small dollar loans from the definition of covered credit transaction.
- *Covered financial institutions*. The Bureau concludes that the initial iterations of data collection under the rule should focus on larger core lenders. This final rule therefore contains two changes to the covered financial institution definition: first, to exclude FCS lenders from coverage; and second, to raise the origination threshold from 100 to 1,000 covered credit transactions for each of two consecutive years. This final rule also contains conforming changes to the bona fide error portions of the enforcement provisions in the rule.
- *Small business*. The Bureau concludes that the focus of the rule, at least initially, should be truly small businesses. This final rule therefore changes the gross annual revenue threshold in the rule's definition of small business from $5 million or less to $1 million or less.

1071 Final Rule (05-01-26)

- This final rule therefore focuses data collection on data points specifically identified in section 1071 and a limited number of other data points needed to facilitate the collection of these statutory data points. This final rule removes the discretionary data points for application method, application recipient, denial reasons, pricing information, and number of workers. This final rule also contains changes to better conform with an executive branch mandate, resulting in modifications to the collection of data concerning business ownership status of small business applicants and to the format of demographic data collected concerning the principal owners of a small business.
- *Compliance dates*. Finally, in light of the changes to the rule, this final rule extends the compliance date to January 1, 2028, for all financial institutions that remain covered by the rule. This final rule also adds certain special transitions rules to provide flexibility to potentially covered financial institutions.
- *Privacy and data publication*. The Bureau does not address in this final rule the privacy discussions in the 2023 final rule or its statements about the eventual publication of data. The 2023 final rule did not purport to make any final or binding decisions concerning its privacy analysis, instead announcing only its "preliminary assessment of how it might appropriately assess and advance privacy interests by means of selective deletion or modification" of data. The 2023 final rule also did not reach conclusions regarding the procedural vehicle it would use to convey its decisions with respect to privacy. Nor has the Bureau conclusively announced a timeline for the publication of application-level data, except for observing that it would need a full year's worth of data to conduct the necessary privacy analysis.

1071 Final Rule (05-01-26)

- The Bureau is currently reconsidering all of these issues and preliminary findings and will continue to engage with stakeholders. The Bureau commits to addressing these issues and findings in a notice of proposed rulemaking to be published likely after the collection of the first year's worth of data. As set out in detail below, the Bureau believes that a full notice-and comment rulemaking would best inform the Bureau on its privacy assessment, including which modifications and deletions to make.
- *Grace period*. The Bureau is retaining and updating the grace period articulated in the final rule, for the 2023 same reasons set out in that notice and as set out in subsequent extensions of the compliance dates. The grace period is now from January 1, 2028, through December 31, 2028, to align with the new single initial compliance date of January 1, 2028.
- The Bureau is adopting revisions to the "time and manner" provisions in § 1002.107(c), as discussed in detail below. Specifically, this final rule amends the provision concerning the timing and manner of the collection of demographic data, clarifying that such collection may take place in certain situations even after a credit decision is made on an application. This flexibility allows indirect lenders to avoid adding complexity to point-of-sale interactions and eliminates the need for dealers or vendors to collect the data on the lender's behalf. Furthermore, because the rule permits this post-decision collection, financial institutions can gather the required information directly from the applicant at a later time, ensuring that the process does not delay or interrupt the underlying commercial sale. Consequently, the Bureau believes
- that these modifications to the data collection procedures largely resolve the operational challenges cited by commenters, rendering a categorical exclusion for these products unnecessary.

1071 Final Rule (05-01-26)

- When requesting minority-owned and women owned business statuses from an applicant, the financial institution shall inform the applicant that the financial institution cannot discriminate on the basis of minority-owned or women owned business statuses, or on whether the applicant provides this information. The financial institution must also inform the applicant of its right to refuse to provide this information.
- The ethnicity, race, and sex of the applicant's principal owners. When requesting ethnicity, race, and sex information from an applicant, the financial institution shall inform the applicant that the financial institution cannot discriminate on the basis of a principal owner's ethnicity, race, or sex, or on whether the applicant provides this information. The financial institution must also inform the applicant of its right to refuse to provide this information.
- (b) *Prohibition on access to certain information*. Unless the exception under paragraph (c) of this section applies, an employee or officer of a covered financial institution or a covered financial institution's affiliate shall not have access to an applicant's responses to inquiries that the financial institution makes pursuant to this subpart regarding whether the applicant is a minority-owned business or a women owned business under § 1002.107(a)(18), and regarding the ethnicity, race, and sex of the applicant's principal owners under § 1002.107(a)(19), if that employee or officer is involved in making any determination concerning that applicant's covered application.

1071 Final Rule (05-01-26)

ProSight™

- (b) *Certain information kept separate from the rest of the application*. A financial institution shall maintain, separately from the rest of the application and accompanying information, an applicant's responses to the financial institution's inquiries pursuant to this subpart regarding whether an applicant for a covered credit transaction is a minority-owned business and/or a women-owned business under§ 1002.107(a)(18), and regarding the ethnicity, race, and sex of the applicant's principal owners under § 1002.107(a)(19).
- *Special transitional rules--(1) Collection of certain information prior to the compliance date*. A financial institution that reasonably anticipates being a covered financial institution as described in paragraph (b)(l) of this section is permitted, but not required, to collect information regarding whether an applicant for a covered credit transaction is a minority-owned business and/or a women-owned business under§ 1002.107(a)(18), and the ethnicity, race, and sex of the applicant's principal owners under § 1002.107(a)(19) beginning 12 months prior to the compliance date as set forth in paragraph (b)(l) of this section.
- A financial institution that is unable to determine the number of covered credit transactions it originated for small businesses in each of calendar years 2026 and 2027 for purposes of determining its compliance date pursuant to paragraph of this section, (b) because for some or all of this period it does not have readily accessible the information needed to determine whether its covered credit transactions were originated for small businesses as defined in§ 1002.106(b), is permitted to use any reasonable method to estimate its originations to small businesses for either or both of the calendar years 2026 and 2027.
- *Alternative time period for determining compliance dates*. A financial institution is permitted to use its originations of covered credit transactions in each of calendar years 2025 and 2026 in lieu of calendar years 2026 and 2027 as specified in paragraphs (b) and (c)(2) of this section.

1071 Final Rule (05-01-26)

- **Sample data collection form**
- Federal law requires that we request the following information to help ensure that all small businesses applying for loans and other kinds of credit are treated fairly and that communities' small business credit needs are met.
- One or more employees or officers involved in making a determination concerning your application may have access to the information provided on this form. However, **FEDERAL LAW PROHIBITS DISCRIMINATION** on the basis of your answers on this form. Additionally, we cannot discriminate on the basis of whether you provide this information.
- Information about your application (without your name or other directly identifying information) may eventually be available to the public. Though filling out this form will help to ensure that all small business owners are treated fairly, **YOU ARE NOT REQUIRED TO PROVIDE THIS INFORMATION**.

1071 Final Rule (05-01-26)

Business ownership status

Please indicate the business ownership status of your small business. For the purposes of this form, your business is a minority-owned or women-owned business if one or more minorities* or women (i) directly or indirectly own or control more than 50 percent of the business AND (ii) receive more than 50 percent of the net profits/losses of the business.

What is your business ownership status? *(Check one or more)*

- ☐ **I do not wish to provide this information**
- ☐ **Minority-owned business**
- ☐ **Women-owned business**
- ☐ **None of these apply**

**Minority means Hispanic or Latino, American Indian or Alaska Native, Asian, Black or African American, or Native Hawaiian or Other Pacific Islander. A multi-racial or muti-ethnic individual is a minority for this purpose.*

Number of principal owners

For purposes of this form, a principal owner is any individual who owns 25 percent or more of the equity interest of a business. A business might not have any principal owners if, for example, it is not directly owned by any individuals (i.e., if it is owned by another entity or entities) or if no individual directly owns at least 25 percent of the business.

How many principal owners does your business have? *(Check one)*

- ☐ **0**
- ☐ **1**
- ☐ **2**
- ☐ **3**
- ☐ **4**

1071 Final Rule (05-01-26)

- As a reminder, **APPLICANTS ARE NOT REQUIRED TO PROVIDE THIS INFORMATION.** We cannot discriminate on the basis of any person's ethnicity, race, or sex. Further, we cannot discriminate on the basis of whether you provide this information. **PLEASE FILL OUT ONE SHEET FOR EACH PRINCIPAL OWNER.**

---

1. What is your ethnicity?
(Check only one)

- ☐ I do not wish to provide my ethnicity
- ☐ Hispanic or Latino
- ☐ Not Hispanic or Latino

---

2. What is your race?
(Check one or more)

- ☐ I do not wish to provide my race
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☐ White

---

3. What is your sex?
(Check only one)

- ☐ I do not wish to provide my sex
- ☐ Male
- ☐ Female

1071 Final Rule (05-01-26)

- The size of the random sample, under column B, shall depend on the size of the financial institution's small business lending application register, as shown in column A of table 1 to this appendix.
- The thresholds in column C of table 1 to this appendix reflect the number of unintentional errors a financial institution may make within a particular data field (e.g., the credit product data field within the credit type data point or the sex data field for a particular principal owner within the ethnicity, race, and sex of principal owners data point) in a small business lending application register that would be deemed bona fide errors for purposes of § 1002.112(b).
- For instance, a financial institution that submitted a small business lending application register containing 11,000 applications would be subject to a threshold of four errors per data field. If the financial institution had made two errors in reporting loan amount and two errors reporting gross annual income, all of these errors would be covered by the bona fide error provision of § 1002.llZ(b) and would not constitute a violation of the Act or this part.

TABLE 1 TO APPENDIX F—TOLERANCE THRESHOLDS FOR BONA FIDE ERRORS

Small business lending application register count (A)	Random sample size (B)	Threshold (#) (C)	Threshold (%) (D)
1,000–100,000	79	4	5.1
100,001+	159	4	2.5

1071 Final Rule (05-01-26)

ProSight™

- *ii. Remove 107(a)(3) Application Method and 107(a)(4) Application Recipient;*
- *iv. Remove 107(a)(11) Denial Reasons, 107(a)(12) Pricing Information, 107(a)(12)(i) Interest Rate, 107(a)(12)(ii) Total Origination Charges, 107(a)(12)(iii) Broker Fees, 107(a)(12)(iv) Initial Annual Charges, 107(a)(12)(v) Additional Cost for Merchant Cash Advances or Other Sales-Based Financing, 107(a)(12)(vi) Prepayment Penalties, and 107(a)(16) Number of Workers;*
- *vii. Remove 107(c)(3) Procedures To Monitor Compliance and 107(c)(4) Low Response Rates;*

OCC final rule escrow accounts (05-15-26)

- The OCC is issuing a final rule to codify longstanding and recognized powers of national banks and Federal savings associations (collectively, banks) to establish or maintain real estate lending escrow accounts and to exercise flexibility in making business judgments as to the terms and conditions of such accounts, including whether and to what extent to offer any compensation or to assess any fees related thereto.
- The terms and conditions of escrow accounts, including whether and to what extent banks pay interest or other compensation, are ultimately a business judgment made by each bank in accordance with safe and sound banking principles. This discretion ensures that banks have the flexibility to make business decisions about how to effectively and efficiently set the terms and conditions of their escrow accounts, which allows banks to appropriately balance the costs and benefits of these accounts and the risks and rewards of real estate lending more generally. As such, it is a core component of banks' mortgage lending powers under applicable law, including provisions of the Federal Reserve Act, the Home Owners' Loan Act of 1933 (HOLA) and the National Bank Act. This is consistent with longstanding agency precedent and bank practices, which the OCC is codifying in its regulations governing the mortgage lending powers of national banks and Federal savings associations, respectively, for the sake of clarity.
- This final rule will also complement the OCC's preemption determination, which it is concurrently finalizing along with this final rule, related to State laws that restrict banks' flexibility to decide whether and to what extent to pay interest or other compensation on funds placed in escrow accounts or assess related fees.

OCC final rule escrow accounts (05-15-26)

ProSight™

- **§ 34.2 Definitions**.
- (b*) Escrow account* means an account established in connection with a loan or extension of credit secured by a lien on interest in real estate in which the borrower places funds for the purpose of assuring payment of taxes, insurance premiums, or other charges with respect to the property.
- **§ 34.3 General Rule**
- (d) National banks may establish or maintain escrow accounts. The terms and conditions of any such escrow account, including the investment of escrowed funds, fees assessed for the provision of such accounts, or whether and to what extent interest or other compensation is calculated and paid to customers whose funds are placed in the escrow account, are business decisions to be made by each national bank in its discretion.
- **§ 160.3 Definitions**.
- *Escrow account* means an account established in connection with a real estate loan in which the borrower places funds for the purpose of assuring payment of taxes, insurance premiums, or other charges with respect to the property.
- **§ 160.30 General lending and investment powers of Federal savings associations.**
- (b) Federal savings associations may establish or maintain escrow accounts. The terms and conditions of any such escrow account, including the investment of escrowed funds, fees assessed for the provision of such accounts, or whether and to what extent interest or other compensation is calculated and paid to customers whose funds are placed in the escrow account, are business decisions to be made by each Federal savings association in its discretion.

OCC Preemption Determination: State Interest-on-Escrow Laws(05-15-26)

- The OCC is issuing a preemption determination concluding that Federal law preempts State laws that restrict OCC-regulated banks' flexibility to decide whether and to what extent to (1) pay interest or other compensation on funds placed in real estate escrow accounts; or (2) assess fees in connection with such accounts. This preemption determination will provide much-needed clarity to banks and other stakeholders.
- **§ 34.7 OCC Preemption Determinations**
- (a*) Purpose*. This section codifies preemption determinations issued by the Office of the Comptroller of the Currency.
- (b) *Escrow*. The OCC has determined that Federal law preempts State laws that restrict a national bank's or Federal savings association's flexibility to decide whether and to what extent to pay interest or other compensation on funds placed in escrow accounts or assess fees for such accounts, including the following State laws:

  (1) California: Cal. Civ. Code sec. 2954.8;

  (2) Connecticut: Conn. Gen. Stat. sec. 49-2a;

  (3) Guam: 11 Guam Code Ann. sec. 106103;

  (4) Maine: Me. Rev. Stat. Ann. tit. 9-B, sec. 429; Me. Rev. Stat. Ann. tit. 33, sec. 504;

OCC Preemption Determination: State Interest-on-Escrow Laws(05-15-26)

(5) Maryland: Md. Code Ann., Com. Law secs. 12-109, 12-109.2;

(6) Massachusetts: Mass. Gen. L. ch. 183, sec. 61;

(7) Minnesota: Minn. Stat. Ann. sec. 47.20, subd. 9;

(8) New York: N.Y. Gen. Oblig. Law sec. 5-601;

(9) Oregon: Or. Rev. Stat. secs. 86.245, 86.250;

(10) Rhode Island: 19 R.I. Gen. Laws sec. 19-9-2;

(11) United States Virgin Islands: V.I. Code tit. 9, sec. 67;

(12) Utah: Utah Code Ann. sec. 7-17-3;

(13) Vermont: Vt. Stat. Ann. tit. 8, sec. 10404; and

(14) Wisconsin: Wis. Stat. secs. 138.051, 138.052.

Statement on ability to repay and immigration status (06-08-26)

ProSight™

- **SUMMARY:** The Consumer Financial Protection Bureau (Bureau or CFPB) is issuing this statement to remind creditors of their obligations under the Truth in Lending Act (TILA) as implemented by Regulation Z, and consistent with Executive Order 14406, titled "Restoring Integrity to America's Financial System.“
- **DATES:** This statement is applicable on June 8, 2026.
- The Truth in Lending Act and its implementing Regulation Z require creditors to assess consumers' ability to repay before offering mortgages and certain open-end credit products. This statement emphasizes to creditors that these requirements may obligate consideration of a consumer's immigration status, especially where removal from the United States may disrupt the consumer's income.
- In making lending decisions, creditors are permitted to take into account a wide range of information in order to make a reasonable assessment of a consumer's ability to repay. Regulation B, which implements the Equal Credit Opportunity Act (ECOA), expressly states that "[a] creditor may take the applicant's immigration status into account,“ and that a creditor "may consider the applicant's immigration status or status as a permanent resident of the United States, and any additional information that may be necessary to ascertain the creditor's rights and remedies regarding repayment.“ Such a consideration may be necessary because an "applicant's immigration status and ties to the community (such as employment and continued residence in the area) could have a bearing on a creditor's ability to obtain repayment.“ As the Bureau recently explained, "[a] credit applicant's immigration or citizenship status may present underwriting risks that typical assessments of financial capacity alone will not fully resolve. As Regulation B acknowledges, this is something creditors may legitimately consider."

Statement on ability to repay and immigration status (06-08-26)

- To the extent a creditor's information regarding the borrower's immigration status indicates that the borrower may be an unlawfully present individual and removed from the United States, there is a danger that removal would render any such borrower unable to earn income derived from employment that requires physical presence in the United States. Accordingly, considering whether information regarding an applicant's immigration status indicates a reasonably expected change in future income is a matter of sound compliance practice. The Bureau expects compliance with the law and failure to account for such a reasonably expected change in income may not comply with a creditor's obligation to reasonably assess a borrower's ability to repay the loan or line of credit sought.
- Of course, there are a wide variety of lawful immigration statuses in the United States. Assessing how each status might bear on a lender's reasonable expectation that a consumer has the ability to repay an obligation with U.S.-based employment income is varied, and it cannot be assumed that consumers with different lawful statuses have identical abilities to repay. Accordingly, the Bureau cannot, and does not, provide a comprehensive analysis of variations in immigration status and the consequent reasonable expectations as to a consumer's ability to repay a loan through expected income from U.S.-based employment. Rather, the Bureau reminds creditors when future changes in borrower income must be considered under Regulation Z.
- Regulation Z enables lenders to make these judgments by affirming their ability to lawfully consider the consumer's immigration status, lawful presence, authorization to work, and other factors that may indicate risk of removal insofar as it bears on their current or reasonably expected income from U.S.-based employment.

CFPB Advisory Opinion rescinded on Regulation B SPCPs (06-17-26)

- **SUMMARY:** The Consumer Financial Protection Bureau (Bureau) is rescinding an advisory opinion issued in December regarding Regulation B, which 2020 implements the Equal Credit Opportunity Act (ECOA), as it applies to certain aspects of special purpose credit programs designed and implemented by for-profit organizations to meet special social needs.
- **DATES:** The advisory opinion is rescinded on June 17, 2026.
- On December 21, the Bureau issued an advisory 2020, opinion entitled "Equal Credit Opportunity (Regulation B); Special Purpose Credit Programs" (the advisory opinion) to address regulatory uncertainty regarding Regulation B, which implements ECOA, as it applies to certain aspects of SPCPs designed and implemented by for-profit organizations to meet special social needs.
- Specifically, the advisory opinion clarified the content that a for-profit organization must include in a written plan that establishes and administers an SPCP under Regulation B. In addition, the advisory opinion clarified the type of research and data that may be appropriate to inform a for-profit organization's determination that an SPCP is needed to benefit a certain class of persons.

CFPB Advisory Opinion rescinded on Regulation B SPCPs (06-17-26)

- In April 2026, the Bureau issued a final rule amending provisions related to, inter alia, SPCPs under Regulation B. The advisory opinion, however, contains statements that conflict with these recent amendments to Regulation B. As one example, the advisory opinion states that all program participants in an SPCP offered or participated in by a for profit organization may be required "to share one or more common characteristics (for example, race, national origin, or sex)"; the April 6 2026 final rule, however, prohibits any SPCP offered or participated in by a for profit organization from using the common characteristic of race, color, national origin, or sex, or any combination thereof, as a factor in determining eligibility for the program. In addition, the advisory opinion addresses SPCP provisions under Regulation B that have since been amended, rendering those discussions out-of-date or, at best, incomplete. The Bureau now hereby rescinds the advisory opinion. This rescission is intended to avoid any confusion about the appropriate standards and related conditions for SPCPs offered or participated in by for-profit organizations.

Loans Odds and Ends

- HUD Notification of Withdrawal of Fair Housing and Equal Opportunity Guidance Documents 4/6/26

  Federal Register :: Notification of Withdrawal of Fair Housing and Equal Opportunity Guidance Documents

Deposits

FDIC Rescinds Supervisory Guidance on Multiple Re-Presentment NSF Fees (04-10-26)

- On June 16, 2023, the FDIC issued a Financial Institution Letter (FIL-32-2023) titled FDIC Clarifying Supervisory Approach Regarding Supervisory Guidance on Multiple Re-Presentment NSF Fees (https://www.fdic.gov/news/inactive-financial-institution-letters/2023/fdic-clarifying-supervisory-approach-regarding-supervisory). This guidance described the FDIC's supervisory approach relating to supervised institutions assessing multiple non-sufficient funds (NSF) fees arising from the re-presentment of the same unpaid transaction. The FDIC is rescinding FIL-32-2023 effective immediately.
- Highlights:
- On June 16, 2023, the FDIC issued FIL-32-2023, which rescinded and replaced FIL-40-2022, entitled "Supervisory Guidance on Multiple Re-Presentment NSF Fees."
- Based on a review and assessment of the guidance in FIL-32-2023, the FDIC concludes that the guidance is overly broad in scope and has raised uncertainty regarding when, for instance, disclosures regarding re-presentments may result in "unfairness" concerns under Section 5 of the Federal Trade Commission Act.
- As a result, the FDIC is rescinding FIL-32-2023 effective immediately.
- Supervised institutions should ensure their disclosures to consumers accurately reflect their practices and are provided in accordance with applicable laws, regulations, and other current legal requirements.

Deposit Odds and Ends

- FDIC updates FAQs covering official sign rules Part 328 Final Rule 5/12/26.
  [Questions and Answers Related to the FDIC’s Part 328 Final Rule | FDIC.gov]

Miscellaneous

CCO Issue 1 2026 (04-01-26)

- Although the FDPA was enacted more than 50 years ago, violations of its requirements regularly appear in the Federal Reserve's list of top-cited compliance violations. The other federal regulatory agencies that enforce the FDPA also frequently cite these violations. A review of 2024 examination data of state member banks, for which the Federal Reserve is the primary federal regulator, listed the following top-cited violations of Regulation H, the Federal Reserve's FDPA implementing regulation:
  - Originating designated loans with an insufficient amount of insurance
  - Failing to provide the required notice to borrowers when they apply for a designated loan
  - Failing to identify lapses in coverage and force place insurance when necessary

CCO Issue 1 2026 (04-01-26)

ProSight™

- Examiners observed that, in most instances, banks understood and complied with Regulation H expectations to require flood insurance for properties located in SFHAs. Violations were most frequently cited because of lender errors that resulted in the borrower purchasing an incorrect amount of flood insurance or in the loan being briefly uninsured post closing. The root cause of these violations was generally a combination of insufficient policies, procedures, and staff training for determining flood coverage combined with the absence of secondary reviews to ensure lenders accurately calculated the required amount and term.
- During the period from the receipt of an application to loan origination, changes may occur that affect the initial flood insurance estimates. For example, assume a loan requiring flood insurance was initially expected to close on June 30, 2025, but the closing date was subsequently changed to June 10, 2025, to accommodate the buyer. If the bank failed to ensure the policy’s effective date was changed to June 10, 2025, the loan would have been uninsured for nearly three weeks.
- Examiners observed banks failing to accurately calculate the insurable value of property covered by flood insurance, a factor in determining how much flood insurance is required and the amount that would be paid on a claim.

CCO Issue 1 2026 (04-01-26)

- Insurable value is defined as the overall value of the property securing the designated loan minus the value of the land on which the property is located. To calculate the amount of required insurance, the lender and borrower (by themselves or in consultation with the flood insurance provider or another appropriate professional) may choose from a variety of ways to establish the insurable value, including:
  - an appraisal based on the cost value, not the market value;
  - a construction-cost calculation;
  - the insurable value used in a hazard insurance policy (recognizing that adjustments may be necessary, as this value does not include the value of the foundation); or
  - any other reasonable approach that is supportable
- Examiners observed lenders choosing the incorrect amount of insurance for commercial loans when multiple properties secured the loan. Consumer Compliance Outlook (CCO) published an article in 2022 that included examples of how to calculate the proper amount of insurance when a designated loan is secured by multiple properties. See Danielle Martinage, “Commercial Flood Insurance Compliance — Washing Away Common Pitfalls,” CCO (Second Issue 2022).

CCO Issue 1 2026 (04-01-26)

- Calculation errors were attributed to:
  - insufficient understanding of flood insurance calculations at the loan officer level;
  - relying on outdated replacement cost values; and
  - absence of secondary reviews to identify lender errors.
- Banks were cited for failing to provide the required flood insurance notice under 12 C.F.R. §208.25(i) to the borrower when a loan was made, increased, renewed, or extended for real property or a mobile home in an SFHA. A model form of the notice is available in Appendix A to Regulation H.
- Lenders were cited for failing to provide the required notice “within a reasonable time.”
- The agencies generally regard 10 calendar days as a “reasonable” time interval.
- In several instances, banks were cited under 12 C.F.R. 208.25(g) because examiners noted flood insurance had lapsed on designated loans for longer than the regulation permits, and the bank failed to force place insurance.

EFTA — REGULATION E

- Examiners found that some financial institutions were not promptly initiating error resolution investigations after the consumer notified them orally of an error, in violation of §1005.11(c).
- One common misconception is that an institution's duty to investigate an alleged error is triggered only when the consumer submits a written notice. But Comment 11(c)-2 of the Official Staff Commentary for Regulation E specifically clarifies that "a financial institution must begin its investigation promptly upon receipt of an oral notice. It may not delay until it has received a written confirmation (emphasis added)."
- Notifying Consumers of Investigation Results: Examiners observed that some financial institutions were not properly notifying consumers that errors had been corrected and that the consumer's account had been credited. If a financial institution determines an error occurred as the consumer alleged, it must provide oral or written notice within three business days after completing the investigation. If an institution determines that no error or a different error occurred, it must provide written notice within three business days.

CCO Issue 1 2026 (04-01-26)

- Examiners cited institutions for violating §1005.11(c)(2)(i), which requires an institution to provide provisional credit for the amount of the alleged error within 10 business days of receiving an error notice if the institution could not complete its investigation within 10 business days. An exception to the provisional credit requirement applies if the institution requests written confirmation of an error that was orally reported but does not receive it within 10 business days. That exception did not apply for the banks that were cited.
- Examiners also cited institutions that provisionally credited accounts but failed to provide consumers with full access to and use of the funds during the investigation.
- Examination reports indicated that some financial institutions provided the notice of provisional credit outside of regulatory time frames and without the information Regulation E requires. These violations occurred because financial institutions failed to adequately oversee the third parties responsible for fulfilling critical error resolution functions.

CCO Issue 1 2026 (04-01-26)

ProSight™

- Examiners cited institutions for failing to correct errors within one business day of completing the investigation and notifying the consumer that the investigation was complete.
- Examiners cited institutions for failing to provide sufficient written explanation of the results of an investigation, failing to provide a notice to the consumer of the right to request the documents that the institution relied on in making its determination, and failing to provide copies of the documents that it relied on in making its error determination when the consumer requested the documents.
- In some cases, the institution failed to provide an adequate explanation, using generic language, such as “no error.”
- Examination reports revealed that some financial institutions failed to notify consumers when the institutions reversed provisional credit. Additionally, some violations were caused by reliance on an inadequate notice generated by the institution’s third-party provider.
- Examiners determined that violations of §1005.11(d) were largely attributable to weaknesses in third-party risk management practices, including oversight of the functions provided by the third parties, the use of third-party templates as well as weaknesses or gaps in Regulation E staff training, policy and procedure documents, and internal controls.

CCO Issue 1 2026 (04-01-26)

- In this article, we discuss the themes and trends of the 8,355 consumer complaints the Federal Reserve received, investigated, and closed in 2024 for the institutions under its supervisory authority (Table 1).
- **COMPLAINT PRODUCTS MIX**
- Of the total complaints investigated and closed in 2024, the products receiving the highest volume of complaints were deposit accounts (57 percent), prepaid cards (25 percent), and credit cards (14 percent). All other types of bank products and services accounted for less than 10 percent of complaint volumes (see Table 2; categories are in bold).
- **2024 TOP 10 COMPLAINT CATEGORIES**
- Here are examples of the common types of complaint allegations within each category.
- ***Restricted/Blocked Accounts***
- Most complaints in this category involved prepaid cards and deposit accounts, and a high percentage of these involved mobile banking services. Consumers alleged that access to their accounts was blocked because they reported identity theft or unauthorized transactions.

CCO Issue 1 2026 (04-01-26)

ProSight™

TABLE 1: Top 10 Consumer Complaints in 2024 for State Member Banks			
	Complaint Topic	Number of Complaints	Percentage of All Complaints
1.	Restricted/Blocked Accounts	3,114	37.27
2.	Fraud/Forgery	1,307	15.64
3.	Error Resolution	926	11.08
4.	Funds Availability/Withdrawals/Unable to Access Funds	862	10.32
5.	Credit Reporting	660	7.90
6.	Fees/Terms/Rates	237	2.84
7.	Account Closures	223	2.67
8.	Applications/Account Openings	198	2.37
9.	Debt Validation	127	1.52
10.	Inability to Repay	103	1.23
Complaints in Top 10 Categories		**7,757**	**92.84**
Total Complaints		**8,355**	**100**

CCO Issue 1 2026 (04-01-26)

ProSight™

TABLE 2: Complaints Against State Member Banks and Selected Nonbank Subsidiaries of Bank Holding Companies by Product and Subject of Complaint in 2024	
Product/Subject of Complaint	**Percentage of All Complaints**
Deposit/Bank Products	**57**
Restricted/Blocked Accounts	25
Fraud/Forgery	9
Deposit Error Resolution	8
Funds Availability Not As Expected	8
Other	7
Prepaid Accounts	**25**
Restricted/Blocked Accounts	16
Error Resolution	3
Fraud/Forgery	3
Inability to Withdraw Funds on the Card	2
Other	1
Credit Card Accounts	**14**
Inaccurate Credit Reporting	5
Fraud/Forgery	4
Request to Validate the Debt Owed	1
Other	4
Nondeposit/Bank Services	**2**
Other Products	**1**
Real Estate Loans	**1**

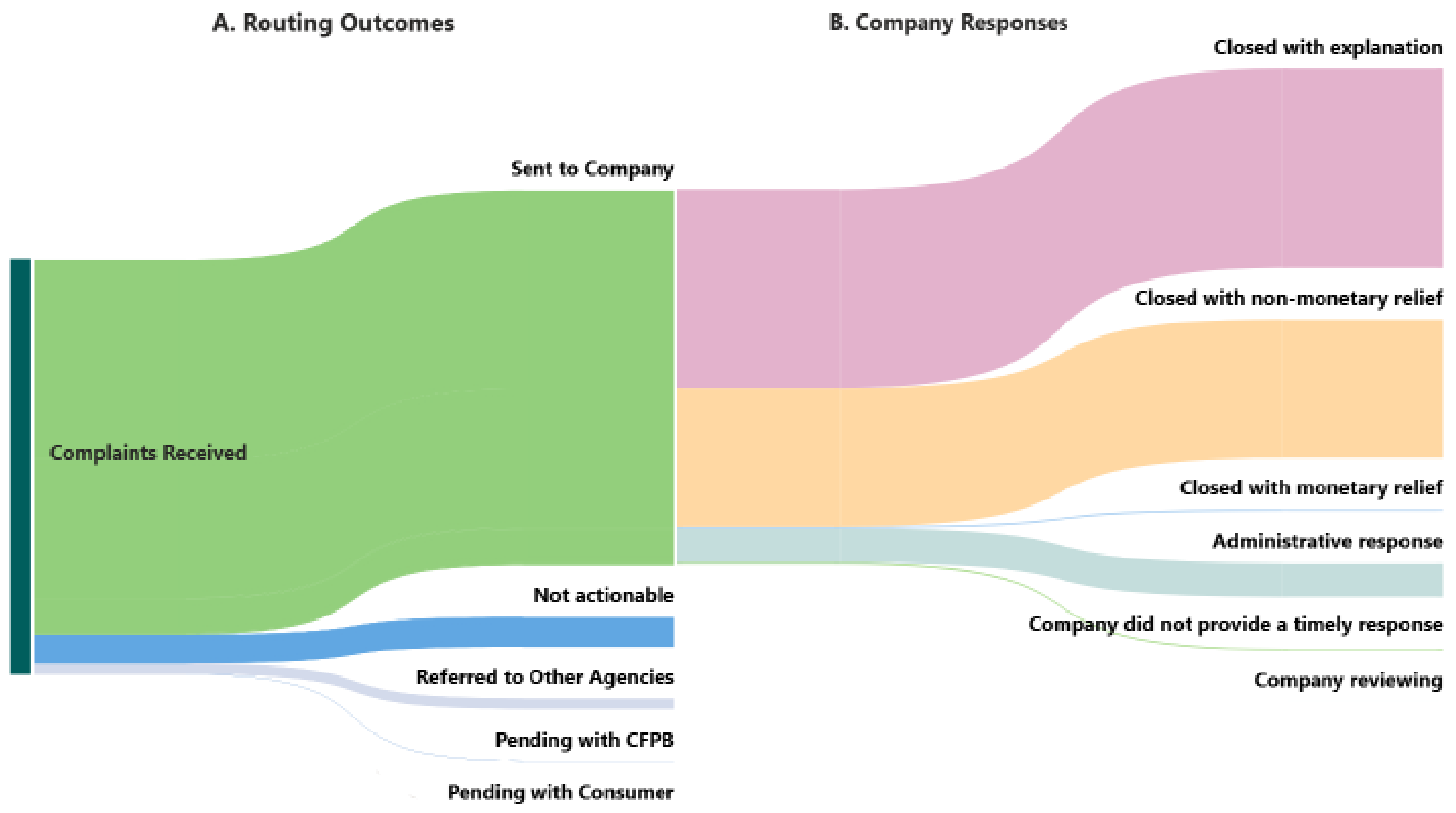
Note: Other products include commercial products, nondeposit products, vehicle loans, customer service, and bank services. Real estate loans include adjustable-rate mortgages, residential construction loans, open-end home equity lines of credit, home improvement loans, home purchase loans, home refinance/closed-end loans, and reverse mortgages.

CCO Issue 1 2026 (04-01-26)

TABLE 3: Cited Violations Resulting from Consumer Complaints for the Past 5 Years							
Violations	**2024**	**2023**	**2022**	**2021**	**2020**	**5-Year Total**	**% of All Violations**
Reg. E (EFTA)	51	161	175	203	171	761	79.8
Reg. B (ECOA)	0	1	5	8	6	20	2.1
Reg. CC (EFAA)	10	15	19	8	6	58	6.1
Reg. DD (TISA)	1	3	5	6	6	21	2.2
Reg. Z (TILA)	7	16	14	5	3	45	4.7
Reg. X (RESPA)	1	1	3	3	4	12	1.3
Reg. V (FCRA)	2	6	10	6	2	26	2.7
Other Regulations	4	0	0	0	2	6	0.6
Reg. P (GLBA)	0	1	1	2	0	4	0.4
Reg. H (FDPA)	1	0	0	0	0	1	0.1
Total Violations	**77**	**204**	**232**	**241**	**200**	**954**	**100**

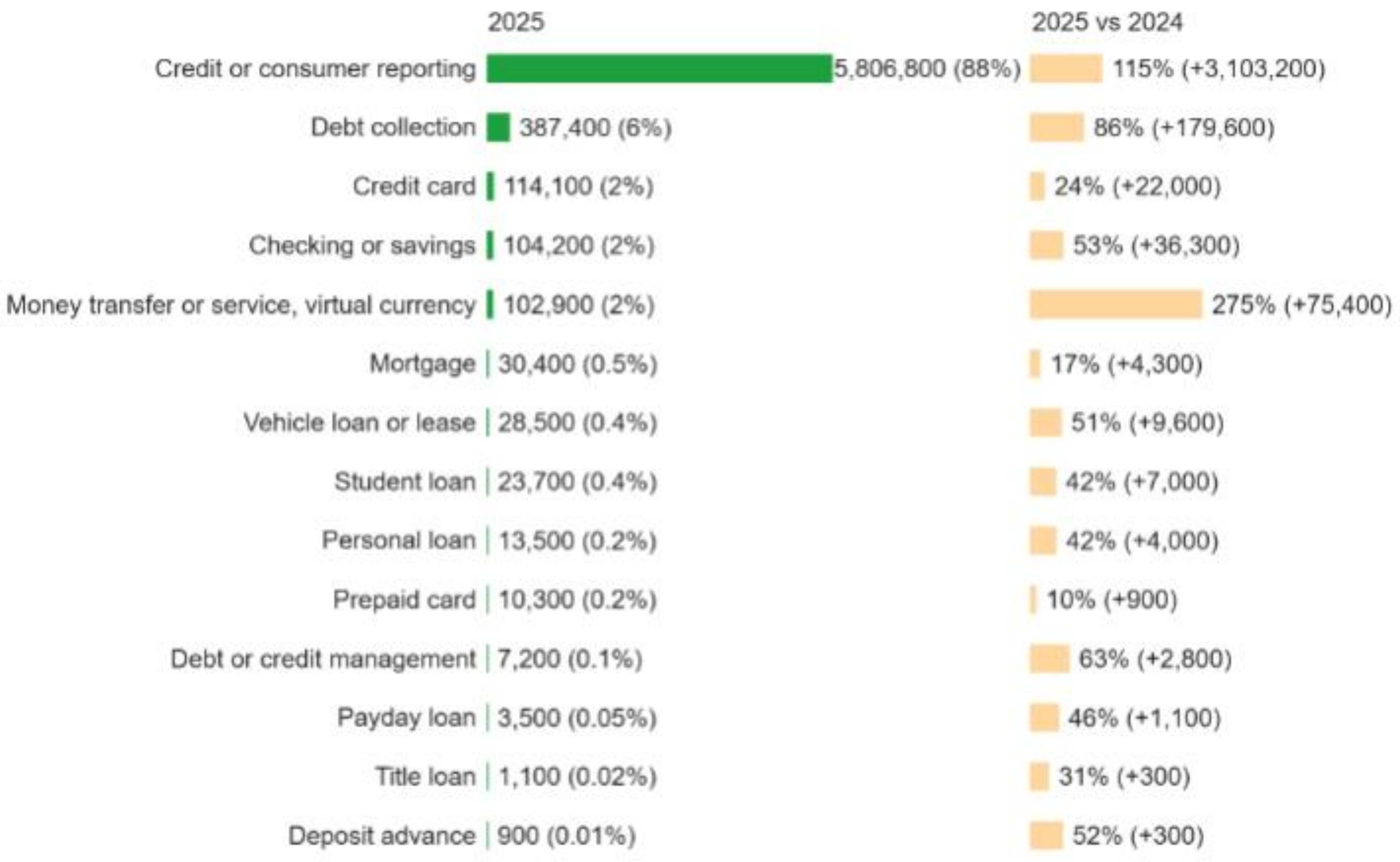
CFPB 2025 CR annual report 2026-03 (04-01-26)

- The number of consumer complaints to the CFPB has continued its year-over-year increase. In 2019, the CFPB received approximately 352,400 complaints. Two years later, in 2021, that number grew to 994,000 complaints. Two years after that, in 2023, the number reached 1,657,600 complaints. Since then, the number of complaints have roughly doubled each year: 3,187,900 complaints in 2024 and 6,635,400 complaints the CFPB received in 2025.
- Of the approximately 6,635,400 complaints the CFPB received in 2025, it sent approximately 5,984,100 (or 90%) to companies for review and response, referred 3% to other regulatory agencies, and found 7% to be not actionable. As of March 2, 2026, 0.03% of complaints were pending with the consumer and 0.03% were pending with the CFPB.
- **FIGURE 1: COMPLAINT OUTCOMES IN 2025**



CFPB 2025 CR annual report 2026-03 (04-01-26)

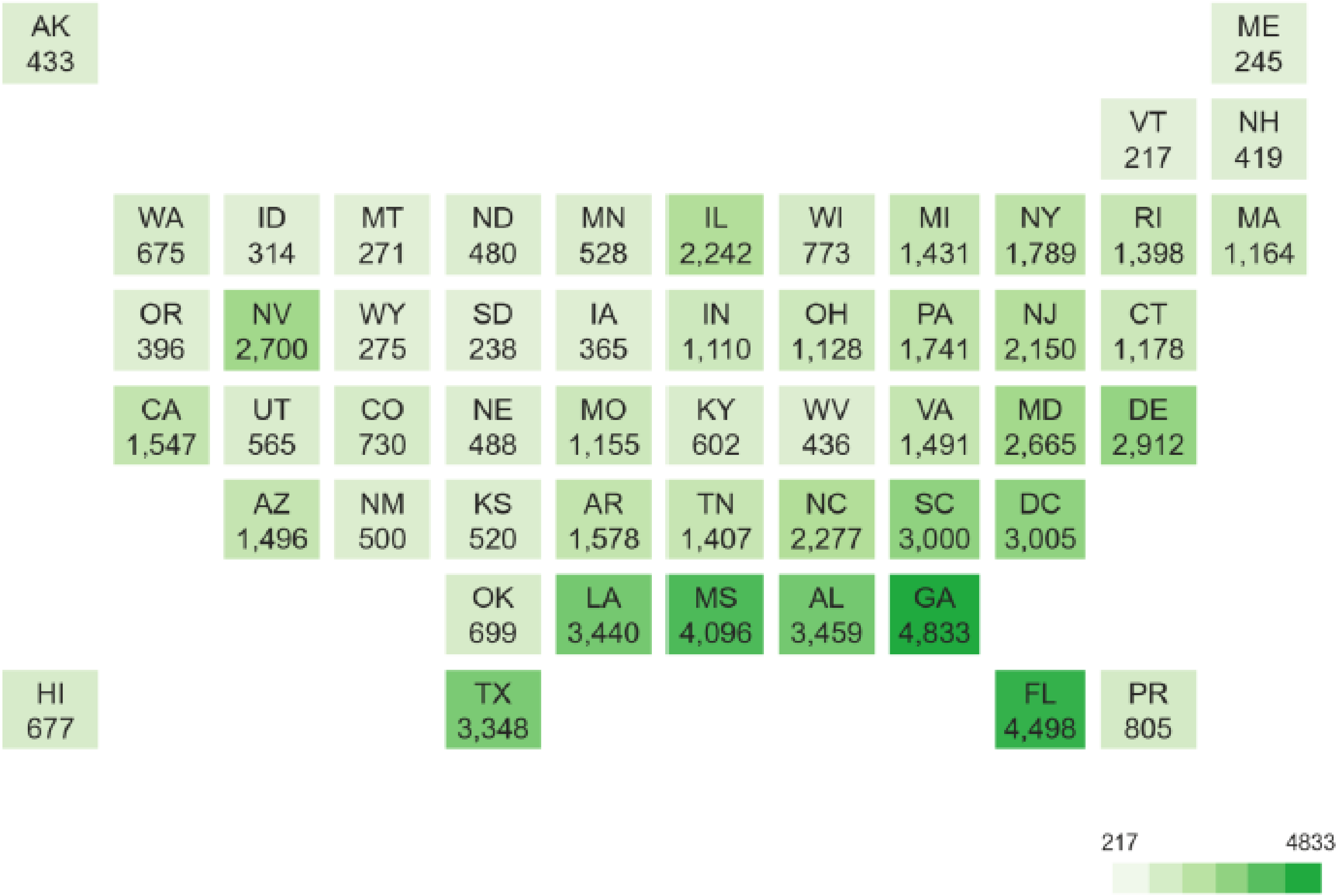
- **FIGURE 2: COMPLAINT VOLUME BY FINANCIAL PRODUCT OR SERVICE**



CFPB 2025 CR annual report 2026-03 (04-01-26)

ProSight

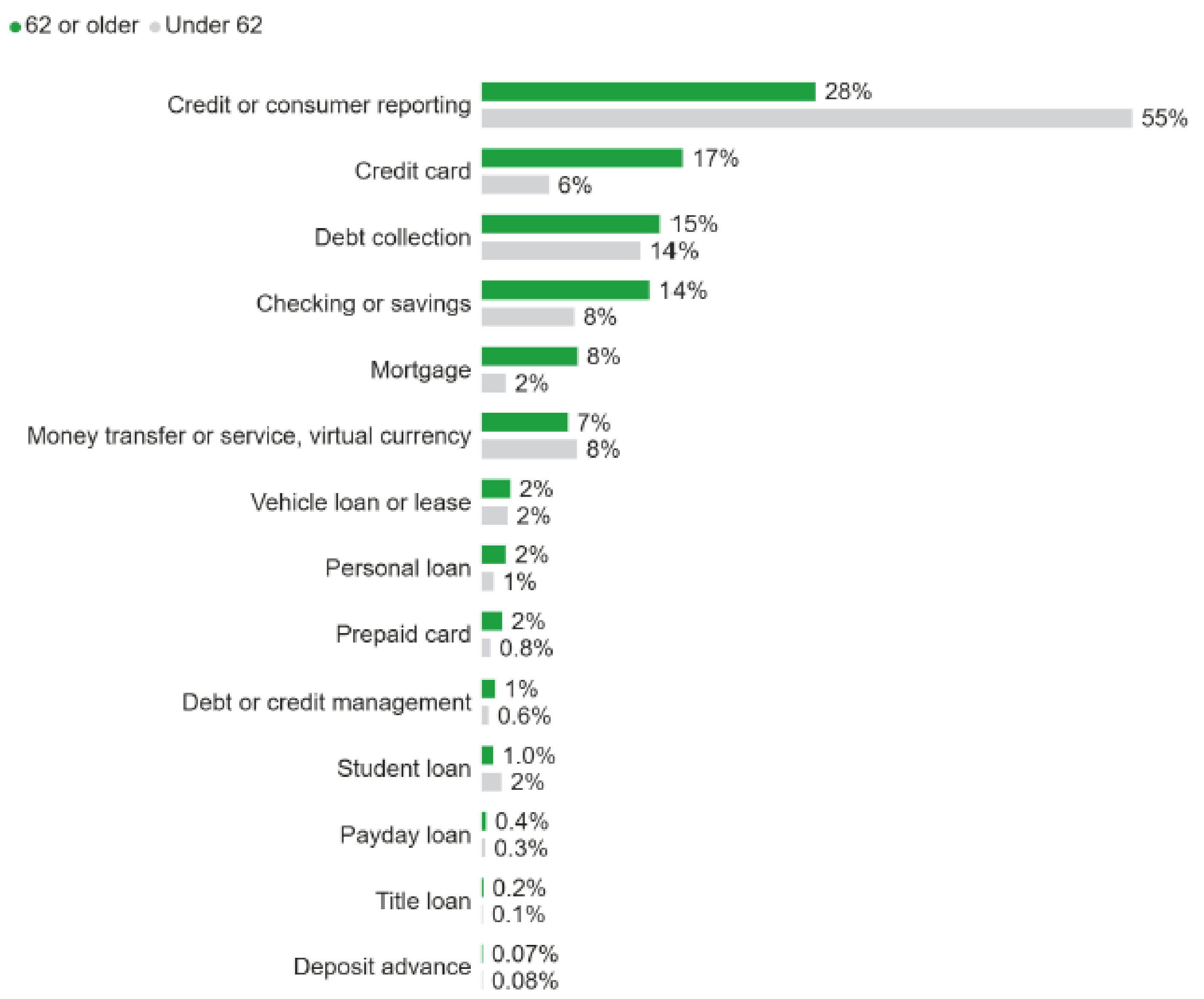
- **Geographic region**
- Consumers from all 50 states, the District of Columbia, and Puerto Rico and other U.S. territories submitted complaints to the CFPB. On a per capita basis, the CFPB received more complaints from consumers in Georgia than anywhere else in the United States, followed by those in Florida, Mississippi, Alabama, and Louisiana.
- **FIGURE 3: U.S. COMPLAINT SUBMISSIONS PER 100K POPULATION**



CFPB 2025 CR annual report 2026-03 (04-01-26)

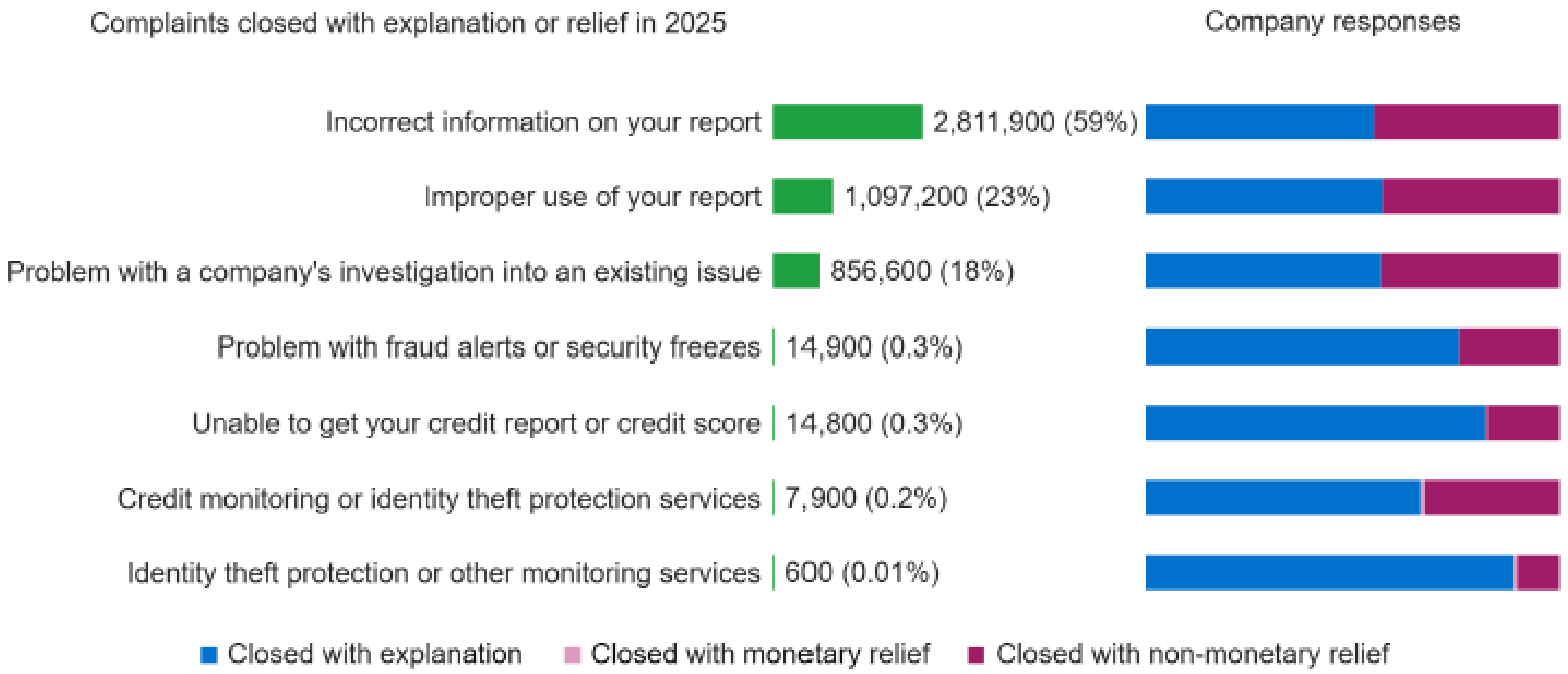
- Consumers provided their servicemember affiliation in approximately 136,300 complaints, or 2.1% of all complaints submitted in 2025.
- Consumers provided their age in approximately 654,200 complaints, or 10% of all complaints submitted in 2025. Figure 5 compares the product breakdown of complaints submitted by self-identified older consumers (age 62 or older) to consumers who reported an age under 62 years old.

FIGURE 5: PERCENTAGE OF COMPLAINTS BY PRODUCT AND AGE GROUP[17]



CFPB 2025 CR annual report 2026-03 (04-01-26)

- **FIGURE 8: CREDIT OR CONSUMER REPORTING COMPLAINTS BY ISSUES AND OUTCOMES**



Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- **§ 330.11 Accounts of a corporation, partnership or unincorporated association.**
- (a) * * *
- (3) Notwithstanding any other provision of this part, deposits at an insured depository institution held as reserves for a payment stablecoin, as defined in the Guiding and Establishing National Innovation for U.S. Stablecoins Act, are deposits of the permitted payment stablecoin issuer's and insured as corporate deposits for purposes of this part.
- **§ 350.0 Purpose and scope.**
- (a) *Purpose.* Subpart A implements certain provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (12 U.S.C. 5901 et seq.) (GENIUS Act) authorizing the FDIC to issue regulations under the Act with respect to permitted payment stablecoin issuers that have been approved by the FDIC and for which the FDIC is the primary Federal payment stablecoin regulator.
- (b) *Scope.* This subpart applies to all permitted payment stablecoin issuers for which the FDIC is the primary Federal payment stablecoin regulator.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- **§ 350.3 Activities.**
- (a) *Permitted activities*. A permitted payment stablecoin issuer may only:
- (1) Issue payment stablecoins;
- (2) Redeem payment stablecoins;
- (3) Manage reserves related to the issuance or redemption of payment stablecoins, including purchasing, selling, and holding reserve assets or providing custodial services for reserve assets, consistent with applicable State and Federal law;
- (4) Provide custodial or safekeeping services for payment stablecoins, required reserves, or private keys of payment stablecoins, consistent with subpart B of this part;
- (5) Undertake any other activities that directly support any of the activities described in paragraphs (a)(l) through (4) of this section;
- (6) Undertake activities that are incidental to any of the activities described in paragraphs (a)(l) through (4) or that are digital asset service provider activities (as defined in section 2(7)(A) of the GENIUS Act to be exchanging digital assets for monetary value, exchanging digital assets for other digital assets, transferring digital assets to a third party, acting as a digital asset custodian, or participating in financial services relating to digital asset issuance) or are incidental thereto that are authorized by the FDIC;

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (7) Assess fees associated with purchasing or redeeming payment stablecoins;
- (8) Pay fees to facilitate customer transactions; and
- (9) In undertaking any activity contemplated by the GENIUS Act (12 U.S.C. 5901 et seq.), act as principal or agent with respect to any payment stablecoin.
- (b) Prohibitions. A permitted payment stablecoin issuer shall not:
- (1) Use any combination of terms relating to the United States Government, including, but not limited to "United States," "United States Government,“ and "USG" in the name of a payment stablecoin;
- (2) Market a payment stablecoin in a manner that a reasonable person would perceive the payment stablecoin to be legal tender, issued by the United States; or guaranteed or approved by the Government of the United States;
- (3) Directly or through implication represent that payment stablecoins are backed by the full faith and credit of the United States, guaranteed by the United States Government, or subject to Federal deposit insurance;
- (4) Pay the holder of any payment stablecoin any form of interest or yield (whether in cash, tokens, or other consideration) solely in connection with the holding, use, or retention of such payment stablecoin;

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (5) Pledge, rehypothecate, or reuse any reserve assets required under § 350.4(a) either directly or indirectly, including through a third-party custodian of the reserve assets.
- (6) Engage in any activity that the FDIC determines is done in evasion of the requirements, standards, or prohibitions found in section 4 of the GENIUS Act (12 U.S.C. 5903) or this part 350;
- (7) Market a product in the United States as a payment stablecoin, or issue a payment stablecoin, unless the product or payment stablecoin is issued in compliance with the GENIUS Act and part 350; or
- (8) Provide a customer credit, directly or indirectly, to enable the customer to purchase or otherwise acquire payment stablecoins from the permitted payment stablecoin issuer.
- **§ 350.4 Reserve assets**
- (a) *Reserve requirement*. A permitted payment stablecoin issuer shall:
- (1) maintain identifiable reserves fully backing the outstanding payment stablecoins of the permitted payment stablecoin issuer, the reserve asset value of which will at all times meet or exceed the total outstanding issuance value of payment stablecoins issued by the permitted payment stablecoin issuer;
- (2) monitor issuance and redemption of outstanding payment stablecoins to ensure compliance with this section; and
- (3) either maintain reserves directly or keep reserves within the custody of eligible financial institutions.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (b) *Reserve Asset Value*. For purposes of calculating the reserve asset value of the reserve assets backing each outstanding payment stablecoin issued by the permitted payment stablecoin issuer, reserve assets shall be valued at fair value, with the exceptions of United States coins and currency which shall be valued at face value.
- (c) *Identifiable Reserves*. The reserves maintained by a permitted payment stablecoin issuer shall be readily identified as backing outstanding payment stablecoins issued and differentiated from assets not backing payment stablecoins.
- (e) *Reserve Composition.* The assets serving as identifiable reserves fully backing the outstanding payment stablecoins are limited to:
- (1) United States coins and currency (including Federal Reserve notes);
- (2) money standing to the credit of an account with a Federal Reserve Bank;
- (3) funds held as demand deposits or other deposits that may be withdrawn upon request at any time at an insured depository institution or insured shares held by an insured credit union (including any foreign branches or agents, including correspondent banks, of an insured depository institution);
- (4) Treasury bills, notes, or bonds with a remaining maturity of 93 days or less, or issued with a maturity of 93 days or less;

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (5) money received under repurchase agreements with the permitted payment stablecoin issuer acting as a seller of securities and with an overnight maturity that are backed by Treasury bills with a maturity of 93 days or less provided the money is received consistent with one or more of the allowable exceptions to rehypothecation, reuse, or pledging as circumscribed in 12 U.S.C. 5903(a)(2);
- (6) reverse repurchase agreements with the permitted payment stablecoin issuer acting as a purchaser of securities and with an overnight maturity that are collateralized by Treasury notes, bills, or bonds on an overnight basis, subject to overcollateralization in line with standard market terms,
- (7) securities issued by an investment company registered under section B(a) of the Investment Company Act of 1940 (15 U.S.C. 80a-8(a)), or other registered Government money market fund, and that are invested solely in underlying assets described in paragraphs (e)(1) through (6) of this section.
- (f) *Asset diversification and concentration*. A permitted payment stablecoin issuer shall on each business day limit its exposure to any one eligible financial institution, regardless of instrument type, to no more than 40 percent of its reserve assets.
- (g) *Monthly Report on Reserve Composition*. A permitted payment stablecoin issuer, for each publicly distinguishable brand of payment stablecoin issued, shall by close of business on the last day of each month, prepare and publish on its website using a format substantially similar to the template provided in table 1 a report containing as of close of business on the last day of the previous month: the total number of outstanding payment stablecoins issued by the permitted payment stablecoin issuer and the value and composition of the identifiable reserves described in § 350.4(e), including the average tenor and geographic location of custody of each category of reserve assets.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (h) *Monthly certification*; *examination of reports by registered public accounting firm.*
- (1) By close of business on the last day of each month, a permitted payment stablecoin issuer shall have a registered public accounting firm examine the information disclosed in the previous month-end report required by this subsection and the registered public accounting firm will issue a written report with findings to the permitted payment stablecoin issuer's audit committee (or board of directors, if no audit committee). The registered public accounting firm's examination report must be published on the website of the permitted payment stablecoin issuer at the same time as the month-end report required under paragraph (g); and
- (2) *Certification*. Each month, the Chief Executive Officer and Chief Financial Officer (or the persons performing the equivalent functions) of a permitted payment stablecoin issuer shall submit to the FDIC a certification as to the accuracy of the previous month-end report, including a copy of the written report prepared in § 350.4(h)(1).
- (i) *Failure to meet minimum reserve assets requirement*.
- (1) In the event that a permitted payment stablecoin issuer determines or has reasonable grounds to suspect that the aggregate reserve asset value of identifiable reserves backing outstanding payment stablecoins is less than the amount required under paragraph § 350.4(a), the permitted payment stablecoin issuer shall notify the FDIC in writing, with a description of measures to be taken pursuant to § 350.4(j), as appropriate.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- **§ 350.5 Redemption**.
- (a) Redemption policy. A permitted payment stablecoin issuer shall establish, implement, and publicly disclose its redemption policy. The redemption policy shall include, at a minimum, the following information:
- (1) The timeframe in which the permitted payment stablecoin issuer will redeem payment stablecoins issued by the permitted payment stablecoin issuer for a fixed amount of monetary value and the timeframe under which the permitted payment stablecoin issuer is required to redeem payment stablecoin under paragraph (b)(l) of this section;
- (2) A statement explaining the limitation in paragraph (b)(2) of this section;
- (3) A statement explaining the scenarios under which the redemption period may be extended as described in paragraph (c) of this section;
- (4) A statement with clear instructions on how a payment stablecoin holder can redeem a payment stablecoin, including a link to the website(s) where a payment stablecoin holder can redeem the payment stablecoin; and
- (5) The minimum number of payment stablecoins, if any, that the permitted payment stablecoin issuer will redeem, provided that the permitted payment stablecoin issuer shall redeem any number greater than or equal to one payment stablecoin, subject to appropriate screening and onboarding.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (b) *Redemption policy requirements*. A permitted payment stablecoin issuer’s redemption policy shall provide clear and conspicuous procedures for timely redemption of outstanding payment stablecoins:
- (1) That timely redemption may not exceed two business days following the date of the requested redemption; and
- (2) That any discretionary limitations on timely redemptions can only be imposed by the FDIC.
- (d) *Disclosures and fees associated with purchase and redemption*. A permitted payment stablecoin issuer shall:
- (1) Publicly, clearly, and conspicuously disclose in plain language and in a format that is readily noticeable, readily understandable, and segregated from other information:
- (i) The name of the permitted payment stablecoin issuer that issues the payment stablecoin;
- (ii) That the permitted payment stablecoin issuer is the entity that is obligated to convert, redeem, or repurchase the payment stablecoin for a fixed amount of monetary value;
- (iii) The link to the monthly composition report of the relevant permitted payment stablecoin issuer’s reserves required under § 350.4(g); and
- (iv) All fees associated with purchasing or redeeming payment stablecoins, if any.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (a) *General operational and managerial standards.*
- (1) *Internal controls and information systems*. A permitted payment stablecoin issuer shall have internal controls and information systems to support effective risk management that are appropriate to the size and complexity of the permitted payment stablecoin issuer and the nature, scope, and risk of its activities and that provide for:
- (i) An organizational structure that establishes clear lines of authority and responsibility for monitoring adherence to established policies;
- (ii) Effective risk assessment;
- (iii) Timely and accurate financial, operational, and regulatory reporting, including with respect to the reports required under this part;
- (iv) Adequate procedures to monitor, safeguard, manage, and control assets, including reserve assets; and
- (v) Compliance with applicable laws and regulations.
- (2) Internal audit system. A permitted payment stablecoin issuer shall have an internal audit system that is appropriate to the size and complexity of the permitted payment stablecoin issuer and the nature, scope, and risk of its activities.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (3) *Interest rate exposure*. A permitted payment stablecoin issuer shall manage interest rate risk in a manner that is appropriate to the size and complexity of the permitted payment stablecoin issuer and the complexity of its assets and liabilities.
- (4) *Asset growth*. A permitted payment stablecoin issuer's asset growth shall be commensurate with risk management and operational capabilities.
- (5) *Insider and affiliate transactions*. A permitted payment stablecoin issuer shall ensure that transactions between the permitted payment stablecoin issuer and insiders or affiliates (other than the insured depository institution of which it is a subsidiary):
- (i) Do not pose significant risks of material financial loss; and
- (ii) (A) Are conducted on terms that are the same or at least as favorable to the permitted payment stablecoin issuer as those prevailing at the time for comparable transactions with or involving non-insiders or non-affiliates;

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (6) *Oversee service provider arrangements*. A permitted payment stablecoin issuer shall:
- (i) Exercise appropriate due diligence in selecting its service providers;
- (ii) Require its service providers by contract to implement appropriate measures designed to meet the applicable requirements of this part; and
- (iii) As appropriate, monitor its service providers to confirm they have satisfied their obligations. As part of this monitoring, permitted payment stablecoin issuers should review audits, summaries of test results, or other equivalent evaluations of its service providers
- (c) *Anti-money laundering and economic sanctions compliance programs required certification.* Not later than days after the date of an 180 approval of an application filed pursuant to section 5 of the GENIUS Act (12 U.S.C. 5904), and on or before April of each year thereafter, a permitted payment stablecoin issuer shall certify that it has implemented anti-money laundering and economic sanctions compliance programs that are reasonably designed to prevent the permitted payment stablecoin issuer from facilitating money laundering, in particular, facilitating money laundering for cartels and organizations designated as foreign terrorist organizations under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189) and the financing of terrorist activities, as required by the GENIUS Act. Such certification signed by authorized persons/individuals responsible for overseeing the programs AML/CFT shall be submitted to the appropriate FDIC regional office.

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- **Subpart B-Requirements for FDIC Supervised Entities Engaged in the Custody or Safekeeping of Payment Stablecoin Reserves and Collateral**
- **§350.100 Purpose and Scope.**
- This subpart B sets forth requirements applicable to persons subject to supervision and regulation by the FDIC, including insured State nonmember banks, insured State-licensed branches of foreign banks, insured State savings associations, and permitted payment stablecoin issuers, for which the FDIC is the primary Federal banking agency or primary Federal payment stablecoin regulator, that are engaged in the business of providing custodial or safekeeping services for payment stablecoin reserves, payment stablecoins used as collateral, or private keys used to issue payment stablecoins pursuant to section 4(a)(7)(A)(iv) (12 U.S.C. 5903(a)(7)(A)(iv)) and section 10 of the GENIUS Act (12 U.S.C. 5909).
- **§ 350.103 Custodial and Safekeeping Requirements.**
- A custodian shall:
- (a) Treat payment stablecoin reserves, payment stablecoins used as collateral, private keys, cash, and other property it receives, acquires, or holds on behalf of a customer as belonging to such customer and not as the property of the custodian;

Federal Register notice genius act requirements and standards – FDIC supervised permitted (04-10-26)

- (b) Take appropriate steps to protect the customer's payment stablecoin reserves, payment stablecoins used as collateral, private keys, cash, and other property from claims of creditors of the custodian and any sub-custodian, as applicable, that are commensurate with the custodian's size, complexity, and risk profile and with the nature of the applicable assets for which it provides custodial or safekeeping services including through adopting implementing, and maintaining written policies, procedures, and internal controls that are adequate to comply with applicable law; and
- (c)
- (1) Maintain possession or control of the customer's payment stablecoin reserves, payment stablecoins used as collateral, private keys, cash, and other property that is held directly, including in a digital wallet for which the custodian controls the associated private keys; however, a custodian may maintain the customer's property through the use of a sub-custodian if consistent with applicable law, provided the custodian maintains adequate safeguards and internal controls reasonably designed to provide the custodian with oversight of such sub-custodian's compliance with the requirements of this subpart;
- § 350.104 Commingling Prohibition and Limited Exceptions.
- (a) General prohibition. A custodian shall not commingle and shall separately account for and segregate the payment stablecoin reserves, payment stablecoins, cash, and other property of a customer from the custodian's assets.

NCUA proposal GENIUS Act (05-18-26)

- The NCUA Board (Board) is seeking comment on proposed regulations to implement portions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act /(GENIUS Act). The GENIUS Act charges the NCUA with licensing, regulating, and supervising Payment Stablecoin issuers that are subsidiaries of federally insured credit unions (FICU subsidiaries). In February 2026, the NCUA issued proposed regulations to govern investments in and licensing of permitted payment stablecoin issuers subject to the NCUA's jurisdiction. This current proposal supplements the previous proposal and would govern the issuance of Payment Stablecoins and certain related activities by entities subject to the NCUA's jurisdiction. This proposal would also make amendments to address share insurance coverage, tokenized shares, and other conforming and clarifying amendments.
- Comments must be received by July 17, 2026.
- The NCUA Licensing Proposal determined that it is preferrable for FICU subsidiaries themselves to submit the required applications to be an NCUA-Licensed PPSI jointly with their FICU Parent Company(ies), as defined in the NCUA-Licensing Proposal, rather than having every single FICU investing in them submit an application. The Board's proposed approach would also require the applying FICU subsidiary, and any of its FICU Parent Companies and Principal Shareholders, to provide written certification that any filing or supporting material submitted to the NCUA contains no material misrepresentations or omissions. Further, as required by the GENIUS Act, all Directors and Officers of the applying FICU subsidiary, its FICU Parent Company(ies), and any of its Principal Shareholders would have to provide certain information so that the NCUA can evaluate their competence, experience, and integrity and ensure they do not have felony convictions prohibited by the GENIUS Act. Finally, the NCUA Licensing Proposal proposed limiting FICUs to investing in NCUA-Licensed PPSIs.

NCUA proposal GENIUS Act (05-18-26)

- The NCUA is issuing this supplemental proposed rule governing the issuance of Payment Stablecoins and certain related activities by entities subject to the NCUA's jurisdiction to supplement the NCUA Licensing Proposal and substantially implement the NCUA's proposed regulatory regime for NCUA-Licensed PPSIs and FICUs.
- **Subpart B-NCUA-Licensed Permitted Payment Stablecoin Issuers**
- **Subpart C-Custody**
- **Subpart D-Capital and Operational Backstop**

FDIC and OCC final rule removing reputation risk (04-10-26)

- **SUMMARY:** The Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation are adopting a final rule to codify the elimination of reputation risk from their supervisory programs. Among other things, the rule prohibits the agencies from criticizing or taking adverse action against an institution on the basis of reputation risk. The rule also prohibits the agencies from requiring, instructing, or encouraging an institution to close an account, to refrain from providing an account, product, or service, or to modify or terminate any product or service on the basis of a person or entity's political, social, cultural, or religious views or beliefs, constitutionally protected speech, or solely on the basis of politically disfavored but lawful business activities perceived to present reputation risk. The rule further forbids the agencies from taking any supervisory action or other adverse action against an institution, a group of institutions, or the institution-affiliated parties of any institution that is designed to punish or discourage an individual or group from engaging in any lawful political, social, cultural, or religious activities, constitutionally protected speech, or, for political reasons, lawful business activities that the agencies or its personnel disagree with or disfavor.
- **DATES:** The final rule is effective June 9, 2026.

Agencies issue guidance on model risk management (04-17-26)

- This guidance highlights sound principles for effective model risk management. As reflected in this guidance, model risk management practices vary from banking organization to banking organization. Each banking organization ultimately is responsible for adopting model risk management practices that are appropriate and effective for managing the specific risks the banking organization faces or is likely to face.
- There are a variety of ways for a banking organization to structure model risk management practices. Not all models present the same level of risk, and a similar model at two different banking organizations may present different risks. As such, practices that are appropriate and effective for one banking organization may be inappropriate and ineffective for a banking organization with a different risk profile or that uses a model for a different purpose.
- Based on supervisory experience and industry feedback, as well as technological advancements in modeling over the past several years, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation (the “agencies”) are issuing this revised model risk management guidance to clarify model risk management principles, and to set forth a risk-based approach to model risk management, tailored to a banking organization’s model risk profile and the size and complexity of its operations.

Agencies issue guidance on model risk management (04-17-26)

- This guidance is expected to be most relevant to banking organizations with over $30 billion in total assets. Models used by banking organizations with total assets of $30 billion or less typically are subject to internal risk management and governance practices appropriate for the size and risk profile of these banking organizations, and generally excluding them from this guidance is consistent with a tailored supervisory approach. However, in some situations, this guidance also may be relevant to banking organizations with total assets of $30 billion or less that have significant exposure to model risk because of the prevalence and complexity of their models or because of activities outside the scope of traditional community banking.
- For the purposes of this guidance, the term “model” refers to a complex quantitative method, system, or approach that applies statistical, economic, or financial theories to process input data into quantitative estimates. The term “model” in this guidance excludes simple arithmetic calculations, such as those found within spreadsheets, as well as deterministic rule-based processes and software where there are no statistical, economic, or financial theories underpinning their design or use.
- Model testing is a core component of model development that evaluates whether a model performs as intended. Testing may include a range of activities, from out-of-sample and out-of- time testing, to a comparison of alternative assumptions and methodologies, to a critical assessment of data quality, relevance, and inputs. Testing may be performed by model developers in collaboration with model users. The specific approach depends on the model’s characteristics. The rigor of effective testing is commensurate with model complexity and materiality. For models that have relatively less material impact or for banking organizations with relatively less complex operations, model testing may be more limited in scope.

Agencies issue guidance on model risk management (04-17-26)

ProSight™

- The timing, nature, and frequency of validation activities vary based on model purpose, model methodology, frequency and scope of model changes, data limitations, and other practical constraints. Sound practice recognizes that validation approaches may differ across models based on their characteristics and use. Validation generally occurs prior to a model's first use. However, certain circumstances (e.g., an urgent business need) may necessitate using the model before validation is completed. In those cases, sound practice involves greater attention to the model's limitations when considering the appropriateness of its use, informing relevant stakeholders of those limitations, and determining appropriate controls (e.g., placing limits on model use or more closely monitoring its performance).
- The widespread use of customized vendor and other third-party products—including data, parameter values, or complete models—can present unique challenges for validation and other model risk management activities. Additionally, because certain components may be proprietary, banking organizations may not receive from the vendor the underlying code, data, or methodology that they would have if a model were developed internally. Nevertheless, the principles of model risk management remain applicable.
- An important element of model risk management is the validation of vendor products, either by internal or outside parties. Sound practice includes developing an understanding of the vendor model, including its conceptual soundness, design, development data, and performance. Similarly, sound practice involves conducting ongoing monitoring and outcome analysis to assess whether vendor models are accurate, remain fit for purpose, and continue to be reliable.

OCC Interim Final Rule Preemption Illinois Interchange Fee (04-29-26)

ProSight™

- The OCC is issuing an interim final order concluding that Federal law preempts the Illinois Interchange Fee Prohibition Act, which purports to prohibit national banks and Federal savings associations from charging or receiving interchange fees on the tax and gratuity portions of payment card transactions; and restrict the use of payment card transaction data. The OCC invites public comments on this interim final order.
- **DATES:** The interim final order is effective June 30, 2026. Comments on the interim final order must be received on or before May 29, 2026.

OCC Interim Final Rule National Bank Non Interest Charges and Fees (04-29-26)

- **SUMMARY:** The OCC is adopting an interim final rule to clarify that national banks' power to charge non-interest charges and fees includes the power to assess, collect, impose, levy, receive, reserve, take, or otherwise obtain non interest charges and fees, including interchange fees from credit and debit card operations. Further, the interim final rule explains that national banks may charge non-interest charges or fees, even when such charges and fees are set by or in consultation with third parties. The OCC invites public comments on this interim final rule.
- **DATES:** The interim final rule is effective June 30, 2026. Comments on the interim final rule must be received on or before May 29, 2026.

NCUA Interim Final Rule National Bank Preemption Non Interest Charges (06-09-26)

- **12 CFR Part 701**
- **ACTION:** *Interim final rule; request for comment.*
- *The NCUA Board is adopting an interim final rule to clarify federal credit unions' (FCUs) power to charge non-interest charges and fees includes the power to assess, collect, impose, levy, receive, reserve, take, or otherwise obtain non-interest charges and fees, including interchange fees from credit and debit card operations. Further, the interim final rule explains that FCUs may charge non-interest charges or fees, even when such charges and fees are set by or in consultation with third parties. NCUA invites public comments on this interim final rule.*
- ***DATES:** The interim final rule is effective June 30, 2026. Comments on the interim final rule must be received on or before July 9, 2026*

Miscellaneous Odds and Ends

- 1. Treasury issues proposal under the GENIUS Act to determine if state regulatory regime is similar to Federal regulatory regime 4/1/26

  Treasury Seeks Public Comment on GENIUS Act Notice of Proposed Rulemaking Concerning State-Level Regulatory Regimes | U.S. Department of the Treasury

- 2. NCUA issued their 9th, 10th and 11th round of amendments to rules related to deregulation 4/7/26, 4/21/26, 5/7/26

  NCUA Announces Ninth Round of Deregulation Proposals | NCUA

  NCUA Announces Tenth Round of Deregulation Proposals | NCUA

  NCUA Announces Eleventh Round of Deregulation Proposals | NCUA

- 3. IRS proposal on excise taxes for certain remittance transfers 4/13/26

  Federal Register :: Excise Tax on Remittance Transfers

- 4. OCC Proposes rescission or amendments to unnecessary regulations 4/24/26

  Notice of Proposed Rulemaking: Streamlining Regulations Concerning Public Welfare Investments, Open Market Collateralized Loan Obligations, and Federal Savings Association Nondiscrimination Requirements | OCC

Miscellaneous Odds and Ends

- 5. HUD proposes removal of ‘gender’ from 30 regulations 4/28/26
  Federal Register :: Equal Access to Housing in HUD Programs Revisions
- 6. Agencies issued host state loan to deposit ratios 5/1/26
  Agencies Issue Host State Loan-to-Deposit Ratios | OCC
- 7. Agencies remove more references to reputation risks 6/2/26
  Agencies Remove Additional References to Reputation Risk | FDIC.gov
- 8. NCUA issues dependent care and Board member expense reimbursement 6/8/26
  2026-11507.pdf
- 9. Brian Johnson nominated to be Director of the CFPB 6/10/26
  Nomination Sent to the Senate – The White House
- 10. OCC proposes information collection, reporting forms and instructions for permitted payment stablecoin issuers 6/12/26
  Federal Register :: Agency Information Collection Activities: Proposed Information Collection; Reporting Forms and Instructions for Permitted Payment Stablecoin Issuers Subject to the Jurisdiction of the Office of the Comptroller of the Currency; Comment Request

Miscellaneous Odds and Ends

- 11. Agencies issue a final joint rule to establish data standards to promote interoperability of financial regulatory data across these agencies 6/11/26

  Federal Register notice: Financial Data Transparency Act Joint Data Standards
- 12. Regulation XX publication of July 1 financial sector liabilities 6/16/26

  Federal Register :: Announcement of Financial Sector Liabilities
- 13. OCC updates minority depository institutions policy statement 6/16/26

  Minority Depository Institutions: Reissuance of Policy Statement | OCC
- 14. OCC clarifies filing decision process 6/17/26

  Filing Decision Process | OCC
- 15. FFIEC reports 2025 data on mortgage lending

  FFIEC Publishes 2025 Data on Mortgage Lending | FFIEC 6/23/36
- 16. CFPB reports fixes to its consumer complaint process 6/24/26

  The CFPB is Correcting Flaws to Restore Integrity and Utility to the Consumer Complaint System | Consumer Financial Protection Bureau

Miscellaneous Odds and Ends

- 17. FDIC Board Approves Proposal to Amend Resolution Submissions by Covered Insured Depository Institutions 6/25/26

  [FDIC Board Approves Proposal to Amend Resolution Submissions by Covered Insured Depository Institutions | FDIC.gov]

ProSight™

Thank-you!