

Realignment in Motion – AML, Digital Assets and Consumer Risk

April 9, 2026

Table of Contents:

- [FinCEN Proposes Reform of AML/CFT Regulations, With Bank Regulators Making Coordinated Proposals](#)
- [SEC and CFTC Issue Interpretive Framework on Digital Assets](#)
- [FDIC and OCC Finalize Rule Removing Reputation Risk From Most Supervisory Actions](#)
- [Consumer Protection Roundup](#)

FinCEN Proposes Reform of AML/CFT Regulations, With Bank Regulators Making Coordinated Proposals

April 9, 2026



By Mercedes Kelley Tunstall
Partner | Financial Regulation



By Christian Larson
Special Counsel | White Collar Defense and Investigations



By Bea Rubin
Associate | Global Litigation



By James Katz
Associate

On April 7, 2026, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a [Notice of Proposed Rulemaking](#) (NPRM) that, if adopted, would significantly reform financial institutions' anti-money laundering and countering the financing of terrorism (AML/CFT) programs under the Bank Secrecy Act (BSA). FinCEN describes the proposed rule as an effort to shift financial institutions away from technical compliance toward AML/CFT programs that effectively identify, prevent, and report financial crimes.

A [Fact Sheet](#) accompanying the proposed rule states that the new rule will refocus compliance expectations on effectiveness by distinguishing between deficiencies that stem from program design—which FinCEN refers to as “establishment”—and program implementation—which FinCEN refers to as “maintenance.” According to FinCEN, establishing an AML/CFT program would require keeping the program current as a financial institution's risk profile evolves. Maintaining an AML/CFT program would require an institution to implement its program in all material respects—in other words, to execute the program in practice. Notably, the Fact Sheet states that FinCEN and other AML/CFT regulators generally will bring a significant enforcement action only if a financial institution has failed to establish an AML/CFT program, or if there is a significant or systemic failure to maintain the program.

In addition, for the first time, federal banking regulators would be required to notify and consult with FinCEN prior to initiating a significant supervisory or enforcement action related to a financial institution's AML/CFT program. The proposed rule fully supersedes a prior proposed rule that FinCEN published on July 3, 2024, which FinCEN is withdrawing. Public comments are due 60 days after publication in the *Federal Register* (Docket No. FINCEN-2026-0034; RIN 1506-AB72) - which will probably be in mid-June. FinCEN has proposed an effective date 12 months after the issuance of a final rule.

Speaking of federal banking regulators, the Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and the National Credit Union Administration (NCUA) (“the Agencies”) [issued a joint NPRM](#) asking for comments on aligning the existing requirements for supervised institutions with the changes proposed by FinCEN. As described in the [related press release](#), the Agencies' NPRM is focused on not only ensuring “consistency between FinCEN's and the Agencies' separately authorized compliance program requirements,” but also to modernize and strengthen the AML/CFT regulatory framework. The Agencies' NPRM has the same window for public comment – 60 days after publication in the Federal Register, or approximately mid-June.

Accordingly, the Agencies' NPRM adds these concepts to how AML/CFT programs should work:

- As with FinCEN's proposal, a bank's AML/CFT program should be risk-based with the goal being to direct more attention to higher-risk customers and activities, rather than toward lower-risk customers and activities.
- Explicitly incorporating FinCEN's existing customer due diligence requirements into the rules enforced by the Agencies and clarifying that a bank's designated AML/CFT officer must be located in the United States.

- Clarify that banks may share any information with FinCEN, related to certain AML/CFT supervisory and enforcement actions and enhance FinCEN's role in the Agencies' supervision and enforcement process by "establishing a new consultation framework for certain actions by the Agencies."

In effect, the two NPRMs are designed to work together in a manner that signals better coordination among FinCEN and the Agencies when it comes to AML/CFT enforcement, which will be a welcome change for the supervised institutions.

SEC and CFTC Issue Interpretive Framework on Digital Assets

April 9, 2026



By Mercedes Kelley Tunstall
Partner | Financial Regulation



By Maurine R. Bartlett
Senior Counsel | Capital Markets



By Christina Mille
Associate | Financial Services

On March 17, 2026, the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission issued a joint interpretive release clarifying the application of the federal securities laws to digital assets.^[1]

The agencies state that the interpretation is intended to (i) provide a “coherent” taxonomy of crypto assets, (ii) explain how a non-security crypto asset may become subject to, and cease to be subject to, an investment contract, and (iii) clarify the treatment of protocol mining, staking, wrapping, and airdrops.

SEC Chair Paul S. Atkins emphasized that the guidance is intended to “draw clear lines in clear terms,” while acknowledging that “most crypto assets are not themselves securities” and that investment contract analyses may evolve over time. CFTC Chair Michael S. Selig similarly characterized the release as establishing “clear and rational rules of the road” and a “workable, harmonized” regulatory framework.^[2]

I. A Functional Taxonomy of Digital Assets

The release introduces a framework distinguishing among categories of digital assets based on their economic function. The SEC identifies several categories of digital assets that, in isolation, generally do not constitute securities:

- **“Digital Commodities – NOT Securities** – These are crypto assets that are intrinsically linked to and derive their value from how crypto systems function, as well as supply and demand dynamics, rather than from the expectation of profits from the essential managerial efforts of others.” These assets typically do not convey rights to income, profits, or assets of a business enterprise, and instead function as integral components of decentralized networks (e.g., facilitating validation, governance, or transaction execution). The release identifies examples including Bitcoin, Ether, and Dogecoin, which operate on decentralized systems and are not dependent on a central promoter for value creation.
- **“Digital Collectibles – NOT Securities** – These are crypto assets that are designed to be collected and/or used and may represent or convey rights to artwork, music, videos, trading cards, in-game items, or digital representations or references to internet memes, characters, current events, or trends, among other things.” However, a digital collectible may be treated as a security where it is offered or marketed with an expectation of profit or where purchasers are led to rely on the ongoing managerial or entrepreneurial efforts of others (e.g., where value depends on a promoter developing, enhancing, or supporting the asset).
- **“Digital Tools – NOT Securities** – These are crypto assets that perform a practical function, such as providing proof of a membership, or acting as a ticket, credential, title instrument, or identity badge.”
- **“Stablecoins^[3] – GENIUS Act Stablecoins NOT Securities** – Defined in the GENIUS Act as ‘payment stablecoin issued by a permitted payment stablecoin issuer.’”^{[4][5]} A payment stablecoin is a digital asset that is used for payment or settlement and whose issuer is obligated to convert, redeem, or repurchase the asset for a fixed amount of monetary value, thereby maintaining a stable value relative to that reference asset. The GENIUS Act further provides that a “payment stablecoin issued by a permitted payment stablecoin issuer” is not a security.

A permitted payment stablecoin issuer is a U.S.-formed entity, including certain bank-affiliated or regulated entities, that is authorized under federal or state regimes to issue such instruments, although it is possible for foreign companies to be approved as foreign payment stablecoin issuers. All such issuers are subject to specific statutory constraints, including a prohibition on paying interest or yield to holders solely in connection with holding

or using the stablecoin. Stablecoins that fall within this statutory framework are categorically excluded from the definition of a security. However, there are other types of digital assets that presently describe themselves as stablecoins, and unless the issuers of such stablecoins become permitted issuers, then the GENIUS Act provides that they may no longer be characterized as stablecoins. At such time, those stablecoins would most appropriately be analyzed under the federal securities laws, depending on their characteristics and use.

The agencies did reaffirm that tokenized traditional financial instruments constitute securities:

- “*Digital Securities* (or ‘tokenized securities’) – Securities – Financial instruments enumerated in the definition of ‘security’ that is formatted as or represented by a crypto asset, where the record of ownership is maintained in whole or in part on or through one or more crypto networks.”^[6]

III. Asset Classification Provides Direction, Not Certainty

The SEC emphasizes that this taxonomy is descriptive, not determinative. While the categories provide a useful way to understand how digital assets function, they do not resolve whether a particular transaction involves a security.

Instead, the classification serves as an analytical starting point for applying the securities laws. The ultimate determination continues to depend on the surrounding facts and circumstances—particularly whether the transaction introduces elements of an investment contract.

As a result, an asset that falls within a “non-security” category in isolation may nonetheless be treated as a security where it is offered, marketed, or supported in a manner that creates a reasonable expectation of profits based on the efforts of others.

III. The Agencies Are Focused on What Issuers and Platforms Do

The SEC reiterates that the analysis turns on whether a transaction involves an “investment contract” under *SEC v. W.J. Howey Co.*^[7], and emphasizes that how an issuer markets and promotes a crypto asset is central to that determination.

- a. Inducement and Managerial Efforts Establish the Investment Contract.** The Commission explains how a non-security crypto asset becomes subject to an investment contract. It states that this occurs where an issuer “induces an investment of money in a common enterprise” through “representations or promises” that it will undertake “essential managerial efforts” from which purchasers would reasonably expect to derive profits. The focus is on inducement and reliance: whether the issuer is positioning itself as central to value creation, development, or maintenance of the network or asset. This includes situations where the issuer undertakes to build out functionality, support secondary markets, enhance token value, or otherwise drive adoption in a manner that creates a reasonable expectation of profit.
- b. Source, Medium, and Content of Representations Control the Analysis.** The Commission provides more granular guidance on the nature of the “representations or promises” that can give rise to an investment contract. It emphasizes that the analysis depends on (i) the source of the statements (e.g., core development team, affiliated entities, or other promoters), (ii) the medium through which they are communicated (including white papers, websites, social media, and ongoing public communications), and (iii) the level of detail and specificity regarding future efforts and expected outcomes. The release makes clear that both pre-launch and post-launch statements are relevant, and that ongoing communications reinforcing reliance on a central team can sustain an investment contract even after initial distribution.
- c. Termination of the Investment Contract Depends on Dissipation of Reliance.** The Commission also addresses when a crypto asset ceases to be subject to an investment contract. It explains that the investment contract may terminate where the issuer has “fulfilled its representations or promises” or where it has “failed to satisfy” them, such that purchasers can no longer reasonably rely on the issuer’s efforts. This reflects the view that the securities law analysis is not static, but evolves with the facts. At the same time, the Commission does not define when reliance has sufficiently dissipated, leaving the determination dependent on whether, in practice, a core group continues to play an essential role in the asset’s value or operation.

Taken together, these points operationalize *Howey* in the digital asset context. The Commission is not changing the test, but is expanding how it will be applied.^[8] For market participants, the implication is that both initial structuring and ongoing conduct must be managed carefully, as the same asset can move into, and remain within, the securities laws based on how it is presented and supported over time.

IV. Further Agency Clarifications

The Commission states that “protocol mining,” “protocol staking,” and the “wrapping” of a non-security crypto asset “do not involve the offer and sale of a security,” and that certain “airdrops” do not involve an “investment of money” under *Howey*.

The SEC states that “payment stablecoins issued by a permitted payment stablecoin issuer” are not securities, focusing on instruments designed to maintain a stable value and function as payment mechanisms.

V. What the Agencies Leave Open, Potential Problems

The release does not define when a token definitively transitions out of securities status, nor does it address how broker-dealer, exchange, or ATS frameworks apply to digital asset platforms.

The framework does not displace the case-by-case application of *Howey*, and outcomes will continue to turn on specific facts and conduct. In practice, this means that two tokens with identical features may be treated differently depending on how they are offered, marketed, and supported. The agencies are making clear that classification alone is not determinative; rather, the presence or absence of representations, the role of a central team, and the structure of the surrounding transaction will drive the analysis.

While the release describes a coordinated approach in which the SEC regulates digital securities and the CFTC regulates digital commodities, it does not resolve how existing regulatory frameworks apply. Platforms operating across asset types will still need to navigate multiple regimes.

The framework may also face limitations post-*Chevron*, as courts are no longer required to defer to the SEC’s interpretation of ambiguous statutory terms.^[9] This raises the possibility of divergence between the Commission’s approach and judicial outcomes, particularly given the release’s reliance on flexible, fact-dependent standards and its attempt to draw distinctions (such as the “lifecycle” concept) that are not expressly grounded in the statutory text.

VI. Industry Takeaways

The central message is that most tokens are not securities in isolation, but that representations, structure, and ongoing involvement determine whether the securities laws apply.

For market participants, the implication is that compliance must be built into product design, communications, and operations from the outset. The framework creates room to structure outside the securities laws, but it does not reduce the importance of execution or the risk of recharacterization.

The SEC has requested public comment on the interpretive release.

^[1] *Securities and Exchange Commission, Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets*, Securities Act Release No. 33-11412, Exchange Act Release No. 34-105020 (Mar. 17, 2026), <https://www.sec.gov/files/rules/interp/2026/33-11412.pdf>.

^[2] Press Release, U.S. Securities and Exchange Commission, *SEC Clarifies the Application of Federal Securities Laws to Crypto Assets*, No. 2026-30 (Mar. 17, 2026), <https://www.sec.gov/newsroom/press-releases/2026-30-sec-clarifies-application-federal-securities-laws-crypto-assets>.

^[3] Stablecoins are crypto assets designed to maintain a stable value relative to a reference asset, typically a fiat currency such as the U.S. dollar. They are commonly used as a means of payment, settlement, or value storage within crypto markets. Stablecoins generally seek to maintain this stability through mechanisms such as asset-backed reserves (e.g., cash or U.S. Treasury holdings) or other stabilization frameworks, and are typically structured to be redeemable at or near par value. The GENIUS Act defines a subset of these instruments, “payment stablecoins issued by a permitted payment stablecoin issuer,” which the release treats as not constituting securities.

^[4] U.S. Securities and Exchange Commission, *Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets* (Fact Sheet, Mar. 17, 2026), <https://www.sec.gov/files/33-11412-fact-sheet.pdf>.

^[5] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, 139 Stat. ____ (2025); see also Cadwalader, Wickersham & Taft LLP, *Operation and Structure of the GENIUS Act of 2025 on Payment*

Stablecoins (June 24, 2025), <https://www.cadwalader.com/resources/clients-friends-memos/operation-and-structure-of-the-genius-act-of-2025-on-payment-stablecoins>.

[6] *Id.*

[7] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) (“*Howey*”). The *Howey* test defines an investment contract as a contract, transaction, or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with an expectation of profits derived from the efforts of others.

[8] The interpretation does not replace *Howey*, but instead conveys the SEC’s views, based on extensive public input, on how certain aspects of the *Howey* investment contract test apply to crypto assets and transactions, and represents the SEC’s first step toward developing a clearer regulatory framework for the treatment of crypto assets under the federal securities laws.

[9] *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984). The Court established a two-step framework under which courts first determine whether Congress has spoken directly to the precise question at issue and, if not, defer to an agency’s reasonable interpretation of an ambiguous statute. That framework was later abrogated by *Loper Bright Enterprises v. Raimondo*, which held that courts must exercise independent judgment in interpreting statutes and are no longer required to defer to agency interpretations.

FDIC and OCC Finalize Rule Removing Reputation Risk From Most Supervisory Actions

April 9, 2026



By Daniel Meade
Partner | Financial Regulation

On April 7, the Federal Deposit Insurance Corporation (“FDIC”) and the Office of the Comptroller of the Currency (“OCC”) approved a **final rule** that prohibits regulators from using “reputation risk” as a standalone basis for supervisory or enforcement actions. This final rule is adopted largely as **proposed** in October.

Below, we detail the core components of the rule and what it means for your institution’s risk management and client onboarding strategies.

The Final Rule explicitly forbids examiners from citing “reputation risk” as the *sole* justification for a formal enforcement action or a downgrade in a bank’s supervisory rating. The **staff memo** to the FDIC Board noted that the concept of reputation risk “increases subjectivity in supervision without adding material value from a safety and soundness perspective.” The staff said that the rule is aimed at:

- **Evidence-Based Supervision:** To take action against an institution regarding its client base, regulators must now point to **concrete, quantifiable risks**—namely credit, liquidity, legal, or operational risks.
- **Neutrality Toward Lawful Business:** The rule codifies the principle that banks should not be pressured to terminate relationships with lawful businesses based purely on the “repute” of the industry. The final rule specifically prohibits encouraging a bank to terminate a contract based on “political, social, cultural, or religious views or beliefs, constitutionally protected speech, or involvement in politically disfavored but lawful business activities.”

The FDIC Board members were vocal about the rule’s intent to curb regulatory overreach. FDIC Chair Travis Hill described the rule as a mechanism to ensure the agency remains “focused on our key responsibilities, color within the lines, and keep the main thing the main thing” during the discussion of the rule at the FDIC April 7 meeting. He noted that while a bank’s reputation is important, focus on it “untethered from other risk channels” can pressure banks into “debanking law-abiding customers who are viewed unfavorably by supervisors.” Comptroller of the Currency Jonathan Gould was even more direct, calling the rule a step toward “reducing the opportunities for regulatory abuse.” Comptroller Gould argued that reputation risk has “too often used it as a pretext for decisions that have nothing to do with safety and soundness,” resulting in lawful businesses and individuals being “denied access to banking services.”

As noted above, the final rule was adopted largely as proposed, but the final rule did make two changes based on comments and feedback during the comment period. Reputation risk is now defined as the risk that an activity could negatively impact public perception for reasons “not clearly and directly related to the financial or operational condition of the institution.” The final rule also made clear that the prohibition on supervisory activity discouraging lawful activities would apply to all agency personnel and not just supervisory staff.

The rule will become effective 60 days after publication in the Federal Register.

Consumer Protection Roundup

April 9, 2026



By Mercedes Kelley Tunstall
Partner | Financial Regulation

In this article, we'll delve into recent news on financial consumer protection, but before doing so, we'll provide an update on the Consumer Financial Protection Bureau (CFPB).

We reported [in the January 15 issue of *Cabinet*](#) that Acting Director Russell Vought asked for funding to keep the CFPB open. Since then, not much has happened at the agency, other than its continued litigation with the National Treasury Employees Union. Citing the need to conform with the funding limits and restricted scope allocated to the CFPB in the One Big Beautiful Bill, the CFPB told the U.S. Court of Appeals for the District of Columbia that it was proposing to “right-size” the agency and proposed a cut to 556 employees, down from 1,100 employees currently, and from the 1,700 employees the CFPB had at the end of the Biden administration.

With more than year having gone by while the CFPB has been hobbled, we are now beginning to see how much other agencies and states are jumping into the breach left behind. Keeping in mind that new investigations can take many months before becoming public, so far we have not seen much activity in financial consumer protection at the state level,

However, we have seen the Federal Trade Commission (FTC) take some actions in the space, and based upon what has been submitted to Congress for its budget next year, it looks as though the FTC is planning to continue being similarly active. This is because in its budget request submitted to Congress (i.e., the FTC is subject to allocations every year), they have proposed to give the Financial Services section of the FTC's Bureau of Consumer Protection one of the largest budget increases

To date, the FTC has been mostly focused upon taking action to prevent companies from facilitating fraud, such as when it [took action against U.K.-based payment processor, Paddle.com](#), to prevent them from continuing process payment for telemarketers engaged in fraudulent tech-support. And, more recently, the FTC has [issued warning letters](#) to PayPal, Stripe, Visa and Mastercard warning them to be careful to ensure that their rules and policies do not deny consumers access to financial products or services based upon their “political or religious views” or other “First Amendment-protected activity” in a manner that would violate the FTC Act, and admonishing them to not “countenance unlawful debanking” by financial institutions with which they interact.