Our Take

PwC's Financial Services Risk & Regulation Update

4.10.26 Topics: AML | Stablecoins | On our radar

1 FinCEN proposes AML overhaul

What happened? On April 7th, Treasury's Financial Crimes Enforcement Network (FinCEN) issued a proposal outlining significant changes to the anti-money laundering and (AML) regulatory framework for a wide range of institutions subject to the Bank Secrecy Act (BSA) including banks, money services businesses, credit card issuers, casinos, loan and finance companies and certain insurance companies.

The same day, the OCC, FDIC and NCUA issued a joint proposal to implement many of the changes to FinCEN's proposed rule.

What would the proposal do? It would adjust the AML framework in a number of ways, including:

- **Compliance expectations focused on effectiveness.** Financial institutions would still be required to maintain AML programs consistent with existing expectations, but examiners would focus on whether those programs are operating effectively. Significant enforcement actions would be tied to "material" or "systemic" failures, rather than isolated or technical issues.
- **Risk assessments elevated.** Financial institutions would be required to have risk assessment processes that (1) comprehensively evaluate AML risks; (2) review and, as appropriate, incorporate FinCEN's AML/CFT Priorities; and (3) be updated to reflect any changes that impact risk. Compared with FinCEN's previous 2024 proposal, the proposal's risk assessment expectations are significantly more flexible, permitting financial institutions to determine the design, frequency and scope of risk assessments.
- **Greater flexibility in program design and resource allocation.** Financial institutions would be able to determine the design, scope, and frequency of risk assessments and how resources are allocated, provided those decisions are reasonable and tied to risk.
- **A new coordination requirement for significant enforcement actions.** Before taking a significant AML-related supervisory action, banking regulators would be required to notify FinCEN at least 30 days in advance and provide an opportunity for input.
- **A clarification of the role of independent testing.** Internal audit or external testing functions would be expected to assess whether the AML program is established and maintained using objective criteria, rather than challenging underlying risk or design decisions. The proposal states that auditors should not substitute their subjective judgment in place of the financial institution.
- **Encouraging responsible innovation.** FinCEN encourages financial institutions to use innovative technologies as part of their AML programs and provides that financial institutions that responsibly experiment with innovation will not incur any additional risk of enforcement actions.

What's next? Comments on the proposal are due by June 9th. As proposed, financial institutions would be required to comply 12 months following the issuance of a final rule.

Our Take

FinCEN turns focus away from check-the-box compliance toward defensible program effectiveness and deference to firm judgment

This proposal is consistent with the direction of change to regulation and supervision that we have seen from Treasury and the leadership of the banking agencies: focusing on material risk, deprioritizing check-the-box requirements, and allowing financial institutions to define, based on a risk view, what "good" looks like and allocate resources accordingly. That change raises the importance of informed judgment across the program, and firms will need to integrate feedback provided by law enforcement and government agencies in determining the proper risk levels.

Risk assessments become the foundation not just for documentation, but for decisions on monitoring, staffing, governance, and escalation. At the same time, the proposal makes clear that internal audit should not impose subjective judgment on AML program design, but it should instead assess programs against objective criteria.

Financial institutions will have more flexibility in how they design and resource their programs, but they will also need to demonstrate that those decisions are consistent, supported by risk, and able to withstand challenge from experienced oversight functions. That will require strong expertise in second line functions and active engagement from Boards to ensure that risk-based decisions are credible and defensible.

Financial institutions will be empowered to decide where to focus – and where to cut

The proposal's deference to financial institutions' risk-based decisions creates an opportunity to shift resources away from lower-value, process-driven activity and toward areas that present the greatest risk. In practice, that will require a clearer and more consistent linkage between risk assessments and how programs are designed and operated, including monitoring, staffing, governance, and escalation decisions.

As financial institutions adjust, they should consider where resources could be reallocated to technologies such as AI and machine learning, blockchain analytics, and more advanced data integration. These tools can improve segmentation, detection, and decision traceability, while also creating opportunities to automate lower-value activities such as routine monitoring, alert handling, and reporting.

What should financial institutions do now?

1. **Review and validate the risk assessment framework.** Given the heavy emphasis on targeting high-risk activities, financial institutions should make sure that their risk assessments cover all relevant products and services, incorporate the National Priorities, and are subject to effective check and challenge. They should also determine how feedback is sourced from law enforcement and courts along with how it informs risk assessments and tools.
2. **Consider new tools and approaches.** Consider whether data analytics, advanced segmentation, or other emerging methods could enhance how risk is identified, measured, and linked to controls. Assess opportunities to automate alert triage, case management, and the filing of lower-risk SARs, reducing manual effort and allowing resources to focus on higher-risk activity.
3. **Bolster governance and accountability.** As the proposal places significant emphasis on financial institutions' abilities to assess and determine mitigation efforts for their own risks, the second line will need to be enhanced to oversee and challenge these efforts. This includes determining whether the second line has sufficient expertise and resources to provide effective oversight.
4. **Deemphasize low value/high burden activities.** The flexibility given to financial institutions in resource allocation provide an opportunity to deemphasize high-intensity, low-value activities that previously may have triggered supervisory actions and required remediation (e.g., completeness of alert dispositioning narratives) to instead invest in mitigating more prominent risks.

2 Stablecoin spotlight: FinCEN, OFAC and FDIC release GENIUS Act proposals

What happened? The following notable events took place this week regarding stablecoins:

- On April 8th, FinCEN and OFAC issued a joint proposal to clarify that stablecoin issuers under the GENIUS Act are subject to the BSA and are required to maintain effective AML and sanctions compliance programs. Notably, the proposal marks the first time OFAC has explicitly required in a proposed regulation that a specific category of financial institutions maintain an effective sanctions compliance program.
- On April 7th, the FDIC issued a proposal that would establish a prudential regulatory framework for FDIC-supervised stablecoin issuers under the GENUS Act.
- On April 8th, the White House's Council of Economic Advisors released a report finding that eliminating stablecoin yield would increase bank lending by $2.1 billion, which translates into an increase in lending of 0.02%.

What does the FinCEN and OFAC proposal contain? Under the proposal, stablecoin issues would be required to maintain risk-based AML and sanctions compliance programs, with non-compliance resulting in penalties of $100,000 per day. In addition to baseline generally applicable AML and sanctions compliance expectations, notable considerations include:

- **SAR filings.** Stablecoin issuers would be required to file SARs subject to a proposed $5,000 reporting threshold, but the proposal would not extend these obligations to certain secondary market transactions between third parties that merely interact with a smart contract.
- **Due diligence for higher-risk customers.** The proposal explains that stablecoin issuers would need to conduct enhanced due diligence on correspondent accounts for foreign financial institutions and private banking accounts. While the proposal does not require that financial institutions monitor secondary market activity, it notes that understanding the secondary market activity certain customers engage in may be a necessary part of customer due diligence.
- **Technical capabilities.** Stablecoin issuers would need to have the ability to comply with lawful orders and block, freeze or reject impermissible transactions, including capabilities related to smart contracts, digital wallets and private keys.
- **Internal audit capabilities.** Under the proposal, stablecoin issuers would be required to have an independent audit that assesses both the AML and sanctions programs. Notably, the proposal states that "in OFAC's experience, internal audits can lack the independence, expertise, and resources to conduct objective and thorough evaluations of an entity's own compliance efforts."

What does the FDIC proposal contain? Most of the requirements around the prudential framework mirror the OCC's February proposal (see *Our Take* here), including 1:1 reserve requirements, a prohibition on the payment of yield or interest, a 12-month operational backstop requirement, a two-day redemption requirement, and similar disclosure requirements. Beyond these requirements, the FDIC's proposal:

- **Clarifies the treatment of "tokenized deposits."** The proposal explains that regardless of whether a digital asset is labelled as a tokenized deposit, if it in effect mirrors the definition of a "deposit" it will be treated as such for regulatory purposes.
- **Clarifies pass-through insurance for reserve deposits.** Under the proposal, deposits held as stablecoin reserves at insured depository institutions would be insured to the stablecoin issuer under corporate deposit rules and would not extend to stablecoin holders on a pass-through basis.

What's next? Both proposals will be open for comments until June 9, 2026.

Our Take

Stablecoin issuers are now on notice with regard to AML and sanctions responsibilities

FinCEN and OFAC's joint proposal significantly reduces ambiguity for stablecoin issuers, creating specific and enforceable requirements with substantial daily penalties. Stablecoin issuers should enhance their programs now, considering the following key areas:

- **Establishing an OFAC sanctions compliance program.** While many stablecoin issuers have sanctions compliance embedded into their overall risk and compliance programs, many do not have formal programs that follow the "five pillars:" management commitment, risk assessment, internal controls, testing and auditing, and training. While OFAC will not expect "check-the-box compliance" and will grant financial institutions flexibility in implementing their sanctions compliance program, financial institutions should nevertheless ensure that they are conducting and documenting all five pillars.
- **Developing technical capabilities for on-chain enforcement.** Issuers will need to have the ability to block, freeze, burn, and reject transactions with sanctioned parties. While this will be a straightforward exercise for listed, sanctioned wallets, it will be far more challenging – and fraught with potential litigation risks – in more gray areas. This will include determining to what extent blocking or rejecting secondary market transactions is necessary
- **Enhancing internal audit capabilities for sanctions and digital assets.** Internal audit teams may lack the technical knowledge to audit smart contract functionality, wallet screening process and the sanctions-specific risks associated with digital assets. Stablecoin issuers should invest in hiring the appropriate staff, developing and/or sourcing tools and providing training to fill these gaps.
- **Establish a defensible approach to secondary market trading under the FinCEN requirements.** While FinCEN has indicated that direct secondary market monitoring is not required, the expectation that firms maintain a reasonable understanding of their customers' secondary market activity creates an obligation that must be addressed thoughtfully and documented clearly.

The FDIC takes the OCC's approach to stablecoins – but the battle over yield is not over

The FDIC's proposal contains few surprises as it largely reflects the prudential framework of the OCC's proposal and recent remarks from Chair Travis Hill on pass-through insurance coverage. If the proposal is finalized as-is, issuers holding reserves in insured deposits will be limited to the $250,000 cap on deposit insurance per depository bank, so large issuers may not be able to obtain sufficient insured deposit capacity for reserves. As pass-through coverage is the feature that can make end users (in this case, stablecoin holders) feel they have deposit-level protection even when funds are held through an intermediary, firms should determine how to clearly explain to their customers what protections exist and avoid any statements that may misrepresent that stablecoin holders would have deposit insurance protection.

Meanwhile, the proposal's mirroring of the OCC proposal's prohibition on paying interest or yield contrasts with the White House's report from earlier this week asserting that such yield payments would have negligible impact to banks. This issue continues to be a subject of great controversy, with stakeholders for and against allowing yield commenting on the OCC's recent proposal and the issue stalling the passage of the CLARITY Act in Congress. Now with the White House (ever so slightly) putting its finger on the scale, this issue is far from settled.

On our radar

FDIC and OCC finalize rule removing reputation risk from supervisory frameworks. On April 7th, the FDIC and the OCC issued a joint final rule prohibiting the use of reputation risk as a basis for supervisory action. The rule bars regulators from taking adverse action or encouraging institutions to restrict customer relationships based on political, social, or religious views, or other lawful activities, and codifies changes to supervisory practices in response to prior executive direction. See previous Our Take for additional details.

CFTC seeks to block state enforcement actions against prediction markets. On April 9th, the CFTC filed a motion in federal court seeking a preliminary injunction and temporary restraining order to halt Arizona's application of state criminal and gambling laws to CFTC-regulated prediction markets. The action is part of a broader lawsuit asserting that the Commodity Exchange Act grants the CFTC exclusive jurisdiction over event contracts and preempts state enforcement against federally regulated exchanges.

Fed proposes expansion of FedNow to support intermediary institutions. On April 8th, the Fed issued a proposal to allow FedNow participants to use intermediary institutions, such as correspondent banks, in payment transactions. The proposal would enable participants to designate intermediary banks in payment orders, facilitating transfers that involve multiple institutions, including those outside the United States, and would update technical and operational requirements to support this functionality. Comments are due by June 9th, 2026.

Treasury launches cybersecurity information sharing initiative for digital asset firms. On April 9th, the U.S. Department of the Treasury announced a new initiative to provide eligible digital asset firms and industry organizations with access to government cybersecurity threat information. The program is intended to enhance firms' ability to identify, prevent, and respond to cyber threats and extends information sharing capabilities currently available to traditional financial institutions.

Additional information

For additional information on the Our Take series or PwC's Risk and Regulatory Practice please contact:

Amanda Cox
Financial Services Risk & Regulatory Leader
773 456 5019
amanda.cox@pwc.com

Adam Gilbert
Global Senior Regulatory Advisor
914 882 2851
adam.gilbert@pwc.com

Martha Pampel
Managing Director
312 833 3385
martha.pampel@pwc.com

Contributing authors: Eric Lorber, Vasilios Chrisos, Michael Lammie, Jim Daly, Gregory Calpakis, Tracy Manella, Hannah Baranowski, Matt Coughlin, Michael Jobling, Matt Blumenfeld, Andrew Hillyer, Stein Berre, Michael Horn, Tanya Pazhitnykh, and Katie Wen.

pwc.com