ALM | LAW.COM

New York Law Journal

A Practitioner's Guide to FinCEN's New AML/CFT Rules

By Laurel Loomis Rimon
May 1, 2026

FinCEN's proposed overhaul of the Bank Secrecy Act's AML/CFT program requirements is billed as reducing the regulatory burden, setting a higher bar for enforcement actions, and providing a modernized, risk-based framework that moves away from the "zero-tolerance focus on process and documentation" that the current Treasury Secretary has publicly criticized. That framing is not wrong, but it is incomplete in ways that matter significantly to fintech companies, crypto platforms, and the banks that partner with them.

Although FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism Programs NPRM is still subject to public comment and revisions before being finalized, it already provides a view of the enforcement roadmap FinCEN and federal and state banking regulators intend to pursue, particularly in light of the significant growth in financial service innovation, technology, and partner relationships.

For both supervisory and enforcement resilience, financial institutions should focus on building a record of compliance meeting the aspects described below.

(Credit: chee siong teh/Adobe Stock)

Although FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism Programs NPRM is still subject to public comment and revisions before being finalized, it already provides a view of the enforcement roadmap FinCEN and federal and state banking regulators intend to pursue

The Establish/Maintain Framework: A New Predicate for Enforcement

The centerpiece of the proposed rule is a two-prong framework requiring financial institutions to both "establish" and "maintain" an effective AML/CFT program. Establishing a program means designing it, i.e. creating the risk-based policies, procedures, and controls, the risk assessment processes, the testing function, the designated compliance officer, and the training program that together constitute a compliant program architecture. Maintaining it means implementing that program in all material respects on an ongoing basis.

This framework applies to all covered financial institutions. For banks with mature, well-documented (established) programs, it carries the additional benefit of limiting significant supervisory and enforcement actions to instances where implementation has led to "significant or systemic failures."

As a practical matter, this is not a major shift in enforcement—significant BSA actions have always focused on systemic failures—but it may have meaningful impact in the supervisory context by limiting examiners who might otherwise pursue findings and remediation requirements that would not rise to that level.

Paired with the proposed FinCEN pre-clearance mechanism requiring federal banking agencies to provide FinCEN written notice at least 30 days before taking certain significant AML/CFT supervisory actions and to consider FinCEN's input on program effectiveness, the proposed rule gives banks a meaningful procedural tool to push back against examiner overreach.

For non-bank financial institutions such as MSBs, money transmitters, broker-dealers, and crypto companies operating under state licenses, the proposed rule does not provide the same enforcement cushion.

FinCEN has explicitly invited comment on whether to extend those protections, but the NPRM makes them only applicable to banks. Non-banks will therefore have broader exposure on both the "establishing" and "maintaining" prongs.

FinCEN also explicitly warns against "paper programs," or those that meet technical requirements on their face but are not genuinely operative. This warning applies most acutely to less mature financial services companies that may not have built out the staffing and compliance infrastructure expected by regulators and required to meet BSA obligations.

Although now explicit, regulators have always been alert to paper programs, as the gap between policies and procedures on the one hand and operations and practices on the other, is an easy enforcement focus.

Dynamic Risk Assessment: The Record You Need Before the Subpoena

Perhaps the most operationally demanding element of the proposed rule, and the one most likely to create enforcement exposure for rapidly growing companies, is the requirement that risk assessment processes be updated "promptly upon any change that the financial institution knows or has reason to know significantly changes" its money laundering/terrorist financing risks. This is not a periodic review obligation. It is a continuous one, triggered by material changes in products, services, customers, geographies, or distribution channels.

For fintech and crypto companies, and the banks who partner with them, business models are defined by rapid product iteration and customer base expansion. A company that has launched a new lending product, onboarded a new category of business customers, or expanded into a new jurisdiction without formally revisiting its risk assessment (and updating necessary controls) is not maintaining a properly established program under the proposed framework.

When investigators reconstruct the compliance history during an investigation, the absence of documented risk assessment updates at each of those inflection points will be exactly the kind of gap to drive enforcement risk.

The documentation obligation goes further. The rule requires that internal policies, procedures, and controls be not merely written, but "reasonably designed," meaning they must actually reflect the institution's risk profile at the time.

If program testing surfaces a high-risk customer type or activity and the institution takes no action to revise its controls, FinCEN's view is that the program will not be considered reasonably designed. For institutions whose compliance programs were built for an earlier version of their business, that gap also creates enforcement risk.

Where Debanking Fits In

The NPRM's risk-based framework has direct implications for financial institutions navigating the current administration's focus on debanking.

The proposed rule explicitly frames a properly established, risk-based AML/CFT program as the appropriate mechanism for customer relationship decisions, meaning that account and service decisions must be grounded in documented ML/TF risk assessment rather than broad categorical exclusions based on reputation or political pressure.

The significance of this aspect is highlighted by the OCC's December 2025preliminary report on its debanking investigation focused on what it alleged were policies restricting access to certain industry sectors (including digital asset activities) based

primarily on reputation risk considerations rather than individualized risk determinations. In this report, the OCC indicated it may refer any "unlawful debanking activities" it uncovers to DOJ.

The U.S.-Based Officer Requirement

The proposed rule sharpens an accountability requirement that was implemented in the AML Act of 2020 at 31 U.S.C. 5318(h)(5) but has not yet been specifically enforced. That is, the duty to establish and maintain an AML/CFT program "remain[s] the responsibility of, and [must] be performed by, persons in the United States" who are accessible to FinCEN and the appropriate federal regulator.

The proposed rule translates that statutory obligation into a concrete requirement for a designated AML/CFT officer to be located in the United States with genuine program authority. Offshore compliance teams and outsourced AML operations are allowed, but the designated officer must be in the United States.

The NPRM's preamble gives meaningful insight into what FinCEN will be looking for, stating that the AML/CFT officer must be "qualified for that role and not overburdened with other responsibilities," must have "decision-making capability" and "sufficient functional stature within the organization," and must have access to adequate compliance funds, staffing, and technology commensurate with the institution's risk profile.

For fintech and crypto companies that have assigned compliance responsibilities to a general counsel, a CFO, or a part-time consultant, arrangements common in early-stage and growth-stage companies, this standard reflects FinCEN's supervisory expectations and signals where enforcement scrutiny will fall.

Technology and Innovation: A Double-Edged Sword

The NPRM's treatment of technology is among its most forward-looking elements, and financial institutions should read it carefully.

FinCEN explicitly encourages institutions to consider whether machine learning, generative AI, blockchain analytics, digital identity tools, and APIs might strengthen their AML/CFT programs, and states directly that institutions that responsibly experiment with innovative technologies will not face additional enforcement risk solely because of that experimentation. For crypto companies, FinCEN notes that these tools may be "especially useful in countering illicit finance activity involving digital assets," a signal that compliance infrastructure for digital asset businesses is expected to evolve alongside the sector itself.

At the same time, FinCEN's embrace of innovation raises the stakes for institutions that have not meaningfully engaged with new technologies. If the tools to build a more effective, risk-calibrated program are widely available and effective, and an institution has not considered whether they apply to its risk profile, or sought to implement them, that gap may create exposure. This is a dynamic familiar to fintech and crypto companies that have wrestled with the challenge of geofencing and IP blocking over recent years.

Building the Record Now

This NPRM should prompt every financial institution, particularly every fintech, crypto company, and bank with significant non-bank partnerships, to ask a hard question.

If a government subpoena arrived tomorrow, would existing compliance documentation reflect a properly designed, established, and operationalized AML/CFT program?

That means examining whether the program reflects the institution's actual current risk profile, verifying that risk assessment updates and corresponding changes to controls were documented upon material inflection points in the business, and having well-documented staffing, vendor, and tools analyses.

For financial institutions that have been building compliance programs with one eye on regulatory expectations and another on business growth, the time to close the gap between those two imperatives is before the subpoena arrives.

Laurel Loomis Rimon *is a partner at Jenner & Block.*