FINANCIAL TECHNOLOGY ASSOCIATION

June 9, 2026

Chief Counsel's Office
Attn: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, DC 20219

Ms. Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314

Ms. Jennifer M. Jones
Deputy Executive Secretary
Attn: Comments/Legal OES
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Regulatory and Strategic Affairs Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

FTA Comment Letter Responding to the Agencies' AML Program Rule Proposal
(Docket Nos. FINCEN-2026-0034, OCC-2024-0005; RINs 1506-AB72, 3064-AF34, 3133-AG08)

The Financial Technology Association (FTA) welcomes the opportunity to respond to the Financial Crimes Enforcement Network (FinCEN), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency, and National Credit Union Administration's (NCUA) proposed rule to fundamentally reform anti-money laundering and countering the financing of terrorism (AML/CFT) program requirements for financial institutions subject to the Bank Secrecy Act (BSA). Our members — including banks, money services businesses (MSBs), broker-dealers, and other fintech entities covered by the BSA — recognize the importance of this rulemaking for setting the parameters of how institutions detect and deter illicit financial activity.

We broadly support the direction of this proposal and appreciate that the Agencies have seriously considered the feedback received in response to the 2024 Program Rule NPRM. We particularly welcome the proposed rule's emphasis on effective, risk-based AML/CFT programs, the explicit recognition that financial institutions should direct more resources toward higher-risk activity and fewer toward lower-risk activity, the distinction between program establishment and maintenance, and FinCEN's affirmative encouragement of innovative technologies including AI and machine learning.

That said, we believe additional changes to the proposed could help ensure that covered institutions have a clear understanding of, and are comfortable calibrating their programs to, a genuinely risk-based approach. In particular, we would recommend the following:

- The Agencies should embed resource redeployment flexibility and good-faith compliance protections directly in the regulatory text;

- FinCEN should tailor its approach to establishing National AML/CFT Priorities to further reinforce the risk-based framework;
- The Agencies should use this rulemaking cycle to modernize SAR filing requirements and enhance law enforcement feedback mechanisms to increase the real-world utility of AML/CFT reporting;
- The "significant or systemic" enforcement threshold should apply to all financial institutions;
- The Agencies, where appropriate, should provide affirmative, durable guidance on AI/ML tools and digital assets;
- The Agencies should provide operational clarity on what program effectiveness looks like in practice;
- FinCEN should clarify how the board approval requirement applies to multi-entity corporate structures; and
- The final rule's effective date should be set at least 24 months from issuance, with a phased pathway for institutions implementing innovative compliance technologies.

These recommendations, taken together, will ensure the proposed rule delivers on its stated modernization goals by pairing clear regulatory text with targeted examiner training to make the U.S. AML/CFT regime more efficient and effective.

I. The Agencies Should Embed Resource Redeployment Flexibility and Good-Faith Protections Directly in the Regulatory Text

We appreciate the emphasis in the preamble of the proposed rule on risk-based resource allocation and the principle that institutions should be able to deprioritize lower-risk areas without fear of supervisory criticism. These are welcome and important signals. However, additional direction in the regulatory text is needed to fully implement this shift.

Currently, financial institutions devote substantial resources to their AML/CFT programs but lack the regulatory certainty to actually redeploy those resources from lower-risk to higher-risk areas within the existing supervision and examination environment. While the Anti-Money Laundering Act of 2020 (AML Act) and this proposal begin to address these concerns, the regulatory text could go farther to give institutions greater comfort around redeployment. We recommend that the proposed regulatory text be modified to explicitly state that if an institution makes a data-driven decision to deprioritize a segment based on its risk assessment, examiners will not retroactively penalize the institution for isolated misses in that segment. Concrete language expressly granting covered institutions such flexibility will further enable them to rebalance their programs — and will give examiners a clear basis against which to assess programs, thereby increasing regulatory certainty for institutions that they will not face undue scrutiny for making risk-based programmatic decisions.
Examiner training and updated examination frameworks will be equally critical to making this shift a reality. Working with industry, exam guidance and expectations will need to be revised to

ensure the appropriate calibration of regulatory assessment approaches. This includes training examiners on how to evaluate programs that use innovative technologies.

Any final rule should also draw a clear line between a program design failure and an operational execution error. As currently drafted, the rule's continuous feedback loop requirement — mandating that both risk assessments and internal controls be updated whenever material changes in risk are identified — creates significant evidentiary demands and leaves the boundary between these two categories vague. Without an explicit definition, examiners retain broad discretion to recharacterize what is functionally an isolated implementation gap as a foundational deficiency in program design, stripping institutions of the maintenance-related protections the rule is otherwise intended to provide. FinCEN should make clear in the regulatory text that where an institution has built a reasonably structured process for identifying and responding to risk changes, a discrete lapse in updating or documenting a particular control is a maintenance issue — not evidence that the program was never properly established. In particular, we recommend adding the following language to any final rule “provided that a financial institution has established reasonably designed risk assessment processes, an isolated or non-systemic delay in updating or documenting a specific internal control shall be considered a deficiency in program implementation, and shall not, standing alone, constitute a failure to establish the AML/CFT program.”

Furthermore, the Agencies should also acknowledge the significant documentation burden the proposed continuous update framework places on institutions and calibrate examiner expectations accordingly. Under the proposed structure, institutions must be prepared to demonstrate, through auditable records, that specific risk signals triggered assessment updates, and that those updates in turn drove changes to control design. This represents a meaningful shift in where compliance resources are consumed — away from executing controls and toward documenting the rationale behind them. Examiners should be directed to evaluate the overall effectiveness of an institution's risk-based program rather than penalizing institutions for documentation that does not conform to any particular format or sequencing preference.

Finally, certain elements of the AML/CFT regime has been viewed as a "check-the-box" exercise because of the supervisory approach. However, recent changes to the Federal Financial Institutions Examination Council’s BSA/AML Examination Manual as well as the proposed changes to the AML Program Rule will help financial institutions move away from that approach. To further encourage this shift in culture, we would recommend inclusion of a statement in the regulatory text that financial institutions' good-faith application of the rule's expectations will be found compliant by examiners. This language would further support the Agencies’ risk-based shift while also promoting a strong compliance program. Separately, given the role of independent audits in evaluating an institution’s AML program, we believe it’s similarly important for the regulatory text to make clear that this cultural shift extends to the audit function.

A. The Agencies Should Preserve Flexibility for Global Operational Models

We believe the Agencies have struck the right balance in the proposed rule with regard to the U.S.-based duty requirement in the AML Act and that no further clarification is needed regarding what duties personnel outside the United States may perform. Retaining the proposed language as drafted provides essential flexibility for financial institutions to structure their global operations effectively. A prescriptive list could inadvertently restrict institutions from scaling their compliance programs efficiently and disrupt established global operational hubs.

II. FinCEN Should Tailor Its Approach to Establishing National AML/CFT Priorities to Further Reinforce the Risk-Based Framework

The proposed rule requires financial institutions to review and, as appropriate, incorporate the National AML/CFT Priorities into their risk assessment processes - in line with Congress's direction in the AML Act. We recognize the importance of the National AML/CFT Priorities to guide a financial institution's programs and believe that in order to truly meet the statutory intent, further refinement to how the Priorities are formulated and applied is needed to help focus institutions' compliance obligations.

The current list of National AML/CFT Priorities is broad and does not provide the level of specificity that many institutions need to meaningfully calibrate their programs. Requiring institutions to consider the full range of possible illicit financial risks beyond the Priorities — without limiting that requirement to "significant" risks relevant to their business activities — risks re-creating the check-the-box dynamic the proposed rule is meant to eliminate. Institutions facing an effectively unlimited risk universe cannot make meaningful risk-based resource allocation decisions.

We continue to recommend that FinCEN reconsider how it establishes and revises the National AML/CFT Priorities, further tailoring it to current U.S. law enforcement and national security focus areas, and modeled after the interagency process used for the National Intelligence Priorities Framework. That framework specifies what information collectors should focus on, identifies key questions to drive useful collection, and establishes who is best positioned to address each priority. Applied to AML/CFT, such a framework would allow FinCEN to specify which illicit financial risks particular types of institutions are best positioned to address, how BSA reporting from those institutions should be used to identify and measure trends, and what emerging threats institutions should be prepared to respond to. The result would be a priorities regime that actually guides resource allocation rather than expanding it.

FinCEN, working with federal financial regulators, should also provide practical guidance to help institutions translate high-level national threat categories into actionable internal controls. One approach would be to anchor the Priorities to a threats-and-vulnerabilities methodology — the same analytical foundation Treasury employs in its national risk assessments. Under this model,

institutions would treat the published Priorities as a defined set of threats and evaluate them against their own specific operational vulnerabilities, such as the nature of their customer onboarding processes or the geographic reach of their banking activity. Concrete worked examples — showing how an institution moves from a national priority to an identified product vulnerability, gap analysis, and into a documented program update — would give institutions a reproducible framework and help ensure the incorporation exercise drives program improvement and avoids becoming the surface-level review the proposed rule explicitly warns against.

At a minimum, the final rule should clarify that institutions are required to account for only those risks that are "significant" to their specific business activities and risk profile. Relatedly, the Agencies should clarify how institutions are expected to update their programs when the Priorities change. As the AML Act envisions material updates to the Priorities to reflect changes in the threat environment, institutions will need reasonable time to assess the implications of any such changes, revise their policies and procedures, and test and calibrate the resulting programmatic adjustments. The final rule should specify that institutions will have at least one year to comply with significant updates to the Priorities.

The Agencies should also clarify what they expect as the proposed rule refers to risk assessment "processes" in the plural. The use of the plural is appropriate and reflects how sophisticated institutions actually operate — running distinct but related assessments across products, customers, geographies, and channels simultaneously. However, without further guidance, the phrasing could be read to require that every individual process be formally updated any time the institution's overall risk profile shifts. The Agencies should make explicit that a change triggering one process does not automatically require parallel updates across all others, and that institutions retain discretion to determine which specific processes are implicated by a given change and require revision.

The Agencies should also reconsider the language they use to define the threshold for triggering risk assessment updates. The proposed standard — requiring updates when an institution "knows or has reason to know" that its risks have "significantly changed" — introduces interpretive uncertainty that could expose institutions to examiner disagreement about whether a given change crossed the threshold. Substituting "materially changes" would provide a more defensible standard, one with an established meaning in legal and audit contexts that ties the update obligation to changes that actually affect an institution's overall risk profile or control framework, rather than routine fluctuations in transaction volume or activity mix. Separately, the Agencies should clarify that the obligation to act "promptly" does not impose a fixed calendar deadline. For institutions operating technology-driven compliance programs, translating a newly identified risk into a validated, tested, and deployed control update requires adequate time for governance review and quality assurance. A reasonable-timeframe standard — calibrated to the complexity of the required change and the nature of the risk — would better reflect operational reality than a bright-line time requirement.

III. The Agencies Should Use This Rulemaking Cycle to Modernize SAR Requirements and Enhance Law Enforcement Feedback

While the proposed rule does not directly address SAR filing thresholds or processes, we urge FinCEN to treat this rulemaking cycle as an opportunity to address these issues in parallel. As we have previously noted, the current SAR framework was built for a traditional banking environment and does not reflect the volume, velocity, or risk profile of modern payments platforms. Without changes to SAR requirements, the shift to a risk-based compliance program will be incomplete.

The current reporting environment drives defensive filing - a genuinely risk-based AML/CFT program should produce BSA reports that are useful to law enforcement. FinCEN should work with industry, law enforcement and federal financial regulators to create a differentiated framework that treats different types of suspicious activity reporting differently, in line with their actual utility to law enforcement.

Increasing law enforcement feedback will also be essential to making this work in practice. Without concrete feedback on which filings are useful, institutions cannot calibrate their monitoring systems or their reporting judgments effectively. We encourage FinCEN to establish simple, scalable feedback mechanisms — including the kind of basic utility signals (such as a confirmation that a SAR contributed to an investigation) that have been discussed in the industry for years. FinCEN should also expand its dissemination of trend information and typologies, and broaden law enforcement engagement with institutions of all sizes, including smaller fintechs and MSBs that may not have access to the regional engagement opportunities available to larger banks.

Finally, we recommend that FinCEN modernize the 314(b) portal to allow participating institutions to communicate directly with one another. Today, communication under 314(b) is slower than the typologies information sharing is meant to address, driven by documentation and other requirements. Direct communication, along with a strong template for sharing useful information, would significantly increase the operational value of the program for real-time fraud and AML coordination, particularly for platforms processing high volumes of fast-moving transactions where speed of information sharing is critical. To incentivize financial institution use of 314(b) given its voluntary nature, institutions could receive credit within the supervisory and exam process for participation in such a program. More generally, credit can also be exemplified through law enforcement letters and other activities that demonstrate institutions' proactive AML/CFT efforts.

Beyond improvements to the 314(b) portal, FinCEN should use any attending rulemaking to advance a broader vision of cross-sector information sharing. Financial crimes — particularly fraud — increasingly originate outside the traditional banking system and migrate across payment platforms, telecommunications networks, and digital services before they manifest as

reportable activity at a financial institution. A regulatory framework that limits coordination to financial institution-to-financial institution reporting is structurally mismatched to this threat environment and also limits the utility of any information ultimately provided to law enforcement as cross-sectoral investigation and analysis provides enhanced leads. We would encourage FinCEN to work toward information sharing frameworks that facilitate timely, appropriately governed coordination across a wider set of participants — including payments platforms, technology providers, and other sectors with visibility into the early stages of fraud and illicit financial activity — so that BSA reporting can reflect a fuller picture of the underlying risk.

IV. The "Significant or Systemic" Enforcement Threshold Should Apply to All Financial Institutions

We strongly support the proposed rule's establishment of a "significant or systemic" threshold for AML/CFT enforcement and significant supervisory actions against banks that have properly established their programs. This is one of the most meaningful reforms in the proposal, and we urge the Agencies to preserve it in the final rule.

However, we are concerned that limiting this threshold to banks will create an uneven playing field that disadvantages MSBs, broker-dealers, fintechs, and other non-bank financial institutions that face compliance challenges of equivalent or greater complexity. Applying the framework unevenly will distort competition, and undermine the broader goal of a consistent, risk-based regulatory approach.

This disparity creates two distinct and concrete problems for non-bank financial institutions. First, it effectively forces MSBs and broker-dealers into a zero-tolerance compliance posture that the proposed rule is otherwise designed to move away from. These institutions operate at high transaction volumes using automated, rules-based systems; an isolated execution error — a temporary data mapping issue, a delayed alert — is by nature a maintenance problem, not a program failure. Without the protection the banks-only threshold provides, non-banks remain fully exposed to enforcement consequences for precisely the kinds of isolated errors the rule's establishment-versus-maintenance framework was designed to treat differently. Second, the asymmetry creates friction in the bank-fintech partnerships that underpin much of the U.S. payments ecosystem. Where a bank and its MSB partner experience the same operational error, a bank examiner may correctly treat it as a non-systemic maintenance issue while the MSB remains subject to full enforcement exposure for the identical gap. This inconsistency complicates due diligence relationships and distorts competitive dynamics. Therefore, we urge FinCEN to extend the "significant or systemic" threshold to all financial institutions subject to the program rule. The distinction between program establishment and maintenance — and the associated enforcement threshold — reflects sound policy that should apply across institution types.

We also request that FinCEN provide concrete examples — in the final rule or in accompanying examination guidance — of what does and does not constitute a "significant or systemic" failure. Without such examples, examiners will fill the gap with their own judgment and the threshold will prove difficult to enforce consistently in practice.

Relatedly, explicit guidance on what a "failure to establish" a program actually requires would similarly be useful. Because the establishment prong of the proposed rule is broad — encompassing the traditional program pillars, customer due diligence obligations, and the continuous risk assessment feedback loop — the potential for examiner overreach is significant. A single perceived deficiency in how an institution weighted a geographic risk factor, or a missed advisory in one cycle of risk assessment updates, should not be sufficient to support a finding that the program was never properly established. The Agencies should make clear that establishment failures are reserved for foundational deficiencies — the absence of a required program pillar, or a wholesale failure to conduct risk assessment processes — and that design disagreements or isolated documentation gaps do not meet that bar.

A related disparity exists wherein the proposed rule expressly provides that FinCEN will consider whether banks have provided highly useful information to law enforcement (to include SARs, 314(a) and 314(b) responses, and other cooperation) as a mitigating factor in pursuing enforcement action, but does not extend that same enforcement guideline to MSBs and other non-bank financial institutions. We respectfully submit there is no principled basis for treating cooperation with law enforcement as a mitigating factor for banks but not for MSBs and other non-bank financial institutions – especially where MSBs and non-bank financial institutions generate a significant amount of law enforcement leads via SARs and other information sharing tools. We urge FinCEN to explicitly extend this enforcement guideline to MSBs and other non-bank financial institutions, making clear that documented cooperation with law enforcement will be considered as a mitigating factor in the same manner it is for banks.

V. The Agencies, Where Appropriate, Should Provide Affirmative Regulatory Guidance on AI/ML Tools and Digital Assets

We strongly support the Agencies' encouragement of innovative compliance technologies, including machine learning, generative AI, blockchain analytics, and related tools. The proposed rule's recognition that institutions using innovative tools will not face adverse examination findings solely on that basis is an important and welcome step. However, positive signals in the preamble are not sufficient to change examiner behavior or provide institutions with the certainty they need to invest in these tools at scale.

Any final rule should include explicit language in the regulatory text — not just the preamble — confirming that AI/ML-based transaction monitoring satisfies the "reasonably designed" standard when the institution can demonstrate that the methodology is sound and the outputs are meaningful. FinCEN should also commit to developing examiner guidance that addresses

how AI/ML compliance tools should be evaluated, including training to ensure that examiners understand the operational characteristics of these systems and do not apply expectations built for rules-based monitoring to fundamentally different AI/ML architectures.

The Agencies should also provide guidance on how examiners should evaluate the outputs of AI/ML tools in practice. Institutions that deploy machine learning to triage the output of legacy rule-based monitoring systems — reducing false positive rates and freeing investigative capacity for higher-risk activity — are doing exactly what a risk-based program dictates. The Agencies should affirmatively recognize this kind of reallocation as a marker of program effectiveness, rather than leaving institutions to defend their technology choices against evaluation frameworks built for static, rules-based systems. More broadly, examiner guidance should direct assessors to evaluate innovative compliance tools based on what they produce — measurable reductions in low-value alerts, improved SAR quality, earlier identification of emerging typologies — rather than whether those tools conform to legacy model validation checklists that were designed for traditional financial models and are poorly suited to dynamic, adaptive systems. Giving institutions the confidence that their AI investments will be assessed on operational outcomes rather than procedural conformity is a prerequisite for the kind of technology adoption the Agencies' stated commitment to innovation is meant to encourage.

Separately, FinCEN should use this rulemaking to provide updated, durable guidance on the AML/CFT obligations of institutions operating in the digital asset space. The agency's existing guidance was developed at an earlier stage of the market's evolution and no longer adequately addresses the range of products, business models, and risk profiles that exist today. At a minimum, FinCEN could codify its existing positions on the treatment of non-custodial arrangements and clarify how travel rule obligations apply to digital asset transfers — two areas where regulatory ambiguity continues to produce inconsistent compliance approaches across the industry. More broadly, any final rule should provide a clear framework for how the risk-based approach applies to institutions operating across both traditional payment rails and digital asset infrastructure, so that compliance obligations scale appropriately to the actual risks each activity presents rather than defaulting to the most conservative possible interpretation of rules designed for a different context. In doing so, FinCEN should ensure that any frameworks addressing digital asset risks do not inadvertently alter or increase the data collection burdens for traditional fiat payment rails that may operate differently.

VI. The Agencies Should Provide Operational Clarity on What Program Effectiveness Looks Like in Practice

The proposed rule describes an effective AML/CFT program as one that is "established and maintained in accordance with applicable requirements" — a formulation that restates the compliance obligation without defining what a successful outcome actually looks like. This circularity creates a practical problem: without affirmative indicators of effectiveness, examiners facing a program with an isolated failure have no clear framework for evaluating whether the

overall program was nonetheless well-designed and functioning. The result is the kind of hindsight-driven, outcome-focused scrutiny that the proposed rule's emphasis on reasonably designed programs is intended to discourage.

The Agencies should address this by including a non-exhaustive list of operational outcomes that affirmatively demonstrate program effectiveness — for example, documented reductions in false positive rates, the proactive identification of previously unrecognized typologies, or a demonstrated record of generating BSA reports that contribute meaningfully to law enforcement investigations. Framing these as illustrative rather than mandatory is important: FinCEN should make clear that the absence of any particular metric does not, on its own, support a negative supervisory finding. The goal is to give both institutions and examiners a shared vision for what good looks like, without creating new quantitative thresholds that could be applied in a check-the-box fashion.

VII. FinCEN Should Clarify How the Board Approval Requirement Applies to Multi-Entity Corporate Structures

The proposed rule requires that an institution’s AML/CFT program be approved by the board of directors, an equivalent governing body, or appropriate senior management. We broadly support this requirement, but request clarification on how it is intended to operate in large, multi-entity corporate structures, including parent companies with licensed subsidiaries operating under an enterprise compliance program. FinCEN should confirm that approval of an enterprise AML/CFT program by appropriate senior management of a parent company can satisfy the requirement for subsidiaries subject to the program. Similarly, subsidiaries operating under enterprise compliance policies should retain the flexibility to make routine updates or adjustments to their programs without independently seeking board or senior management approval, provided those routine updates or adjustments are consistent with the enterprise framework approved by the board or senior management. Without these clarifications, institutions face the prospect of duplicative and resource inefficient approval obligations that are not consistent with the rule’s underlying policy goals.

VIII. The Final Rule's Effective Date Should Be Set at Least 24 Months from Issuance

We support the proposed 12-month implementation period as an improvement over the 2024 Program NPRM's six-month window. However, 12 months may be insufficient for institutions undergoing significant compliance technology transitions — particularly those replacing legacy rules-based monitoring systems with AI/ML platforms, which require substantial lead time for model development, validation, testing, and calibration.

We recommend that the Agencies set the final rule's effective date at least 24 months from issuance. This timeline is consistent with recent precedent for other significant AML/CFT rulemakings, including FinCEN's Customer Due Diligence Rule, and would allow institutions to

conduct thorough reviews of their products, services, and reporting frameworks, revise policies and procedures, and test and calibrate programmatic changes appropriately. Notably, for institutions that are already deploying advanced AI and machine learning, this will allow them to align these advanced tools with the new continuous 'establishment' standard, which will require a significant implementation period for governance reviews, quality assurance testing, model validation, and board approvals.

Separately, for institutions that are actively implementing AI/ML-based compliance tools, FinCEN should also build in a phased compliance pathway or formal no-action period, consistent with its stated commitment to encouraging responsible innovation. Such a pathway would allow the industry to modernize without the risk of enforcement exposure during the transition period, and would provide a meaningful signal that FinCEN's encouragement of innovation is reflected in its enforcement posture as well as its preamble.

The final rule should also address the interaction between the implementation timeline and future updates to the National AML/CFT Priorities. If significant Priorities updates occur shortly after the final rule takes effect, institutions should have at least one year from the date of those updates to incorporate the changes into their programs.

* * *

FTA members take their AML/CFT compliance obligations seriously and are committed to programs that genuinely detect and deter illicit financial activity. We believe this rulemaking is a meaningful step toward a modernized, risk-based AML/CFT framework. We would welcome the opportunity to discuss our comments further and work collaboratively with the Agencies as this rulemaking moves forward.

Respectfully submitted,

Angelena Bradfield
Head of Policy
Financial Technology Association