coinbase

To:

Andrea Gacki, Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, Virginia 22183

June 9, 2026

Submitted electronically via the Federal eRulemaking Portal (www.regulations.gov), Docket No. FINCEN-2026-0034, RIN 1506-AB72

Re: Anti-Money Laundering and Countering the Financing of Terrorism Programs, Docket No. FINCEN-2026-0034

Coinbase Global, Inc. ("**Coinbase**") appreciates the opportunity to respond to the U.S. Department of the Treasury's Notice of Proposed Rulemaking ("**NPRM**") on Anti-Money Laundering ("**AML**") and Countering the Financing of Terrorism ("**CFT**") Programs.

Coinbase is the most trusted service provider of crypto trading, custody, and infrastructure in the world. Founded in 2012 and publicly listed on the NASDAQ, we offer a secure interface for millions of verified retail and institutional investors globally. We are committed to building an open financial system and are doing so with the strongest regulatory compliance and security protocols available.

Coinbase fully supports the Department of the Treasury's efforts to modernize the U.S. AML/CTF regulatory framework and reduce compliance burden. We also appreciate the efforts being made by the Department of the Treasury to focus on effectiveness of compliance programs and encourage financial institutions to devote more attention and resources to higher risk products and services.

To assist the Department of the Treasury in these efforts, Coinbase is providing the following comments that are based on our extensive experience in implementing an effective AML/CTF compliance program. We look forward to working with the Department of the Treasury on this initiative going forward.

Yours sincerely,

Gerard Monusky

Gerard Monusky
Director - Financial Crimes Legal Department
Coinbase

Executive Summary

Coinbase supports the core objectives of the NPRM and commends the Department of the Treasury's efforts to modernize the U.S. AML/CTF regulatory framework through a more risk-based, outcomes-oriented approach to compliance. The proposed rule's emphasis on institutional flexibility, risk-based resource allocation, and encouragement of innovative compliance technologies represents a meaningful step forward. However, we believe that several provisions require clarification, expansion, or amendment to fully achieve these goals. Coinbase offers the following principal recommendations for strengthening the final rule.

Resource Allocation Flexibility Requires Corresponding Regulatory Reform

While the proposed rule's directive that financial institutions focus greater resources on higher-risk activities is a sound policy objective, it cannot be operationalized without corresponding amendments to existing Bank Secrecy Act ("**BSA**") regulations and corresponding guidance. So long as current rules impose rigid, risk-insensitive obligations – e.g., Suspicious Activity Report ("**SAR**") and Currency Transaction Report ("**CTR**") filing thresholds, non-flexible customer due diligence requirements – financial institutions will lack the regulatory confidence to meaningfully reallocate resources. The Financial Crimes Enforcement Network ("**FinCEN**") should pair this proposal with amendments to these attendant regulations and corresponding guidance that more directly recognizes risk-based KYC models that leverage emerging technologies and by codifying simplified due diligence for demonstrably low-risk customers.

The "Significant or Systemic Failure" Standard Must Apply to All Financial Institutions

While we support the proposed rule's limitation of enforcement to cases of "significant or systemic failures", the NPRM's proposal to only grant such relief to banks creates an unjustified disparity across the financial sector. There is no basis for creating such a disparity, as other financial institutions, such as Money Services Businesses ("**MSBs**") and broker-dealers, are subject to the same core AML/CTF Program Rules as banks. Subjecting financial institutions to different standards would also create an unlevel playing field, one in which banks may confidently explore use of innovative technologies in their AML/CTF programs, while non-bank financial institutions would need to maintain more conservative approaches due to the risk of enforcement for non-significant violations. This disparate approach does not go towards achieving the NPRM's ultimate goal, which is to modernize the *entire* U.S. AML/CTF regime.

The Innovation Safe Harbor Must Extend to Non-Bank Financial Institutions

The safe harbor for responsible use of innovative compliance technologies – currently codified only for banks – must be extended to all financial institutions. Digital asset MSBs and other non-banks are frequently the primary drivers of compliance innovation, pioneering uses of real-time blockchain analytics, AI-assisted SAR preparation, and decentralized digital identity verification. Excluding these institutions from safe harbor protections is inconsistent with the NPRM's stated objectives and risks chilling innovation in the sector most capable of advancing it.

Risk Assessment Standards Should Reflect Operational Reality

The risk assessment provisions would benefit from two targeted clarifications. First, the trigger for mandatory risk assessment updates should be based on material – rather than significant – changes, preventing the expectation of continuous updates driven by common and frequent operational changes. Second, FinCEN should issue supplemental guidance that timelines for implementing changes necessarily vary – from near-real-time for automated system adjustments to twelve months or more for enterprise-wide enhancements – and that the relevant supervisory question is whether an institution's response was proportionate to the risk involved.

Taken together, these recommendations reflect Coinbase's commitment to a regulatory framework that is rigorous, risk-based, and operationally effective across the entire financial ecosystem. We look forward to continued engagement with FinCEN as this rulemaking proceeds.

I. An "Effective" AML/CFT Program (V.B.)

NPRM Question 2: *The proposed rule reflects a determination by FinCEN that financial institutions are best placed to identify risks and allocate resources, and that providing them with greater discretion in these areas will improve the quality of AML/CFT compliance and reporting to law enforcement. Is this correct or should FinCEN consider adding more requirements regarding allocation of resources? How might financial institutions assess changes in the total allocation of resources devoted to an AML/CFT program in a changing risk and cost environment?*

Recommendation: FinCEN should grant financial institutions the discretion to allocate compliance resources based on risk without additional regulatory requirements, while simultaneously reducing burdens on low-risk activities through updated filing thresholds, digital-first KYC standards, AI guidance, and improved feedback mechanisms from law enforcement.

Coinbase agrees that financial institutions are best situated to identify risks and determine resource allocation, and that they should have broad discretion, within the parameters of the law, to design their AML/CTF Programs accordingly.

FinCEN should *not* add more requirements regarding resource allocation. Granting financial institutions the leeway to make risk-based decisions around where resources should be allocated – in order to protect the financial institution, its clients, and the financial system at large, as well as to assist law enforcement efforts – will allow them to more thoughtfully focus on higher risk activity instead of spending resources on check-the-box activities. As part of a truly risk-based program, financial institutions will create governance mechanisms to consistently validate resource requirements. Such governance functions and operational health of compliance programs are already subject to regulatory oversight.

However, in order for financial institutions to properly reallocate resources to higher risk activity, other BSA requirements demand amendments that will reduce the compliance burdens attendant to low risk activity. For example, FinCEN should consider revisions to the BSA, such as:

1) increasing the monetary thresholds for SAR and CTR filings;
2) expanding the statutory definition of "verification through non-documentary methods" to include specific references to reliable innovative technologies, such as digital identifications;
3) specifically referencing reliable technologies, such as artificial intelligence ("**AI**") and blockchain analytics, as acceptable methods of performing ongoing monitoring; and
4) codifying a simplified due diligence process for low risk customers.

In addition to amending the BSA to properly capture these changes, FinCEN should also offer supplemental guidance responsive to the increasing use of these innovative technologies to satisfy AML obligations and provide further clarity on the permissible use of AI in compliance programs (e.g., as part of its ongoing monitoring and SAR filing processes).

Additionally, in order for financial institutions to optimize for effective outcomes, there needs to be more effective feedback from FinCEN and law enforcement. For example, FinCEN could explore publishing SAR typologies that are of low-value to law enforcement to help financial institutions focus resources on higher value SAR investigations. The current lack of feedback on effectiveness leads to an overemphasis by both reporting entities and regulators on "total full time employees", "total spend", and other quantitative measures as poor surrogates for effectiveness. Innovative and emerging technologies allow for more precise and efficient assessment of a program's effectiveness, and FinCEN guidance and/or regulatory changes must also reflect that.

Such changes are among those needed to truly give financial institutions the flexibility to confidently reallocate resources to higher-risk activity. These types of changes not only enhance financial institution's ability to engage in risk-based resource allocation, they represent the digital-first nature of today's economy and world.

II. Establishing and Maintaining an AML/CFT Program (V.C.)

NPRM Question 3: *Do financial institutions distinguish between "establishing a program" and "maintaining a program by implementing the program"? If so, how? Should FinCEN add anything to further define these terms in the final rule?*

NPRM Question 4: *Should the proposed rule's distinction between "establishing" and "maintaining" a program be modified? Is the distinction between "establishing" and "maintaining" a compliance program useful for financial institutions?*

Recommendation: FinCEN should maintain the distinction between "establishing" and "maintaining" an AML/CFT program by explicitly aligning these terms with the industry standards of "Control Design" and "Operating Effectiveness," and provide further guidance to clarify the overlapping definitions of "maintaining" and "implementing."

Financial institutions currently distinguish between the two proposed components of an AML/CTF Program as "Control Design" and "Operating Effectiveness", particularly when looking at the control environment in the context of a risk assessment. The prevailing view is that if a program is reasonably designed to comply with law, it is effectively established. If there are deficiencies in *implementing* the policies, procedures or controls, those would be considered failures in Operating Effectiveness, not flaws in the design/establishment of the program. The distinction is also useful given the new section providing that a bank (and, as we argue below, all financial institutions) would not be subject to a "significant AML/CTF supervisory action" if it "establishes" an AML program, except with respect to a "significant or systemic failure" to "implement" the program.

Coinbase recommends that FinCEN further clarify in both the preamble and through supplemental guidance the distinction between "maintaining" and "implementing" the program. The preamble provides that the proposed rule "would require a financial institution to *establish* an AML/CFT program and then *maintain* the AML/CFT program by *implementing*, in all material respects, the established AML/CFT program." While the two terms appear largely interchangeable in FinCEN's preamble discussing 31 CFR 10XX.210(c), further guidance on the differences – if any – between these terms could help financial institutions more effectively comply with the rule.

NPRM Question 5: *Is clarification needed for banks to determine what constitutes a "significant or systemic failure" to implement an effective AML/CFT program (i.e., a*

failure to implement, in all material respects, a properly established AML/CFT program)?

Recommendation: FinCEN should extend the enforcement limitation for "significant or systemic failures" to all financial institutions and add an explicit materiality qualifier to the rule's text, supported by clear guidance that prevents isolated, technical, or self-remediated implementation errors from triggering enforcement actions.

As further detailed in response to Question 20 below, Coinbase advocates for implementation of this new provision limiting enforcement only to "significant or systemic failures" in all financial institutions' AML/CTF Program Rules. Further, while the discussion in the preamble makes clear that the goal of this new provision is to remove regulatory focus on "isolated, technical, or immaterial implementation issues", the language of the rule itself should include a qualifier that captures this more clearly (e.g. a "significant or systemic failure *that impacts the overall effectiveness of the AML/CTF program"*) to further eliminate the risk that financial institutions face enforcement for minor failures or significant failures in just one aspect of their programs.

FinCEN should issue supplemental guidance that provides examples of what types of activity does not constitute a "significant or systemic failure". Coinbase offers the following, non-exhaustive list of examples of the types of isolated, technical, or immaterial implementation issues the rule should expressly protect against:

- A financial institution's transaction monitoring system experiences data quality issues for a short period of time, resulting in delays in alert generation and related SAR filings
    - The NPRM's preamble identifies systems that fail to capture *material* volumes or types of transactions as being problematic. A temporary, self-identified gap affecting a specific product line or time window should not meet that materiality threshold, particularly where the institution identifies the issue through its own controls, remediates it, and files any resulting SARs.
- A financial institution's enterprise-wide AML/CFT risk assessment is generally robust and kept current, but updates to some lower-risk product lines lag or are found to be incomplete following modest operational changes
    - These types of localized gaps should not trigger enforcement, as FinCEN's guidance requires deficiencies that have a material impact on ML/TF risk mitigation. A stale risk assessment for a non-material product line, within an otherwise sound program, does not meet this threshold.
- Isolated errors in individual SAR filings, such as data entry mistakes or transposed digits in transaction amounts that do not materially affect the report's utility to law enforcement

- Mistakes in SARs that are indicative of isolated errors rather than a pattern of issues should not be treated as program implementation failures; a handful of clerical errors in reporting, absent a systemic data quality or training failure, does not approach that threshold.
- Missing information from SARs, even if systemic, that is due to the information being variable, not applicable in all cases, or of dubious value (e.g. IP address) should also not be treated as systemic issues if intentionally made in a good faith attempt to comply with AML requirements.

III. Internal Policies, Procedures, and Controls (V.D.1.)

NPRM Question 8: *Do financial institutions expect any changes to their existing internal* policies*, procedures, and controls under the proposed rule, which requires that internal policies, procedures, and controls be "risk-based" and "reasonably designed" to ensure compliance with the BSA?*

Recommendation: FinCEN should codify the flexible "discretion" text within the rule itself and structurally bifurcate the ongoing customer due diligence mandate into separate Customer Due Diligence (KYC) and Ongoing Monitoring (Transaction Monitoring) obligations to prevent compliance dilution.

Risk-Based and Reasonably Designed Refinements

Most covered financial institutions already develop and implement risk-based programs that are reasonably designed to comply with the BSA. The "risk-based" and "reasonably designed" standards allow for KYC models that are bespoke to particular product types. Moreover, these standards help financial institutions design flexible programs for emerging architectures, such as tokenized assets and on-chain trading, without prescribing an impractical one-size-fits-all KYC obligation.

The preamble's statement that financial institutions should "have significant flexibility and discretion in their decisions and determinations related to risk identification and resource allocation" is a positive step towards giving financial institutions more leeway to define their risks. However, this language will not provide the intended impact if similar language is not also included in the rules themselves. Coinbase thus recommends that FinCEN add language to the rule giving financial institutions "discretion" to build a risk-based and reasonably-designed program.

Proposed Amendment to CDD requirements under section (b)

To ensure operational clarity and improve the efficacy of AML programs, we recommend restructuring the "Ongoing Customer Due Diligence" requirements. The current phrasing

conflates distinct compliance functions – **KYC** and **transaction monitoring** – into a single, overly dense mandate.

We propose bifurcating these obligations to reflect the functional reality:

1. Customer Due Diligence ("**CDD**"): Conduct CDD to obtain an accurate understanding of the nature and purpose of customer relationships, establish a dynamic customer risk profile, and update and maintain customer information on a risk-based basis.
2. Ongoing Monitoring: Utilize the established customer risk profile as part of a risk-based program of ongoing monitoring for the specific purpose of identifying and reporting suspicious activity.

While there are synergies between the two, separating "KYC" from "Transaction Monitoring" prevents the dilution of both functions and ensures that institutions can deploy resources more effectively.

IV. Risk Assessment Processes (Generally) (V.D.1.i.)

> **NPRM Question 9:** *The proposed rule refers to risk assessment processes rather than a risk assessment process. This leaves financial institutions free to use findings from one or more processes to holistically assess their ML/TF risks. Does this description of how financial institutions would assess their ML/TF risk under the proposed rule provide sufficient flexibility? How should FinCEN describe "risk assessment processes" to better reflect how financial institutions assess ML/TF risks?*
>
> **NPRM Question 10:** *Should risk assessment processes be required to take into account additional or different criteria or risks than those listed in the proposed rule? If so, what additional factors should FinCEN consider requiring?*
>
> **NPRM Question 11:** *How long does it generally take a financial institution to incorporate the results of a risk assessment into the other aspects of its AML/CFT program? What factors determine this timeframe?*

Recommendation: FinCEN should maintain the flexible, plural designation of "risk assessment processes" by granting institutions explicit discretion over factor weighting, materiality of system updates, and implementation timelines, while acknowledging that incorporating assessment results is a variable, iterative process dependent on technological complexity rather than a rigid regulatory schedule.

Flexible processes (Q9): Coinbase supports the plural "processes," as it allows institutions to assess ML/TF risks holistically. To ensure this flexibility is functional, FinCEN should:

- Grant materiality discretion: Institutions must have the discretion to determine when a discrete system update or process is "material" enough to warrant an update to the risk assessment. For example, through routine monitoring and change management processes, financial institutions regularly update their transaction monitoring models by tuning alert thresholds, adding a new detection logic, or updating blockchain wallet attribution data. Such changes reflect a program working as intended and should not necessitate an update to an enterprise-wide risk assessment. FinCEN should thus clarify that these and similar program management activities are distinct from the type of material change that warrants a more holistic risk assessment update, and that institutions retain discretion to make this determination based on whether the change alters the institution's understanding of its overall ML/TF risk profile rather than merely its operational implementation.

Risk factors (Q10): The rule should not mandate additional factors beyond the current list (business activities, products, services, distribution channels, customers, and geographic locations). Instead:

- The rule must explicitly state that institutions have the authority to weight these factors based on their judgment as informed by the specific risk profile of each institution.
- An institution’s judgment on factor weighting should be given deference absent clear evidence that it is willfully ignoring risk or manipulating outcomes.
- FinCEN should allow, but not require, institutions to incorporate supplemental factors as they see fit (e.g. explicit reference to national priorities as a potential addition).

Implementation timelines (Q11): The time required to incorporate risk assessment results into an AML/CFT program varies significantly based on the complexity of the finding.

- Timeframes are driven by the scale of the required technological changes, the depth of data gathering necessary to assess residual risk, and the resource allocation required.
- FinCEN should avoid rigid timelines, acknowledging that meaningful integration of assessment results into an AML/CTF program is an iterative process that may vary based on the size and complexity of the institution. For example, timeframes for incorporating risk assessment results into program changes for larger, technologically complex institutions can vary from near-real-time to 12 months or more for enterprise-wide program enhancements:

i. where risk assessment outputs feed directly into automated systems such as transaction monitoring rules or customer risk scoring models, incorporation may be nearly immediate;
ii. where findings require modest policy or procedural updates, 90 days may be a reasonable timeframe for drafting, review, approval, and training to affected teams; and
iii. where findings require significant technological changes, such as building new customer-facing workflows to capture additional information or retraining machine learning models to incorporate such details, 12 months or more may be required, even for a well-resourced, mature institution.

FinCEN should reflect this spectrum in its guidance and explicitly state that no single timeframe applies across all types of findings or institution sizes. The relevant question is not whether a change was made within a prescribed period, but whether the institution's response was proportionate to the risk level and complexity of the required program updates. The real risk is not the timeframe in which institutions respond, it is whether the institution has an enterprise issues management process by which these issues can be tracked, validated, and closed, or escalated to senior management if the institution identifies problems or unwarranted delays with incorporating the results of the risk assessment.

V. Risk Assessment Processes (AML/CFT Priorities) (V.D.1.i.b.)

NPRM Question 12: *What, if any, difficulties do financial institutions anticipate when incorporating the AML/CFT Priorities as part of their risk assessment processes?*

NPRM Question 13: *What additional guidance on how to incorporate the AML/CFT Priorities into a financial institution's risk assessment processes would it be useful for FinCEN to provide?*

Recommendation: FinCEN should provide actionable/operational guidance, explicit implementation timelines, and sector-specific "safe harbor" examples for incorporation of national AML/CFT Priorities into risk assessments so financial institutions can confidently reallocate compliance resources from lower-risk areas to high-priority threats without fear of regulatory penalties.

Coinbase supports the flexibility of the proposed rule, which indicates that AML/CFT Priorities should be incorporated “as appropriate”. However, for effective implementation, two primary areas require guidance from FinCEN:

Lack of Actionable Guidance (Q12): The current Priorities (e.g., Terrorist Financing, Fraud, Cybercrime, Corruption) are too high-level and lack practical guidance for

meaningful incorporation into risk assessment processes. The main difficulty is the lack of actionable pathways by which financial institutions can confidently reallocate resources to higher-risk areas with confidence that they will not be penalized for deemphasizing areas of lower priority. For example, it is unclear if investments in a priority area (like hiring cybercrime specialists) would justify reducing monitoring controls in low-priority areas (like turning off structuring monitoring scenarios). FinCEN must provide such guidance in conjunction with its future issuance of new priorities.

Need for Process Clarity (Q13): Coinbase requests that Treasury share guidance on operational expectations, specifically concerning the expected timeline for incorporation (as applicable) of new Priorities. For example, FinCEN could publish 'safe harbor' examples of compliance activities that would be consistent with a given AML/CFT Priority for different institution types, such as confirming that a digital asset exchange maintaining real-time "know your transaction" screening, blockchain analytics, and SAR filing for cybercrime typologies would satisfy regulatory expectations for prioritizing resources towards the cybercrime Priority. The absence of such guidance or feedback loops would otherwise leave institutions investing in Priority-related compliance activities with no assurance that examiners will credit those investments, a dynamic that undermines the AML Act's goal of focusing resources on the highest-risk activities.

VI. Risk Assessment Processes (Updates) (V.D.1.i.c.)

> **NPRM Question 14:** *The proposed rule requires that risk assessment processes are updated promptly upon any change that the bank knows or has reason to know significantly changes the bank's ML/FT risks. Would the proposed update requirement change the way financial institutions currently update their risk assessment processes, and if so, how? Is additional explanation needed concerning when a financial institution would be required to update its risk assessment? In particular, how might FinCEN clarify how risk assessment processes would be updated "promptly"? Would an alternative approach, such as periodic updates or a set schedule for updates, be preferable? Would an alternative standard, such as "materially changes," be clearer than "significantly changes"?*

Recommendation: FinCEN should replace the "significantly changes" trigger with a well-established legal "materially changes" standard and provide supplemental guidance defining "promptly" as a reasonable, risk-based timeframe, thereby allowing institutional discretion and preventing risk assessments from turning into perfunctory administrative logs for minor operational updates.

Deferring to Institutional Discretion on Timelines

As noted above in response to Questions 9 and 11, we recommend that FinCEN avoid mandating specific, rigid timelines for risk assessment updates. Instead, in alignment with the proposed rule's mandate to defer to an institution's judgment regarding the incorporation of AML/CFT Priorities ("a financial institution may use its judgment and apply a reasonable, risk-based determination on whether to focus on a specific aspect of an AML/CFT Priority"), the decision of when to update a risk assessment should remain within the institution's discretion.

A "one size fits all" mandate is less effective than a risk-based approach. It should be left to the institution to determine whether changes in its business model, product suite, geographic footprint, or customer base necessitate an update.

Clarifying "Promptly" via Guidance

While Coinbase does not support a fixed schedule, there is a need for clarity regarding the term "promptly." Rather than defining this through strict deadlines in the rule itself, we recommend that FinCEN issue supplemental guidance that both defines "prompt" as a "reasonable and risk-based" timeframe based on the size and complexity of the institution, and also acknowledges that the duration of an update may vary depending on the complexity of the change that triggered it.

Standardizing "Material" vs. "Significant" Changes

Coinbase advocates for changing the risk assessment trigger standard from "significantly changes" to "materially changes." The concept of "materiality" is a well-established legal and regulatory standard. Using this term would allow financial institutions to focus more attention on the highest-risk changes than on technical issues. Shifting to a materiality standard will allow risk assessments to remain high-level strategic documents rather than becoming administrative logs for every minor operational adjustment.

The case for "material" over "significant" changes is particularly compelling in the digital asset context, where rapid product iteration, frequent blockchain protocol changes, and evolving counterparty risk profiles create a constant stream of operational changes. Under a "significantly changes" standard, an institution like Coinbase, which may add new blockchain network support or frequently expand its product offerings to a new jurisdiction, could be faced with an expectation of rolling, formal risk assessment updates. This would perversely incentivize institutions to either slow product innovation or to produce largely perfunctory risk assessment updates that satisfy the letter of the rule without adding meaningful analytical value. A "materiality" standard, by contrast, allows institutions to apply a principled, threshold-based judgment: does this change alter our understanding of our ML/TF risk profile in a way that requires a programmatic response? For Coinbase, adding support for a new, well-established blockchain network

with existing analytics coverage likely would not be material, whereas launching a brand new, higher-risk product line likely would be.

VII. AML/CFT Officer Located in the United States (V.D.3.)

> **NPRM Question 17:** *Under the proposed rule, while the AML/CFT officer must be located in the United States, personnel located outside of the United States would still be permitted to perform certain AML/CFT functions. This language does not alter existing regulations and guidance that generally prohibit the sharing of SARs with personnel located outside of the United States other than limited circumstances, such as a bank's foreign head office or controlling company. Are any further clarifications on what duties personnel outside the United States may perform needed?*

Recommendation: FinCEN should provide further clarity on the type of investigative roles and system maintenance functions non-U.S. personnel may perform in a financial institution's SAR processes and fully implement the wider SAR-sharing program mandated by Section 6212 of the Anti-Money Laundering Act of 2020 ("**AMLA**").

Coinbase believes that financial institutions would benefit from more guidance on which SAR-related functions may be performed by employees located outside of the United States, so long as proper safeguards remain in place to preserve SAR secrecy. Regulators have long permitted the outsourcing of BSA compliance functions to third parties, including non-U.S. entities or affiliates, so long as the party that is outsourcing these functions retains ultimate responsibility for BSA compliance in the U.S. and exercises proper due diligence and oversight over the outsourced activity. Many financial institutions use a multi-step investigation process and rely on foreign resources to perform portions of the SAR investigation process, subject to strict confidentiality guardrails to avoid "tipping-off". Such outsourcing realizes tremendous efficiencies (i.e., "round the clock coverage"), facilitates prompt regulatory filings, and reduces compliance costs - all direct goals of this NPRM.

However, the current law and corresponding guidance have limited the extent to which financial institutions can utilize such non-US personnel to realize these efficiencies. For example, non-U.S. personnel are prohibited from viewing prior SAR data on a customer, including investigative files that resulted in a "no" SAR filing. The rationale provided by FinCEN being that, "[w]ere FinCEN to allow disclosure of information when a SAR is not filed, institutions would implicitly reveal the existence of a SAR any time they were unable to produce records because a SAR was filed."[1] Such an absolute position is not clearly aligned with the permissibility of sharing the underlying facts, transactions, and documents that form the basis for the SAR, nor is it facially consistent with the prohibition against sharing only SARs that have been filed.

[1] FinCEN, *Confidentiality of Suspicious Activity Reports*, 75 FR 75593, 75595 (December 3, 2010).

Congress has already attempted to remedy this issue with Section 6212 of AMLA, which required the launching of a pilot program that permitted financial institutions to share SARs and related information with foreign branches, subsidiaries and affiliates for the purpose of combating illicit financing risks. Congress' issuance of this provision made clear its recognition of the utility in sharing such information with non-US affiliates. That pilot program has since ended and has yet to be replaced with a permanent rule that fully authorizes such permissible SAR sharing.

Any risks of "tipping-off" in these intra-entity, SAR-sharing arrangements are also mitigated by pre-existing safeguards. The primary basis for the SAR confidentiality provisions of the BSA was to prevent alerting the SAR subject that a SAR had been filed against them, as such disclosure could negatively impact any law enforcement investigation. Expanding the SAR sharing exceptions for non-U.S. personnel would not run afoul of this principle, as such persons would be subject to the same internal confidentiality requirements as U.S. employees (i.e., not to disclose such information to third parties).

As such, we believe FinCEN should issue additional guidance that clarifies that personnel located outside of the U.S. who provide assistance in a financial institution's SAR investigative process (e.g., systems maintenance, alert triage) should be permitted to view prior SAR information maintained by the institution - specifically whether a prior transaction monitoring alert was generated on a customer, the underlying facts of prior investigations, and whether a SAR was or was not ultimately filed on that customer. Access to such information would enhance the efficiency of a financial institution's AML/CTF program, continue to prevent tipping-off, and fulfill the intent of AMLA's pilot program.

VIII. Supervision and Enforcement (V.F.)

> **NPRM Question 20:** *The proposed rule would add a new § 1020.221 to set forth a supervision and enforcement framework for banks. The new supervision and enforcement requirements would apply only to banks and the Federal banking agencies in the proposed rule. FinCEN welcomes comment on whether these provisions should apply to other financial institutions.*

Recommendation: FinCEN should extend the proposed supervision and enforcement safe harbor to all federally regulated financial institutions, including money services businesses and broker-dealers, to ensure regulatory parity and provide equal latitude for implementing creative, risk-based compliance programs without the risk of enforcement for minor implementation deficiencies.

Coinbase asserts that the provision at § 1020.221 – currently proposed only for banks – must apply equally for all financial institutions, including broker-dealers and MSBs, as the policy rationale for the bank safe-harbor also applies to these other financial institutions.

It is unclear why banks are the only type of "financial institution" that should benefit from such a safe-harbor. All financial institutions subject to AML/CTF Program Rules are required to maintain largely similar program components: customer due diligence, transaction monitoring, SAR filing, AML/CTF training and the appointment of a BSA officer, amongst other core obligations. In fact, entities such as MSBs are typically subject to greater AML/CTF scrutiny given their maintenance of State licenses - meaning they are subject to both Federal and State AML/CTF requirements.

Subjecting financial institutions to different standards would also create an unlevel playing field, one in which banks may confidently explore use of innovative technologies in their AML/CTF programs while non-bank financial institutions would need to maintain more conservative approaches due to the risk of enforcement for non-significant violations. Since the goal of this NPRM is to modernize the entire U.S. AML/CTF regime, FinCEN should extend the proposed supervision and enforcement safe harbor to all federally regulated financial institutions, including MSBs and broker-dealers.

> **NPRM Question 27:** *Is the definition of the term "significant AML/CFT supervisory action" sufficiently clear? Does the inclusion of "unsafe or unsound practices or conditions" introduce confusion about what types of supervisory actions would be subject to the FinCEN consultation requirement, since those terms are not found in the BSA?*

Recommendation: FinCEN should refine the definition of a "significant AML/CFT supervisory action" by narrowing its scope to "significant or systemic failures," establishing objective benchmarks for "remedial measures," and codifying a formal "opportunity to respond" period to ensure regulatory predictability and transparency.

We recommend refining the definition of "significant AML/CFT supervisory action" to make it more predictable and transparent. Specifically, FinCEN should:

- **Narrow the scope**: Explicitly include in the definition of "significant AML/CFT supervisory action" in the newly-proposed section § 1020.221(a)(3) the term "significant or systemic failures" (for example, the term could be added to section (a)(3)(i), which defines a significant AML/CFT supervisory action as one that "identifies one or more alleged deficiencies, weaknesses, violations of law, or unsafe or unsound practices or conditions relating to an AML/CFT requirement") to avoid over-capturing minor issues and to maintain language consistency.
- **Provide objective benchmarks**: Define "remedial measures" by using specific examples, such as business restrictions, the imposition of a monitor, or remediation efforts that cross a defined monetary or revenue-based threshold.

Additionally, Coinbases recommends including a formal "opportunity to respond" period to FinCEN for institutions facing significant supervisory action. By allowing this, FinCEN

can make more informed enforcement decisions and more effectively align public and private resources toward high-risk priorities.

> **NPRM Question 28**: *FinCEN welcomes comment on provisions related to the use of innovative tools to achieve effective outcomes, specifically on how the Director may consider the performance of innovative activities that produce demonstrable outputs under the proposed supervision and enforcement framework.*

Recommendation: FinCEN should eliminate the regulatory gap by extending the innovation "safe harbor" protections to all financial institutions – not just banks – and establish a governance-based framework that credits demonstrable compliance outputs, such as AI-driven SAR narratives and blockchain analytics, while protecting responsible experimentation from supervisory penalties.

We support FinCEN's stated goal of encouraging innovative activities that produce demonstrable AML/CFT outcomes. However, the proposed rule creates an **unjustified regulatory gap** by explicitly providing "safe harbor" protections to banks while omitting them for other financial institutions, such as digital asset exchanges and broker-dealers.

To ensure the framework is effective across the entire financial ecosystem, we recommend the following:

Codify the safe harbor for all financial institutions

The preamble states that *institutions* "responsibly experimenting" with innovation will not face heightened enforcement risks solely based on the use of new technologies. However, this protection is currently only codified in the proposed rules for *banks*.

FinCEN should extend the specific "safe harbor" language to the AML/CFT Program rules for **all** financial institutions for the following reasons:

1) As noted in our response to Question 20, there is no basis for treating banks as a special class of financial institution over other financial institutions, as they are all subject to the core requirements of the BSA.

2) Innovation is not unique to the banking sector. In fact, MSBs operating as virtual asset service providers are often the primary driver and most knowledgeable users of cutting-edge compliance tools, such as blockchain analytics and decentralized identity.

3) Excluding non-banks from these protections creates a "chilling effect" on the very experimentation FinCEN seeks to encourage.

As such, all financial institutions should be permitted to avail themselves of this safe-harbor.

Incentivize Demonstrable Outputs

In order to promote the use of such innovative solutions, FinCEN should separately issue guidance that indicates how the responsible use of these technologies to satisfy AML/CTF obligations should serve as a mitigating factor in supervision and enforcement for *all* financial institutions. In particular, the guidance should set forth how financial institutions will be deemed to have responsibly used innovative technologies, such as:

- **Blockchain Analytics:** The use of real-time "Know Your Transaction" (KYT) and clustering tools that offer higher precision than legacy monitoring.

- **Artificial Intelligence:** The deployment of AI solutions such as machine learning and large language models to improve the accuracy of SAR narratives – and potentially the speed of filing SARs if FinCEN clarifies that AI can be leveraged in more stages of filing SAR filings – and reduce the "noise" of false-positive alerts.

- **Digital Identity:** The use of decentralized identifiers (DIDs) and zero-knowledge proofs to enhance customer verification while protecting data privacy.

Please refer to Coinbase's submission to the U.S. Department of the Treasury in response to its "Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets" for further detail on the benefits of these innovative solutions and how they can be unlocked further by FinCEN.

Establish Governance-Based Safe Harbors

More than just protecting specific technologies, FinCEN should focus on the governance behind the innovation. A codified safe harbor should protect any institution that demonstrates:

- Clear internal testing and validation of new tools;
- Ongoing monitoring of the tool's performance against its AML/CFT goals;
- A reasonable fact-based review standard that a new system will be as or more effective at producing beneficial outcomes than an old system; and
- A framework under which an institution is not penalized if an innovative pilot fails to meet expectations, provided there was no systemic neglect.

For the proposed rule to truly modernize the AML/CFT regime, it must provide a **consistent and inclusive safe harbor**. All financial institutions – regardless of their charter

– should be empowered to deploy innovative technologies without fear that responsible experimentation will lead to supervisory action.

Conclusion

Coinbase appreciates the opportunity to provide comments on this important rulemaking and commends FinCEN's commitment to modernizing the U.S. AML/CTF framework in a manner that prioritizes risk-based outcomes over prescriptive, check-the-box compliance. The proposed rule represents a meaningful step toward a more effective and adaptive regulatory regime, and Coinbase strongly supports its core objectives.

To fully realize those objectives, we urge FinCEN to extend the "significant or systemic failure" enforcement standard and innovation safe harbor to all financial institutions, pair the resource allocation directive with targeted reforms to attendant BSA regulations, and provide greater clarity on risk assessment standards and implementation timelines. These refinements would ensure that the final rule delivers on its promise of a flexible, outcomes-driven framework that empowers financial institutions of all types to deploy their compliance resources where they matter most – identifying and disrupting genuine illicit finance threats.

Coinbase looks forward to continued collaboration with FinCEN and the Department of the Treasury on this initiative and remains committed to working constructively toward an AML/CTF framework that is both rigorous in its protections and rational in its demands.