THE DIGITAL CHAMBER, ZUNERA MAZHAR

Proposal and Comment Information

Title: Anti-Money Laundering and Countering the Financing of Terrorism Programs, R-1835

Comment ID: FR-0000-0133-02-C42

Submitter Information

Organization Name: The Digital Chamber

Organization Type: Organization

Name: Zunera Mazhar

Submitted Date: 09/08/2026

The Digital Chamber (TDC), the world's largest digital asset and blockchain trade association representing more than 250 members across the ecosystem, welcomes the opportunity to comment on the Federal Reserve Board's proposed rule to require Board-supervised banks to maintain effective AML/CFT programs.

TDC strongly supports modernizing the Bank Secrecy Act framework to better serve financial institutions while effectively combating illicit finance and offers recommendations to provide greater clarity and strengthen the proposed rule, particularly for banks engaged in digital asset activities or interacting with digital asset counterparties.

Via Electronic Submission
September 8, 2026

Benjamin W. McDonough
Secretary of the Board and Ombudsman
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

RE: RIN 7100-AG78 - Anti-Money Laundering and Countering the Financing of Terrorism Programs

The Digital Chamber (***"TDC"***) welcomes the opportunity to comment on the Board of Governors of the Federal Reserve System's (***"Board"***) proposed rule that would require Board-supervised banks to establish and maintain effective anti-money laundering and countering the financing of terrorism (***"AML/CFT"***) programs reasonably designed to identify, assess, and mitigate risks of illicit finance.

TDC strongly supports the Board's broader effort to modernize the Bank Secrecy Act (***"BSA"***) framework in a manner that better serves the needs of financial institutions while continuing to combat illicit finance effectively. TDC writes to offer recommendations that would strengthen the proposed rule in ways that further the Board's stated objectives and provide much-needed clarity to regulated institutions, particularly those engaged in digital asset activities or that interact with counterparties conducting significant digital asset activity.

TDC is the world's largest digital asset and blockchain trade association, representing more than 250 members across the global blockchain ecosystem, including stablecoin issuers, digital asset firms, national and community banks, blockchain analytics firms, custodians, tokenization platforms, and companies building core blockchain infrastructure. Guided by the principle of industry compliance with applicable law, TDC works to foster a regulatory environment that provides clarity and stability for digital asset users and innovators as they apply blockchain technology across a broad range of commercial, financial, and societal use cases.

I. TDC and Its Membership's Interest in BSA Reform

TDC has actively engaged in the parallel BSA modernization rulemakings issued by the Financial Crimes Enforcement Network (***"FinCEN"***), the OCC, the NCUA, and the FDIC on April 10, 2026 (***"the Agencies"***), given the substantial number of TDC members regulated as banks, money services businesses (***"MSBs"***), and other BSA-covered financial institutions under those agencies'

respective frameworks. [1] TDC submits these comments to ensure the Board's proposed rule aligns closely with those parallel proposals and meets the Board's own stated intent that "banks will not be subject to any additional burden or confusion from needing to comply with differing standards between regulatory agencies." [2] Many TDC members operate multiple business lines and maintain subsidiaries or affiliates spanning several categories of BSA-regulated institutions (including banks, broker-dealers and futures commission merchants registered with the SEC and CFTC, and MSBs regulated by FinCEN) so inconsistencies between the Board's final rule and the parallel FinCEN/Agency rules could create compliance burdens even where the Board supervises fewer of these entities directly.

TDC also notes that some state member banks are beginning to explore blockchain-based products and services such as stablecoin-based payments, tokenized deposits, and digital asset custody, and that TDC separately represents digital identity companies, blockchain analytics providers, and regulatory technology (***"RegTech"***) providers whose tools are increasingly relevant to the risk assessment, transaction monitoring, and customer due diligence functions this proposed rule would require. TDC offers the comments below primarily in the interest of harmonization across the Board's, FinCEN's, and the Agencies' respective AML/CFT program rules, and to ensure the Board's final rule remains workable for banks and their affiliates as they engage with digital asset activity.

II. TDC Support for the Goals of the NPRM

TDC strongly agrees with the impetus behind this proposed rule. TDC and its membership are strongly supportive of the Board's critical mission in securing the U.S. financial system from illicit financial activity. For the digital asset industry to flourish, it is essential that all participants in the ecosystem work together to identify bad actors and prevent them from laundering funds, financing terrorist activity, or engaging in similar illicit conduct.[3]

TDC concurs with the proposed rule's view that BSA compliance should be judged by whether a bank effectively prevents illicit financial conduct, not by whether it has checked the right boxes through a rigid, one-size-fits-all set of requirements ill-suited to its particular business model. TDC commends this shift away from "check-the-box" compliance and toward risk-tailored programs,

[1] The Digital Chamber, *Comment Letter on Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements*, RIN 1506-AB73, Docket No. FINCEN-2026-0100 (submitted by Chapman and Cutler LLP) (June 9, 2026); The Digital Chamber, *Comment Letter on the FDIC, OCC, and NCUA Proposed Rule Related to Anti-Money Laundering and Countering the Financing of Terrorism Programs*, RIN 3064-AF34 (submitted by Steptoe LLP) (June 9, 2026).
[2] Board of Governors of the Federal Reserve System, *Notice of Proposed Rulemaking*, 91 Fed. Reg. 42364 (2026), Docket No. R-1835, RIN 7100-AG78. Federal Register, p. 42364
[3] The Digital Chamber, *Blockchain and National Security: A Strategic Imperative* (2026), https://digitalchamber.org/national-security-report/

which is precisely what banks engaged in digital asset activity need to respond nimbly to an evolving risk landscape.

As detailed below, TDC offers concrete recommendations to help ensure rulemaking intent translates into effective practice. These recommendations are offered in a spirit of collaboration since TDC is fundamentally aligned with the Board's goals and wants to see the rule succeed for banks operating in digital assets.

III. Establishing and Maintaining an "Effective" AML/CFT Program [4]

TDC supports the Board's effort to make "effectiveness" the organizing principle of AML/CFT program supervision. The proposed rule appropriately evaluates AML/CFT programs based on whether they are risk-based, reasonably designed, and capable of producing meaningful outcomes for law enforcement and national security authorities — not on technical compliance for its own sake. This approach is consistent with the Anti-Money Laundering Act of 2020 (***"AML Act"***)'s modernization objectives and with the Board's stated goal of focusing supervisory expectations on higher-risk activity while reducing unnecessary burden. [5]

TDC also supports the proposed rule's two-part formulation of an "effective" AML/CFT program: (1) established in accordance with the rule's establishment requirements under proposed §208.63(c), and (2) maintained, meaning the established program is implemented "in all material respects" under proposed §208.63(d). This distinction between establishment and maintenance is a constructive improvement, and one particularly relevant to TDC members that operate in fast-evolving markets and deploy innovative compliance tools such as blockchain analytics, artificial intelligence, digital identity solutions, and other technology-enabled controls. TDC recommends the Board strengthen this standard in three respects to ensure it is applied consistently, predictably, and in a manner that encourages responsible innovation.

First, the Board should clarify the meaning of "implemented in all material respects." The phrase itself remains open to interpretation, and inconsistent examiner conclusions about materiality pose particular risk for institutions building AML/CFT programs around emerging technologies. The Board should clarify, in the regulatory text itself, not only the preamble, that a program is

[4] Board of Governors of the Federal Reserve System, *Establishing and Maintaining an Effective Anti-Money Laundering and Countering the Financing of Terrorism Program*, 91 Fed. Reg. 42364, 42414–17 (2026), Docket No. R-1835, RIN 7100-AG78. Federal Register, Questions 1–8

[5] Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, div. F, 134 Stat. 3388, 4547–4608 (2021); Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1118 (1970); Board of Governors of the Federal Reserve System, *Establishing and Maintaining an Effective Anti-Money Laundering and Countering the Financing of Terrorism Program*, 91 Fed. Reg. 42364, 42368–72 (2026). Federal Register, pp. 42368–72

implemented in all material respects where a bank has reasonably operationalized the core components of its program consistent with its documented risk assessment and business model. The standard should ask whether the program, viewed as a whole, is functioning as reasonably designed; not whether every individual control operates perfectly in every instance.

Second, the Board should expressly state that effectiveness does not require perfection. No AML/CFT program can prevent or detect every instance of illicit activity, and an isolated missed alert, delayed investigation, documentation gap, technology calibration issue, or good-faith judgment call should not, standing alone, establish a maintenance failure. The final rule should make clear that the relevant inquiry is whether the bank's overall AML/CFT framework is reasonably designed and materially operational, not whether hindsight suggests a different control might have produced a better result in a particular instance. As with the point above, TDC believes the preamble reflects this view; codifying it in §208.63(d) would remove ambiguity for examiners and banks alike.

Third, the Board should require examiners to articulate the factual basis for any determination that a program is not effective. Where an examiner concludes a program was not established under §208.63(c) or not maintained under §208.63(d), the examiner should identify with specificity: (1) the relevant program requirement; (2) the facts supporting the deficiency; (3) why the deficiency is material to the bank's risk profile; (4) whether the deficiency relates to establishment or maintenance; and (5) why ordinary remediation would be insufficient. This would promote accountability, reduce inconsistent supervisory applications, and give banks a meaningful opportunity to respond.

IV. Risk Assessment Updates [6]

TDC supports the Board's proposal to require state member banks to maintain risk assessment processes that are dynamic and responsive to changes in illicit finance risk. A risk assessment that is never revisited, or that fails to account for material changes in a bank's business, will not meaningfully support an effective AML/CFT program.

However, TDC is concerned that the proposed requirement that risk assessment processes be "updated promptly upon any change that the [bank] knows or has reason to know significantly changes" its illicit finance risks could be interpreted in an overly broad or unworkable manner. The term "promptly" does not establish a workable supervisory standard because it does not specify when the obligation is triggered, how quickly an update must occur, or whether timing should account for the institution's size, complexity, or the significance of the risk at issue. Without

[6] *Establishing and Maintaining an Effective Anti-Money Laundering and Countering the Financing of Terrorism Program*, 91 Fed. Reg. 42364, 42418–19 (2026) (Questions 15–16). Federal Register, Questions 15–16

clarification, the term may invite hindsight-based criticism whenever an examiner concludes an update could have occurred sooner.

This concern is significant because risk assessments require time for banks to identify relevant changes, assess materiality, gather and validate data, consult relevant stakeholders, and determine whether updates to policies, procedures, monitoring, staffing, or governance are warranted. An immediate update to a formal document is often less useful than a deliberate, well-documented assessment of whether a change materially affects the institution's risk profile. If interpreted too rigidly, "promptly" could encourage frequent, superficial, or defensive updates rather than substantive risk analysis, thus reintroducing the check-the-box burden the Board seeks to reduce.

The issue is especially acute for banks engaged in digital asset activity, where products, protocols, counterparties, and threat typologies can evolve rapidly. A "promptly" standard could be read to require continuous formal revisions even where a development has not yet been validated, has limited relevance, or is already addressed through existing operational controls or enhanced monitoring.

TDC recommends that the Board revise proposed §208.63(c)(1)(i)(C) to replace "updated promptly" with a more precise, materiality-based formulation. For example, requiring that risk assessment processes be reviewed and updated "within a reasonable period of time after the bank identifies a material change to its illicit finance risk profile, taking into account the bank's size and complexity and the complexity of the change identified."[7] TDC agrees a materiality-based standard is preferable, and recommends the Board apply that same principle to the timing of updates, not only the trigger.

Finally, the Board should clarify that (1) not every change in business activity, customer behavior, technology, or threat intelligence requires an immediate formal update, and (2) a bank may satisfy the requirement through documented risk assessment processes rather than a single static document, as the preamble already supports. Many institutions evaluate risk continuously through processes that may identify and mitigate risk before a formal document is revised, including governance forums, product approvals, transaction monitoring outputs, audit findings, and typology reviews. The Board should recognize that such processes are consistent with an effective AML/CFT program; provided material changes are appropriately documented and incorporated within a reasonable time.

V. Allocation of Resources [8]

[7] *Id.* at 42364, 42418 (2026) (Question 15). Federal Register, Question 15
[8] *Id.* at 42364, 42392, 42415 (2026). Federal Register (1) Federal Register, Question 2

According to the preamble of the proposed rule, under proposed §208.63(c)(1)(ii), a state member bank's efforts to mitigate its ML/TF risks would involve "directing more attention and resources toward higher-risk customers and activities, consistent with the risk profile of [a bank], rather than toward lower-risk customers and activities." The preamble emphasizes that the Board "envisions Board-supervised banks exercising more flexibility in deploying attention and resources... without fear of supervisory criticism or action from examiners" and "does not contemplate second-guessing of a bank's reasonable determinations regarding appropriate resource allocation."[9]

TDC strongly supports this goal but is concerned the current language is not sufficient to foreclose examiners from penalizing a bank based on their own subjective view that resources were not appropriately allocated toward higher-risk customers or the AML/CFT Priorities. If not carefully implemented, this provision could become merely another enforcement vector rather than the flexibility it is meant to provide.

This concern is especially acute for banks in the digital asset space, where risk presents differently than in traditional financial systems. TDC appreciates that the Board has recognized as much, noting that "[i]nnovative approaches could involve machine learning, generative artificial intelligence (GenAI), digital identity, blockchain monitoring and analytics, or application programming interfaces (APIs)," and that the Board "encourages banks to engage in responsible AML/CFT innovation."[10] The Board is exactly right, but those innovative methods have not always been met with comparable support from examiners in practice.

To address this, TDC proposes two modifications to proposed §208.63(c)(1):

First, the phrase "reasonably designed" defined as a program which "Establishes a risk-based set of internal policies, procedures, and controls that is reasonably designed to ensure compliance with the Bank Secrecy Act" — should not open the door to regulatory uncertainty. Examiners often lack the insight into a bank's business to judge whether a decision is "reasonable," and may instead substitute their own judgment for the bank's, limiting bank's ability to follow the rule's intended spirit. Instead, the term should be interpreted as asking whether a program is reasonably and specifically designed to ensure compliance with the Bank Secrecy Act. This would create a more objective test, namely determining whether a bank can demonstrate that it evaluated its risks and built a bespoke AML/CFT program responsive to them. This should satisfy the requirement regardless of an examiner's personal view of its reasonableness.

TDC notes that the Board and its fellow regulators have already endorsed a version of this interpretation. The 2019 Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money

[9] *Id.* at 42364, 42392 (2026). Federal Register
[10] *Id.* at 42364, 42379, 42385 (2026). Federal Register (1) Federal Register (2)

Laundering Supervision (issued jointly by the Board, FDIC, NCUA, OCC, and FinCEN) explains that to assure BSA/AML compliance programs are reasonably designed to meet the requirements of the BSA, banks structure their compliance programs to be risk-based.[11] The Board should codify that interpretation directly in the regulatory text of §208.63(c)(1), rather than leaving it to sub-regulatory guidance alone, so that "reasonably designed" is understood as a matter of binding rule text, not just examiner practice, to mean a program that is risk-based and specifically tailored to the bank's own risk assessment.

Second, language should be added to §208.63(g) (Enforcement and supervision policy) making clear that this resource allocation flexibility is a tool to assist banks, not a new enforcement vector. The Board should confirm that examiners should not bring AML/CFT enforcement actions or significant AML/CFT supervisory actions based on a bank's allocation and prioritization of resources unless such actions would have been appropriate under the current rule.

VI. FinCEN Consultation in Enforcement Actions[12]

TDC recognizes that the Board occupies a distinct position relative to the OCC, FDIC, and NCUA with respect to BSA/AML program rule authority specifically. While FinCEN has delegated its authority to examine Board-supervised banks for BSA compliance to the Board, the Board also possesses independent authority to prescribe AML/CFT program requirements under Section 8(s) of the Federal Deposit Insurance Act, 12 U.S.C. 1818(s), separate from FinCEN's delegated examination authority. The Board's proposed rule reflects this distinction by omitting the notice-and-consultation framework included in the Agencies' April 10, 2026 proposal.

TDC's core position remains that meaningful FinCEN involvement in supervisory and enforcement decisions is valuable, and without it, the fairness and consistency benefits of AML/CFT modernization are harder to realize across the regulatory landscape. At the same time, the Board's distinct statutory footing may counsel against importing an identical notice-and-approval mechanism wholesale. TDC therefore recommends that the Board adopt a "notice" obligation, informing FinCEN when it contemplates a significant AML/CFT supervisory action, without conditioning its authority to act on FinCEN's affirmative approval, preserving the coordination benefits TDC has urged throughout this rulemaking while respecting the structural differences between the Board's supervisory posture and the Agencies'.

---

[11] Board of Governors of the Federal Reserve System et al., *Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision* (July 22, 2019, revised July 24, 2019). Federal Reserve, Joint Statement on Risk-Focused BSA/AML Supervision

[12] *Establishing and Maintaining an Effective Anti-Money Laundering and Countering the Financing of Terrorism Program*, 91 Fed. Reg. 42364, 42421 (2026). Federal Register, relevant section

Should the Board decline to adopt a notice obligation, TDC urges it to maintain consistency across the AML/CFT framework through ongoing engagement with relevant oversight entities, including the Government Accountability Office, to assess and mitigate the risk of fragmentation between the Board's approach and that of FinCEN and the Agencies. Whichever approach the Board ultimately adopts, TDC reaffirms the position raised throughout prior comments that meaningful FinCEN involvement in supervisory and enforcement decisions is essential to fair and consistent AML/CFT modernization and urges the Board to monitor whether its chosen approach achieves those objectives, revisiting the question if inconsistencies emerge.

VII. U.S. Location Requirement for BSA Officer[13]

TDC generally supports proposed §208.63(c)(3)'s requirement that a state member bank's AML/CFT officer be located in the United States and be "accessible to, and subject to oversight and supervision by, FinCEN and the Board." However, the proposed regulatory text does not address the preamble's guidance that "personnel located outside of the United States would still be permitted to perform certain AML/CFT functions," and the word "certain" leaves ambiguous which functions are considered appropriate for non-U.S.-based personnel.

TDC recommends that the Board add clarity in the regulatory text itself, making clear that except where specifically prohibited under existing law (such as restrictions on sharing SARs with personnel located outside the United States) state member banks may carry out any or all compliance functions using non-U.S. personnel, provided ultimate authority rests with an AML/CFT officer located in the United States.

Without this clarification, banks may unnecessarily centralize compliance functions in the United States, potentially reducing staffing, limiting 24-hour compliance coverage, or discouraging the use of non-U.S. compliance technology vendors even where those vendors offer the most effective tools to combat illicit finance.

VIII. Judgment of Examiners and Auditors

The preamble to the proposed rule states that "the Board does not believe that an examiner should substitute his or her own subjective judgment in place of the bank's."[14] TDC strongly agrees with this sentiment, and this is particularly important in the digital asset context. Examiners and independent testers may not have the same technological expertise in cutting-edge compliance tools that banks engaged in digital asset activity do, making the bank's own risk-based judgment more reliable in such instances.

---

[13] *Id.* at 42364, 42419 (2026) (Question 18). Federal Register
[14] *Id.* at 42364, 42366–67 (2026). Federal Register

TDC notes, however, that this guidance does not appear in the proposed regulatory text itself. It is critical that the final rule be amended to ensure examiners defer to risk judgments that a bank can demonstrate are specifically tailored to its business based on the risk assessment processes required under proposed §208.63(c)(1)(i). The same principle should extend to independent testing conducted under §208.63(c)(2): testing personnel, whether internal or third-party, should evaluate a bank's program against the bank's own documented risk assessment rather than substituting their own view of what the program should look like, which is consistent with TDC's recommendation above that examiners be provided objective criteria against which to evaluate banks' AML/CFT programs, with limited room to substitute subjective perceptions.

IX. Training of Examiners with Respect to Novel Technologies

The proposed rule emphasizes the importance of AML/CFT programs including an "ongoing employee training program."[15] TDC concurs but notes the proposed rule omits any parallel training requirement for Board examiners. As linchpins in the regulatory ecosystem, examiners should be held to just as high a standard of training and certification as the state member banks they supervise. In the digital asset space, a lack of examiner training and experience has been a recurring issue, with examiners at times inappropriately evaluating digital asset compliance methods against traditional standards with which they are more familiar.

TDC recommends that the Board add language to the final rule requiring examiners to engage in training equivalent to that required of state member banks under §208.63(c)(4), including specialized digital asset training and certification for examiners assigned to banks engaged in digital asset activity. The same requirement should extend to examiners overseeing banks involved with other innovative technologies, such as agentic payments or digital identity solutions. This proposed rule's goals will only be fully realized if examiners have training commensurate with the activities and technologies they are evaluating.

X. The Board Should Embrace Innovative Financial Technologies and Compliance Tools[16]

TDC notes that FinCEN's parallel April 10, 2026 proposal includes a specific request for comment (Question 28) on how the Director may consider the performance of innovative activities that produce demonstrable outputs under its proposed supervision and enforcement framework. [17] The Board's proposed rule includes no similar request. Given the Board's stated intent to align its final

[15] Board of Governors of the Federal Reserve System, *Anti-Money Laundering and Countering the Financing of Terrorism Programs*, 91 Fed. Reg. 42,363, 42,414 (2026).
[16] *Id.* at 42364, 42379, 42385 (2026). Federal Register (1) Federal Register (2)
[17] Financial Crimes Enforcement Network, Anti-Money Laundering and Countering the Financing of Terrorism Programs, 91 Fed. Reg. 18,704, 18,713 (Apr. 10, 2026).

rule with FinCEN's and the Agencies' rulemakings, and given that state member banks face the same technology-driven shifts in risk and compliance infrastructure, TDC urges the Board to consider this issue and ensure its final rule preserves comparable flexibility for banks to develop, pilot, and adopt emerging compliance infrastructure, particularly given the pace of change in tokenized securities, real-world assets, payment stablecoins, and agentic finance, where compliance models built around static reporting and retrospective audits may prove insufficient.

Many TDC members are actively building compliance tools suited to this environment, including AI- and blockchain-powered compliance infrastructure that illustrates the "art of the possible" for modernized AML/CFT supervision, including deterministic policy controls, continuous monitoring, AI-assisted governance, cryptographically verifiable proof artifacts, and tamper-evident audit trails. Preserving this flexibility, and crediting demonstrable innovation outputs in supervision and enforcement, would directly advance the proposed rule's objectives by encouraging more effective outcomes and giving examiners, law enforcement, and national security authorities more timely, reliable compliance evidence. Below, TDC briefly addresses certain evolving technologies and the need for a regulatory sandbox to encourage their adoption.

a. Digital Identity

TDC encourages the Board to recognize privacy-preserving digital identity, including wallet-based credentials, mobile driver's licenses, and other tools emphasizing user control, consent, and data minimization. This is an important component of a modernized AML/CFT framework, directly relevant to the Customer Identification Program requirement at §208.63(f) and ongoing customer due diligence at §208.63(c)(1)(iii). [18] [19] Current identity verification often relies on outdated methods (physical document uploads, excessive personal information collection, fragmented third-party databases) that increase fraud and privacy risk, particularly as AI tools make fraudulent documents, synthetic images, and deepfakes easier to produce. Properly implemented digital credentials can verify identity with high confidence while reducing unnecessary data exposure, directly supporting customer identification, due diligence, fraud prevention, and sanctions screening. [20]

---

[18] The Digital Chamber, Re: NCCoE's March 18 Proposal to Create a Project Focused on Software and AI Agent Identity and Authorization, April 27, 2026, available at https://digitalchamber.org/wpcontent/uploads/2026/04/TDC-NIST-RFI-Response-%E2%80%93-Software-and-AI-Agent-Identity-4.27.26.pdf.

[19] The Digital Chamber Re: NIST NCCoE's Draft Guidance for Fis Accepting Mobile Driver's Licenses, available at https://digitalchamber.wpenginepowered.com/wp-content/uploads/2026/05/TDC-NIST-mDL-ImplementationGuide-for-FIs-Response.pdf.

[20] Digital credentials, cryptographic signatures, device-based presentation, biometrics, wallet-based identity, verifiable credentials, and privacy-preserving verification that enables individuals to prove claims without repeatedly transmitting underlying personal data. See, e.g., National Institute of Standards and Technology, *Digital Identity Guidelines*, SP 800-63-4, available at https://pages.nist.gov/800-63-4/; SpruceID, *What Are Verifiable*

The Board should provide clear, technology-neutral guidance confirming that banks may use digital identity tools to satisfy or support BSA obligations under §208.63(c) and (f), where such tools are reasonably designed, risk-based, auditable, and governed – without prescribing a single identity architecture, and instead recognizing multiple models including credential issuer frameworks, wallet-based presentation, and interoperable standards-based credentials. [21] The Board should also recognize that identity and authorization are distinct but related functions, as authentication establishes who an actor is, authorization determines what it may do. This distinction will grow more important as AI agents and delegated authority models become more common and should ensure the AML/CFT framework remains flexible enough to accommodate both human and non-human actors provided banks can establish accountability and appropriate controls.

b. Blockchain Analytics, Transaction Monitoring, and Ecosystem Monitoring

TDC encourages the Board to recognize the role that blockchain analytics, transaction monitoring, ecosystem monitoring (***"know-your-ecosystem" or "KYE"***), compliance evidence, and security assurance tools can play in modern AML/CFT compliance. This is directly relevant to the Board's supervisory perimeter, as an increasing number of state member banks maintain subsidiaries, correspondent relationships, or counterparty relationships with Permitted Payment Stablecoin Issuers (***"PPSIs"***) and other digital-asset entities and need effective tools to monitor risk from those relationships under §208.63(c)(1).

While public blockchains present attribution challenges from pseudonymous addresses and cross-chain activity, they also provide transaction transparency unavailable in traditional finance.[22] Paired with appropriate analytics, this transparency can help banks, examiners, and law enforcement identify illicit finance, trace proceeds, and support recovery. [23] Blockchain analytics can identify exposure to sanctioned entities and other illicit activity; transaction monitoring can detect suspicious patterns directly relevant to a bank's ongoing due diligence obligation under

---

Digital Credentials?, available at https://spruceid.com/learn/vdc-intro; SpruceID, *How Do Verifiable Digital Credentials Prove Who I Am?*, available at https://spruceid.com/learn/proving-id; W3C, *Verifiable Credentials Data Model v2.0*, available at https://www.w3.org/TR/vc-data-model-2.0/.

[21] 9 Credential issuer frameworks, wallet-based presentation, derived-attribute verification, cryptographic proof of possession, and standards-based credentials. See, e.g., W3C, Verifiable Credentials Data Model v2.0, available at https://www.w3.org/TR/vc-data-model-2.0/; International Organization for Standardization, ISO/IEC 18013- 5:2021, Personal identification — ISO-compliant driving license — Part 5: Mobile driving license application, available at See, e.g., https://www.iso.org/standard/69084.html.

[22] Public blockchain transparency and digital asset transaction traceability generally.

[23] General ecosystem of digital asset compliance tools: Elliptic; Solidus Labs; Glassnode; CAT Labs; CoinStructive; CompliLedger; SpruceID; Cryptio; ZenLedger.

§208.63(c)(1)(iii); and compliance evidence tools can document control operation to support examiner review under the independent testing requirement at §208.63(c)(2).

One emerging approach combining these capabilities is ecosystem monitoring, or KYE, which uses blockchain transparency to analyze stablecoin activity behaviorally across an issuer's full permissionless footprint, rather than transaction-by-transaction against private customer records, surfacing layering, structuring, and other risk invisible to point-in-time screening.[24] This is particularly relevant for banks with PPSI exposure: empirical research on transaction topology finds that over 80% of known exploiter addresses are non-KYC-adjacent wallets, many operating more than five transaction "hops" from any regulated counterparty. [25] [26] Ecosystem monitoring is not a replacement for customer due diligence or sanctions screening, but a complementary risk-management tool, and the Board should encourage banks to pilot and adopt such tools where reasonably designed, risk-based, auditable, and governed.

Real-time observability also supports asset tracing and security assurance, since banks may identify suspicious source-of-funds exposure before accepting a deposit, detect links to known exploits before permitting withdrawals, or generate verifiable evidence of how controls operated. This evidence is directly relevant to independent testing under §208.63(c)(2). Because many illicit finance events originate from technical compromises, smart contract vulnerabilities, or private key theft rather than pure financial crime, tools supporting security audits, proof-of-reserves verification, and incident response can meaningfully reduce downstream laundering and victim losses, consistent with the Board's own view that an effective program is one reasonably designed to manage risk, not one that satisfies a fixed checklist. [27]

c. Supervisory Treatment of Innovative Compliance Tools

[24] Stablecoin Monitoring and Ecosystem Monitoring Solutions. See, e.g., Solidus Labs, Stablecoin Monitoring, available at https://www.soliduslabs.com/solutions/stablecoin-monitoring.

[25] Japan's Financial Services Agency has similarly found that on-chain data alone is insufficient to assess ecosystem integrity without correlation to off-chain data such as accounts and redemption patterns, and Gartner's March 2026 Innovation Insight identifies combined on-chain/off-chain monitoring as the emerging institutional standard for managing secondary-market risk.

[26] Japan Financial Services Agency & QUNIE Corporation, *Report of FSA's Joint Research on Analyzing Decentralized Financial System Using On-Chain and Off-Chain Data* (June 2023); Christophe Uzureau, David Furlonger & Hannah Edmunds, Gartner, *Innovation Insight: Fractionalization and Tokenization of Assets Transform Financial Markets* (Mar. 9, 2026). JFSA/QUNIE Report; Gartner Report.

[27] Digital asset forensic investigation, tracing, and recovery providers. See, e.g., CAT Labs, Recovery CAT, available at https://www.catlabs.io/recoverycat; CoinStructive, PathTracer, available at https://www.coinstructive.com/company/pathtracer; CoinStructive, Our Crypto Investigation Process, available at https://www.coinstructive.com/company/our-process.

Consistent with that principle, the Board should make clear that banks may use these tools as part of the risk-based controls required under §208.63(c)(1) and should neither treat them as categorically required nor categorically sufficient, since their appropriate use depends on a bank's risk profile, products, and operational role. The Board should avoid rigid standards that lock banks into a single vendor, methodology, or architecture, and should recognize that these tools are most effective when paired with strong governance and human review. Consistent with TDC's recommendation above regarding examiner judgment, examiners should not treat the absence of any particular tool or vendor as evidence of a program deficiency; the relevant question is whether a bank's program is reasonably designed to manage its illicit finance risk, and the Board should expressly encourage adoption of these tools as part of that technology-neutral, risk-based approach.

XI. Creation of Regulatory Sandbox to Support Compliance Innovation

Banks increasingly need flexibility to test and deploy new technologies to keep pace with evolving illicit finance risks, but often face substantial regulatory uncertainty when piloting new AML/CFT tools, and may hesitate to test promising technologies, such as AI-enabled transaction monitoring or digital identity solutions, if doing so could later be second-guessed by examiners or characterized as a program weakness. To address this, the Board should create a regulatory sandbox or comparable supervised pilot framework allowing state member banks to test innovative AML/CFT technologies without fear that good-faith experimentation will itself result in supervisory criticism or enforcement action.

A meaningful sandbox should include an express safe harbor: at minimum, the Board should provide that a bank participating in an approved pilot will not be subject to an AML/CFT enforcement action or significant AML/CFT supervisory action under §208.63(g) solely because the pilot does not achieve its intended results, identifies gaps in existing monitoring, or requires calibration during testing. The purpose of a pilot is to test and learn; if banks face penalties for unsuccessful but responsible experimentation, many will reasonably avoid innovation and continue relying on legacy systems that may be less effective against modern illicit finance threats. Such a safe harbor would be consistent with prior interagency recognition in 2018, when the Board, FinCEN, and the other federal banking agencies jointly encouraged banks to consider innovative approaches to BSA/AML compliance, and Treasury's accompanying release similarly noted that pilots identifying program gaps would not necessarily result in supervisory action. [28]

[28] FinCEN, Treasury's FinCEN and Federal Banking Agencies Issue Joint Statement Encouraging Innovative Industry Approaches to AML Compliance, December 3, 2018, available at https://www.fincen.gov/news/newsreleases/treasurys-fincen-and-federal-banking-agencies-issue-joint-statement-encouraging

TDC recommends that the sandbox or pilot framework include, at minimum, the following elements:

- A regulatory safe harbor providing that good-faith participation in an approved pilot will not form the basis for an AML/CFT enforcement action or significant AML/CFT supervisory action;
- Protection for unsuccessful pilots, provided the bank acts in good faith, maintains appropriate controls, and continues to satisfy its established AML/CFT program obligations under §208.63(c) and (d);
- Examiner guidance directing examiners not to penalize banks merely because a pilot uses novel methods or produces different outputs than legacy systems;
- Confidential information-sharing mechanisms that allow banks to share pilot results, lessons learned, and typology insights with the Board and other banks without creating undue litigation, supervisory, or competitive risk; and
- Post-pilot feedback from the Board to support broader adoption of successful technologies and refinement of supervisory expectations.

TDC recognizes that a fully harmonized sandbox framework would require coordination across the Board, FinCEN, and the Agencies. TDC believes the Board can preserve appropriate supervisory oversight while reducing the fear that responsible experimentation will be punished, and that this balance is especially important in the current fast-moving financial environment.

XII. Conclusion

TDC is grateful for the opportunity to comment on the Board's proposed rule and supports the Board's goal of a process that is more equitable, and that empowers state member banks to engage creatively in compliance tailored to their needs. Implemented properly, TDC believes the Board is correct in its assessment that this approach will result in greater success in combatting AML/CFT issues across the financial system.

TDC would be pleased to engage further on any topics covered in this comment and look forward to future engagement with the Board in navigating these critical issues in the digital asset space.

Best,

Zunera Mazhar, Head of Global Policy and Government Affairs

CC:

Jonathan Rufrano, Policy Director
Abraham Fich, Policy Associate