FTA
FINANCIAL
TECHNOLOGY
ASSOCIATION

February 14, 2022

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Response to Request for Information on Review of Bank Secrecy Act Regulations and Guidance
(FINCEN-2021-0008)

The Financial Technology Association (FTA) appreciates the opportunity to respond to this request for information (RFI) regarding a review of Bank Secrecy Act (BSA) regulations and guidance issued by the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN). The FTA applauds FinCEN's forward-leaning approach to modernizing financial crime regulation and its related efforts in recent years.

FTA is a nonprofit trade organization that educates consumers, regulators, policymakers, and industry stakeholders on the value of technology-centered financial services and advocates for the modernization of financial regulation to support inclusion and innovation. FTA focuses on informing tomorrow's regulations, policy frameworks, and public understanding to safeguard consumers and advance trusted digital financial markets and services.[1] We welcome the opportunity to engage with FinCEN on the critically important topic of modernizing application of the Bank Secrecy Act (BSA) and related AML compliance to ensure the efficiency and effectiveness of the overall regime in satisfying national security interests without undue burden on financial services activity.

FTA Members: At the Forefront of BSA/AML Compliance Innovation

Many FTA members are subject to BSA requirements, and all are at the front lines of financial services innovation and digital customer engagement. It is this spirit of innovation that allows our members to provide services in ways that traditional financial institutions cannot and reach underserved or unbanked populations and bring them into the formal financial sector. Because our members deal with the most sensitive aspect of our customers' lives, their finances, FTA members accordingly develop robust BSA compliance teams and policies that apply a risk-based

[1] FIN. TECH. ASS'N, www.ftassociation.org (last visited Jan. 4, 2022). The FTA's members include Afterpay, Betterment, BlueVine, Brex, Carta, Figure, Klarna, Marqeta, MX, Nium, Plaid, Ribbit Capital, Sezzle, Stripe, Truework, Wise, Zest AI, and Zip.

framework to novel scenarios and are active leaders advancing modern compliance solutions. Whether in the context of lending, payments, buy-now-pay-later, investment, or robo-advisory services, FTA members are engaged in the most timely and relevant areas of BSA application.

More specifically, FTA members frequently rely on the most innovative technologies and customer engagement channels to offer services, which means they deal with the most timely issues relating to BSA compliance on a regular basis. FTA members are leaders in using new technologies to satisfy compliance requirements giving them a key perspective in understanding how existing AML regulatory frameworks facilitate or impede the development of promising regtech or related compliance solutions. Against this backdrop, FTA respectfully submits the following recommendations to advance innovative, effective, and efficient AML compliance frameworks and solutions.

Importantly, FTA members do not operate in a vacuum. Many of our members partner with more traditional financial institutions of all sizes, so the regulatory intersection between established financial institutions and FTA members is also an area of deep interest and innovation, including with respect to AML compliance. Additionally, many fintech firms are actively seeking and securing bank and related charters, which further increases the importance of the topics raised in this request and the recommendations provided below.

RFI Recommendations

Support of the BSAAG AMLE Working Group Recommendations & Call for Greater Fintech Participation

FTA strongly supports prior BSAAG AMLE working group recommendations and respectfully urges further expansion of the group to include AML compliance expertise from the financial technology sector. BSAAG has been and will continue to be a resource that fosters critical collaboration between the government and industry in combating financial crime. By increasing participation from the fintech sector, BSAAG can build on its prior recommendations to produce smarter, more technology-focused regulations that go to the central goals of protecting the U.S. financial system from abuse and providing law enforcement with timely, highly valuable intelligence.

Ensuring the Effectiveness of BSA/AML Regulations and Guidance

The BSA/AML regime has grown organically over time and accumulated many “best practices” that, while not codified, have taken on the force of law. The FTA applauds FinCEN and its partner agencies in clarifying the legal status of these “best practices” and, in some cases issuing new guidance that clarifies regulatory requirements. However, despite these efforts, the concept of what constitutes an "effective" BSA program remains elusive. To that end, FTA makes the following recommendations:

- **Promote Consistency in How Regulator's Measure Effectiveness.** FinCEN should provide a clear, objective standard for effectiveness that applies across all BSA regulators to reduce regulatory arbitrage. To this end, FTA agrees with specific recommendations set forth in the Bank Policy Institute's November 16, 2020 comment to FinCEN's advance notice of proposed rulemaking related to AML program effectiveness.[2] Specifically, FTA agrees that a financial institution's AML program should be judged based on: (1) the institution's unique activities and risks; (2) the program's output, including but not limited to SARs, law enforcement engagement, and other efforts to provide timely, valuable data to law enforcement; and (3) continuous improvement and innovation. The program should not be judged based on: (i) the technical structure of the program; (ii) "best practices" not grounded in binding law or regulation; and/or (iii) a standard that requires near perfection and focuses on technical violations rather than program failures.

  Additionally, FinCEN should ensure that risk assessments are sufficiently flexible to allow institutions to develop and maintain a reasonable, risk-based program and ensure that resources can be dedicated to actual, rather than perceived, regulatory risks. FinCEN should explicitly acknowledge that institutions may make risk-based decisions to stop undertaking certain tasks even where that decision may result in lost SARs where the loss is significantly outweighed by the cost of the control and the degree of usefulness of the information.

  Finally, FinCEN should work with its peer regulators to ensure that expectations regarding effectiveness are examined consistently across each agency. Currently, regulators may take different positions on what practices satisfy an effectiveness standard. This inconsistency can be costly and time-consuming for the regulated entity, and it can undermine program effectiveness by incentivizing a race to the lowest common denominators across regulators. Regulators should therefore coordinate closely on examination expectations in order to ensure consistent interpretations and outcomes. Regulators might also consider having a common set of examiners across the agencies who focus on fintech firms or issues in order to ensure consistency.

- **Enhance Communication.** FinCEN should work closely with law enforcement, national security, and regulatory agencies to determine an approach for tactical AML priorities.

[2] Bank Policy Institute, *Re: Request for Comment Regarding Anti-Money Laundering Program Effectiveness* (Nov. 16, 2020), available at https://bpi.com/wp-content/uploads/2020/11/BPI-Comment-Letter-re-FinCEN-AML-Program-Effectiveness-ANPRM-vF.pdf.

These tactical priorities must be appropriately bounded in scope and time not to become amorphous "best practices" or part of a laundry list of other priorities that are not part of the overall AML priorities process. Additionally, as has been consistently promoted by BSAAG, it is critical to continue building channels for regular and ongoing feedback between law enforcement and financial institutions to more effectively integrate new AML priorities into compliance programs.

Modernizing Outdated or Inefficient Regulations

The existing AML/CFT regime includes outdated regulations that fail to account for new, technology-driven entrants to the financial services sector. To better leverage current and future technological innovations and ensure new entrants, including nonbank financial services companies that can meaningfully contribute to AML/CFT efforts, we recommend changes to four primary aspects of the BSA regime: (i) Information Sharing, (ii) Transaction Monitoring and Reporting, (iii) CIP and CDD, and (iv) BSA Examination. Below we aggregate the first two categories, and further on in the comment specify ways that technology and innovation can improve all aspects of the BSA regime.

Information Sharing & Transaction Monitoring and Reporting:

Currently, financial institutions are limited in the type of information they can share and the reasons for sharing such information with other financial institutions. This inability to proactively share, except in cases of an actual suspicion of financial crime, has severely limited transaction monitoring innovation, including through federated learning for models or joint detection scenarios among peer institutions. Additionally, FinCEN can further enhance public-private information sharing by implementing new processes for agencies to communicate investigative priorities to financial institutions regularly.

- **Facilitate Greater Industry Collaboration.** FinCEN should allow FIs to share customer information for the express and limited purposes of joint detection of financial crime and joint investigations. FIs should further be permitted to file one joint SAR, subject to appropriate privacy controls, to drive a more efficient reporting system.

- **Enhance Public-Private Information Sharing.** The FinCEN Exchange launched in 2017 to improve communication between government and industry and thereby enable financial institutions to better identify risks and prioritize efforts. FinCEN should build on this positive initiative by developing and implementing a technology-enabled mechanism for government authorities to provide regular feedback to financial institutions on investigative priorities, as well as filed SARs, to allow FIs to target their internal monitoring to serve law enforcement and national security goals better.

Additionally, FinCEN should employ a "customer-centric" model and ensure that dialogue related to changes and prioritization of AML/CFT efforts in the United States reflects the input, needs, and objectives of the end-users of SAR data (primarily law enforcement and national security agencies). A technology-enabled platform can facilitate this level of collaboration, which benefits government and industry alike. For example, an accessible, regularly updated, and substantive database that facilitates the ability of FIs to share their data and that fosters communication on emerging threats, risks, and opportunities can vastly improve controls to detect and fight crime.

As is well documented, FinCEN receives more data than it can adequately consume, and much of the data does not serve regulatory or law enforcement interests. To reduce the burden of sharing unhelpful information, FinCEN should:

- **Update SAR Filing Triggers.** FinCEN should modernize the criteria that trigger SAR filing obligations and remove any that are obsolete or which offer little law enforcement or national security value based on statistical rather than anecdotal evidence. All key terms and advisories published by FinCEN should be time-bound to ensure that they become inactive after a set time unless affirmatively renewed to keep institutions focused on current threats. For those key terms and advisories that are renewed, FinCEN should routinely review and update them to ensure that they remain relevant. Additionally, FinCEN should eliminate the 90-day continuing activity review requirement for any matters where there is not law enforcement engagement.

- **Raise the Bar for Materiality.** Ambiguity regarding the materiality or severity of information that should be reported incentivizes over-reporting of information of little real-world value to law enforcement. FinCEN should accordingly specify the scope of the type of conduct and clarify the level of suspicion or evidence of that conduct that triggers an obligation to file a SAR to reduce defensive filing. For example, the filing of SARs based on "transaction[s] [with] no business or apparent lawful purpose" should require that there are additional facts beyond this standard that provide a basis for suspicion. A SAR should not be required simply because a transaction lacks an identifiable business or lawful purpose, or is not a transaction in which a customer would normally be expected to engage. Additionally, FinCEN should update its SAR form to keep up with reported typologies, including increasing the file size limit and the narrative character limit.

- **Clarify Expectations Regarding Low-Risk SARs and Client Decisioning.** FinCEN should clarify the scope of certain expectations with respect to SAR filings. In particular, it should clarify that after the institution reaches the requisite level of suspicion to file a SAR, it is not required to conduct a further review of additional transactions or counterparties related to the filing unless and until the SAR generates engagement with law enforcement. Additionally, for no-SAR decisions, a short, concise statement describing an institution's rationale for not filing a SAR should be sufficient documentation. The institution should not be expected to draft a detailed description of the investigation or retain supporting documents, as this creates undue and unnecessary burden. Additionally, if an institution files multiple SARs on a single customer, there should be no requirement or expectation that the institution will exit the customer after filing a certain number of SARs. Instead, the actual financial crime risk should be the sole deciding factor in whether a customer is retained.

- **Reduce Unnecessary and Duplicative Reporting.** In addition to sharing what is highly relevant, FinCEN could specifically carve out categories of information that can be excluded from reporting. For example, FinCEN should update guidance, including the application of the 2016 advisory addressing cyber-events, to specify that where information has been provided to law enforcement through another channel (such as often occurs with Cyber events), no additional SAR reporting is required.

Customer Identification Program (CIP) and Customer Due Diligence (CDD):

Regulatory expectations and requirements regarding CIP and CDD elements of BSA compliance programs must keep pace with the nature of threats, FI relationships with third-parties, and technology-driven solutions. As a threshold matter, given the prevalence of partnerships between FIs and third-party fintechs and vendors, FTA urges FinCEN to clarify that non-BSA regulated entities who partner with BSA regulated entities are covered by BSA safe harbors when they are engaged in BSA activities on behalf of the regulated partner. This necessary certainty will enhance collaboration between all involved parties in ensuring an effective compliance program.

With respect to CIP expectations, in light of the rapidly changing technology landscape, the legacy CIP regime is outdated both as to the elements institutions are required to collect, as well as the required methods of collection and validation. Additionally, due to existing reliance on outdated methods for identity verification, the CIP regime is subject to significant exploitation by criminals through use of synthetic IDs and perpetration of identity theft and other forms of identity fraud.

In light of these issues, and the helpful role that new technologies could play in identity verification, FTA recommends that FinCEN develop a dedicated workstream focused on identity. To this end, FTA applauds FinCEN for partnering with the FDIC on its recently announced digital identity tech sprint, and further encourages FinCEN to pursue revisions to existing CIP rules, subject to notice and comment, with a focus on providing FIs with more flexibility in terms of what identity elements they collect and how they collect and validate them. Revisions to existing requirements should focus on future-proofing regulation by allowing institutions much greater flexibility to update CIP programs in order to take advantage of future innovations in identifying their customers—including the ability to source customer information from third-party vendors and to leverage new technologies, such as those based on zero-knowledge proofs, to help solve for privacy and identity requirements simultaneously.

With respect to CDD requirements, FinCEN should address the undue burden placed on financial institutions by current rules on recollection and instead move to a risk-based approach for all recollection. FinCEN should also provide additional exemptions for low-risk legal entity customers, such as foreign publicly traded companies and supranational entities, that remain subject to the CDD rule's beneficial ownership collection requirement.[3]

Finally, pursuant to the BSA, FIs can rely on another institution's CIP and CDD provided that the other institution is regulated by the BSA. With the increased partnership between fintechs and BSA-regulated institutions, we recommend that reliance be expanded to situations in which a BSA regulated entity has partnered with a technology company that voluntarily maintains a BSA program and where the BSA regulated entity has satisfied itself that the program meets relevant standards. Standards may be established through industry practice and public-private standards setting organizations. This approach can streamline BSA compliance, avoid duplication of activities, and incentivize the development of more effective compliance solutions.

Examinations:

One of the greatest challenges facing modernization of the BSA are the differing examination standards and compliance requirements imposed by different federal regulators. It is not uncommon, for example, for FIs to receive conflicting requirements from different regulators as to the same provision of the BSA. Accordingly, we strongly recommend that FinCEN – in partnership with its peer banking regulators – issue guidance that provides a consistent, single interpretation of the BSA and AML program requirements.

As part of this effort, FTA recommends the following:

[3] FTA provides further comment on the beneficial ownership registry in the section below, but underscores here that FinCEN should ensure that the information in the registry is reliable as a centralized source of beneficial ownership information about reporting companies and that financial institutions and their partners may rely on that information if they choose to do so.

- The Federal Financial Institutions Examination Council (FFIEC) manual should focus on high-risk attributes rather than "high-risk" activities.
- The FFIEC should ensure that both the Manual and examiner training reflect the regulatory amendments and the objectives of AMLA/AML Program Effectiveness ANPRM, as well as the flexibility afforded by recent FinCEN guidance, including the Model Risk Management Interagency Statement.
- The FFIEC Manual should be clear that institutions are expected to reallocate resources, as appropriate, in light of the regulatory amendments, and that such amendments are not intended to cause a net increase in overall program resources.
- Incentives for financial institutions to develop innovative methods for identifying and otherwise taking proactive measures to assist law enforcement should be included in the Manual, even if those improvements fall outside the current requirements of the BSA. This could take the form of recognition in exam reports of proactive efforts by financial institutions, which go beyond both statutory and regulatory requirements—embodying the stated statutory purpose of the BSA regime. These efforts should be commended and incentivized.
- Ensure that SAR filing standards are consistent across regulators.
- Provide additional guidance and training to examiners making it clear that they should not substitute their judgment on SAR decisions absent a systemic program failure.
- Clarify that monitoring or other program failures caused by technology issues should not be the basis for a formal or informal enforcement action provided: (1) the institution corrected the failure; (2) the institution took a risk-based approach to remediating the impact if any; and (3) the failure was not part of a larger systemic issue with the overall program.

Fostering Innovation and Technology Adoption

As highlighted throughout this comment letter, FTA believes that further innovation and adoption of technology-driven AML solutions is a central pillar of overall program modernization and effectiveness. FTA commends FinCEN on its forward-leaning posture and steps that have been taken in recent years to foster responsible use of technology, including joint federal regulatory initiatives.[4] The following are specific ways to build on this progress:

- **Support Use of AI/ML Tools and Automation Through Enhanced Guidance**. Dynamic AI/ML tools hold promise in leapfrogging the efficiency and effectiveness of legacy, rules-

[4] *See, e.g. Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), available at https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf.

based detection software. FinCEN should foster the development of such tools by updating guidance to provide industry with greater certainty regarding regulatory expectations around AI/ML adoption. While explainability of AI/ML models is an important requirement, regulators should consider the particular application of AI/ML tools when determining what degrees of explainability are permissible. For example, the context of suspicious activity detection is distinct from consumer credit underwriting, which should translate into different regulatory expectations.

Additionally, regulators should provide guidance, including by way of no-action letters, for financial institutions to satisfy their SAR filing obligations through automated processes. For example, very little benefit is derived from investigating and manually reporting smurfing activity or funnel accounts. However, significant time is lost due to the standard investigation timeline. In cases such as this, institutions should be able to automate this detection and file SARs without manual intervention.

In 2019, the OCC issued an interpretive letter that clarified that a financial institution could, in a particular instance, use software to automate identification and reporting of a suspicious activity.[5] FTA commends the OCC's approach and encourages all regulators, including FinCEN, to identify opportunities where automation can responsibly reduce manual activities that provide little benefit to an AML program's effectiveness.

Additionally, FinCEN should leverage technological innovation to make CTR filing automated above a certain threshold, which will increase the timely submission of "highly useful" information to law enforcement. This automated filing would permit FinCEN to then remove current aggregation requirements. It could also lead to the elimination of the static CTR form itself, which could be replaced by direct submission of basic cash transactional data from financial institutions to FinCEN.

- **Facilitating Testing and Implementation of New Tools**. Advances in AI/ML and automation are driving the rapid development of new regtech solutions that can result in more efficient and effective compliance outcomes. FTA applauds federal banking agencies for launching a number of initiatives in recent years to advance these efforts. For example, in December 2018, FinCEN, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency issued a joint statement encouraging financial institutions to take innovative approaches in their AML compliance

[5] OCC, *Interpretive Letter #1166* (Sept. 27, 2019), available at https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2019/int1166.pdf.

programs. More can be done to build on this forward-leaning posture, including the following measures, which would speed the pace and adoption of new AML compliance solutions:

- *FinCEN Sandbox*. FinCEN should develop a voluntary sandbox environment for innovators to develop, test, and showcase new AML detection and compliance solutions. The sandbox could offer developers properly curated and/or anonymized data sets to help train new models. If FinCEN clearly defines objectives and provides guideposts, innovators can further develop and implement "smart" machine learning-based technologies that can help identify patterns and behaviors that current rules-based systems, built on static monitoring rules, are incapable of detecting. Greater latitude for regtech innovation can optimize efficiency without further complicating legacy systems and processes and perhaps eventually replace static rules. A sandbox environment would further benefit both innovators and FinCEN in understanding the benefits of particular innovations and speeding their in-market introduction.

- *Reduce Duplication Requirements*. Banks seeking to implement a new AML compliance solution are generally required to run the new system alongside legacy systems for a significant period to ensure the effectiveness of the new system and avoid gaps in the compliance program. The cost and operational burden of running parallel systems is a large disincentive to adoption of new technologies. This is especially true for small and midsize institutions that do not have the employee bandwidth or size to maintain two systems for a longer period of time. Regulators should reduce the timeframe for such parallel operation and instead allow the financial institution to rely on reasonable evidence of new model sufficiency in order to retire legacy systems.

- *Allow Reliance on Vendors*. Many small and midsize institutions are unable to develop their own monitoring systems or models due to lack of expertise and cost. Accordingly, they rely on vendors to supply monitoring systems and ensure that such systems are fit for purpose. Such institutions should be allowed to rely on these vendor solutions and not be required to test or validate them. Rather, FinCEN should validate such systems and their models – or rely on public-private standards setting organizations and third-party validators to do so – which would both create cost efficiency and level the playing field with larger institutions who can afford to build and test systems.

  - *Accept Trade-Offs*. Related to the prior recommendation that regulators allow FIs to rely on reasonable evidence of model effectiveness, regulators should also explicitly note that a new model may be preferable to a legacy system even if the new model fails to fully flag all low-value alerts as compared to that prior system. In other words, regulators must recognize that there are always tradeoffs with new AML compliance models and approaches, and that the goal should be focused on the efficient and effective identification of high-value information for law enforcement. A failure to explicitly accept trade-offs will chill adoption of new technologies.

- **Fintech Access to an API-Driven Beneficial Owner Registry**. A range of fintech third-party vendors and state-regulated money services businesses (MSBs) partner with BSA regulated entities and share BSA responsibilities with such partners. FinCEN could substantially enhance the efficiency and effectiveness of BSA compliance programs by allowing these third-parties, subject to appropriate safeguards, to access the beneficial owner registry via an API-based system, which would allow automatic and real time access for authorized users.

  With respect to the types of safeguards FinCEN might require, state-regulated MSBs frequently have established written policies and procedures, as part of BSA-required risk-based AML compliance programs, to identify and verify beneficial owners of legal entity customers as required by FI customers. Additionally, FinCEN might condition third-party access to use of the beneficial ownership registry information solely to verify beneficial ownership information for the purpose of compliance under the BSA.

Conclusion

The FTA appreciates the opportunity to provide recommendations in response to FinCEN's request for information. We believe that further modernization of the BSA/AML regime can result in a more effective and efficient system to combat financial crime. We look forward to serving as a resource to FinCEN on this important effort.

Sincerely,

Penny Lee

Penny Lee
CEO
Financial Technology Association