SIIA

SIIA Comments on FinCEN's AML/CFT Proposed Rule

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide comments on FinCEN's "Anti-Money Laundering and Countering the Financing of Terrorism Programs" NPRM.[1] SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include roughly 375 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide, and companies specializing in data analytics and information services.

We recognize the laudable goals of the proposed rule. In this vein, we hope to point out specific concerns we have around the context of the rule, specifically as it relates to the availability and processing of beneficial ownership information (BOI) and barriers to the productive adoption of privacy-enhancing technologies (PETs). As a practical matter, we emphasize that the Corporate Transparency Act (CTA), as currently drafted and interpreted, would unintentionally hamstring the goals of the proposed rule and its focus on anti-money laundering (AML) and countering the financing of terrorism (CFT) priorities. Furthermore, regulatory barriers to the adoption of PETs in the financial sector continue to limit the potential of PETs to advance AML and CFT objectives.

Question 3: How can FinCEN make the AML/CFT Priorities most helpful to financial institutions in the context of the proposed rule?

The Proposed Rule would require financial institutions to establish AML/CFT programs with a new series of explicit minimum requirements, most notably incorporating government-wide AML/CFT priorities along with implementing a mandatory risk assessment process. As FinCEN works to finalize the Proposed Rule to promote an effective and risk-based AML/CFT framework, it should also expand access to its BOI registry to third-party service providers, on an ongoing basis, which analyze and augment this data on behalf of financial institutions. This is particularly true of enabling financial institutions to undertake the Proposed Rule's mandatory risk assessments in the specified categories of illicit finance activity risks around distribution channels, customers, geographic locations, and intermediaries.

Notably, this would require a reexamination of FinCEN's current interpretation of the CTA that FinCEN data may only be disclosed to financial institutions, and thus entities under contract with them including service providers, "[u]pon receipt of a request from a financial institution subject to customer due diligence requirements under applicable law for information reported pursuant to § 1010.380 to be used in facilitating compliance with such requirements."[2]

[1] Federal Register :: Anti-Money Laundering and Countering the Financing of Terrorism Programs.

[2] 31 CFR 1010.955(4)(i); *See* 31 CFR 1010.955(a).

Doing this will help to achieve the goals of the Proposed Rule and address an impediment to effective AML/CFT compliance created by the regulations implementing the CTA.

Background

On December 21, 2023, FinCEN issued a final rule implementing provisions of the CTA that altered the circumstances under which BOI reported to FinCEN may be disclosed to authorized recipients, as well as how those recipients must protect BOI.[3] Under the CTA and the rule, FinCEN may disclose BOI to financial institutions subject to customer due diligence requirements, which includes third-party service providers acting on the financial institutions' behalf.[4]

Notably, prior to the CTA and the rule, these service providers enjoyed general access to a series of databases that included BOI. Such firms then undertook a range of risk data services to assist financial institutions in complying with AML and CFT requirements, as well as know-your-customer (KYC), sanctions, performing customer risk ratings and monitoring transactions more generally, and complying with a host of other regulatory obligations.

The new 31 CFR 1010.955(a) regulations, which went into effect February 20, 2024, permit third-party service providers to access FinCEN BOI only through their financial institution customers on a case-by-case basis, and for use only in connection with assisting the financial institution that provided access to the BOI. They do not permit third-party service providers to use FinCEN BOI in combination with other data the third-party service providers maintain and collect to assist in critical diligence obligations – an integral part of the service they previously provided to multiple financial institutions.

How Service Providers Enable Risk-based AML/CFT Compliance

Aggregating BOI with other data, however, is essential to make sense of BOI, and provide financial institutions and the market at large with critical functions that advance compliance with regulatory requirements and the tracking of illicit financial activity. On the other hand, restrictions on aggregation renders any risk-based AML/CFT regulatory structure less sound because of the important role that third-party service providers in the data risk business provide. In general, this reduces the ability of financial institutions to implement effective and risk-based AML/CFT programs in line with government priorities under the proposed rule, particularly the effectiveness of mandatory internal risk assessments conducted by these institutions around distribution channels and geographic locations.

---

[3] See FinCEN, Fact Sheet: Beneficial Ownership Information Access and Safeguards Final Rule (Dec. 21, 2023), https://www.fincen.gov/news/news-releases/fact-sheet-beneficial-ownership-information-access-and-safeguardsfinal-rule.

[4] https://www.federalregister.gov/d/2023-27973/p-384.

First, the 31 CFR 1010.955(4)(i) limitation that BOI may only be provided upon receipt of a request by a financial institution will have a notable impact on small and mid-sized financial institutions, such as regional and community banks, that have limited internal resources to conduct robust AML/CFT diligence processes without the help of screening services provided by third parties. Furthermore, data aggregation is essential to track activity by criminals and malicious actors who are adept at evading regulations. For third-party service providers not to possess ongoing access to BOI renders it impossible to combine this data with other data sets, and consequently more challenging for financial institutions of all sizes to track illicit activity and make informed risk management decisions.

There are several examples of services provided by third-party service providers that illustrate how this rule will hamper the effectiveness of AML/CFT programs as well as the proposed risk assessments. First, it leads to dilution of the quality of implicit sanctions data, which service providers undertake to uncover corporate ownership connections to blocked persons. This has a direct impact on sanctions, AML/CFT, and other core components of the financial crime regulatory structure.

The current rule also dilutes financial institutions' abilities to identify politically exposed persons (PEPs). Third-party service providers that undertake PEPs analyses identify entities that are 25 percent or more owned or controlled by PEPs. This is critical to preventing PEPs that are engaged in criminal activities from hiding ill-gotten proceeds through legal entities. On the other hand, without a fulsome identification of PEPs, financial institutions would be unable to identify all entities that PEPs may be using to engage in illicit activity. This, in turn, directly affects the Proposed Rule's risk assessment priorities to protect against illicit finance activity risks around both customers and intermediaries.

To better effectuate the intent of the proposed rule, SIIA encourages FinCEN to reexamine its interpretation of the CTA that FinCEN data may only be disclosed to financial institutions or service providers on a per-request basis. Alternatively, FinCEN may wish to work with Congress to amend the CTA to clarify that it broadens access to FinCEN's BOI registry for third-party service providers that are in the business of helping companies combat illicit finance and comply with the AML/KYC obligations that are the focus of the Proposed Rule.

Question 38: The proposed rule provides for the consideration of innovative approaches to help financial institutions more effectively comply with the BSA, but does not require that institutions use such approaches. Should alternative methods for encouraging innovation be considered in lieu of a regulatory Provision?

Question 40: Are there specific further considerations that FinCEN should take into account in the proposed rule related to how financial institutions may use technology and innovation to increase the effectiveness, risk-based nature, and reasonable design of AML/CFT programs?

SIIA has previously recommended that FinCEN amend its AML/CFT regulations to incentivize the adoption of PETs.[5] As we noted, widespread adoption of PETs has not occurred despite advances in PET technology. A key reason for this is the asymmetry between evolving technological capabilities and regulatory frameworks. With the goals of confidentiality and privacy, legal and regulatory regimes explicitly and implicitly prevent uses and transfers of personal and financial information. Yet these regimes create numerous countervailing long term challenges to these very goals. Particularly relevant are barriers created by limitations in the applicable legal and regulatory frameworks. Legal frameworks governing AML/CFT require internal controls, but do not incentivize or require firms to adopt advanced technologies to improve the identification of suspicious activity through data sharing and analysis that would ultimately better protect the privacy and confidentiality of the underlying data.

In line with the proposed rule's intent to enable the private sector to align and incorporate government AML/CFT priorities into their risk management programs, we encourage FinCEN to update its approach to PETs. This includes adopting recommendations on regulatory reform to promote the adoption of PETs in data sharing, analysis, and collaboration to detect suspicious financial activity and improve compliance with domestic, foreign, and international laws.

As demonstrated in a growing literature and pilot projects undertaken globally, PETs have proven effective in the detection, reporting, compliance, and remediation of suspicious financial transactions associated with money laundering (as well as corruption, human trafficking, and other illicit activities). Government authorities have already begun to examine how PETs can help to improve detection of suspicious activity, and PETs will likely show similar promise in the context of financial institutions' AML/CFT programs. The U.S. government has even made this application of PETs a priority, as demonstrated in the Summit for Democracy and the U.S.-U.K. prize challenges on PETs.

Due to its relevance to the goals of the proposed rule, we encourage FinCEN to explore rulemaking to incorporate PETs into the guidelines for data sharing under 31 CFR 1010.520 (information sharing between financial institutions and government agencies) and 31 CFR 1010.540 (voluntary information sharing among financial institutions). These data sharing measures require financial institutions to maintain confidentiality and security of data. Advancements in the PET space can enable financial institutions to do so with greater confidence, increasing the quality of data shared as well as the confidentiality of customer information relevant to that data. We encourage FinCEN to amend these rules to incentivize use of PETs, where feasible, to accelerate their adoption. This would lead to increased data sharing without materially increasing the risk to confidentiality of underlying financial data.

Furthermore, FinCEN regulations govern both AML and customer identification (CID) program requirements for banks and other financial institutions. These program requirements

[5] SIIA Comments on the Request for Information on Advancing Privacy-Enhancing Technologies – August 2022 - SIIA.

differ depending on the type of financial institution. For banks, the relevant rules are contained at 31 CFR 1020.210 (AML) and 31 CFR 1020.220 (CID). As noted above, pilot projects and proofs of concept in the financial services space have demonstrated an increased ability to identify suspicious transactions without revealing confidential information by incorporating different types of PETs. Requiring use of PETs as part of the "system of internal controls" required by the AML and CID rules would create a regulatory driver for banks to adopt PETs and improve their ability to detect financial crime. We would further recommend that use of PETs be incentivized as part of the due diligence program requirements at 31 CFR 1020.610 and 31 CFR 1020.620.

* * *

Thank you for considering our views. We look forward to continued engagement with FinCEN and would be happy to discuss any of these issues further with you, if helpful.