Financial Crime Intelligence and Insight
111 Town Square Place, 14th Floor
Jersey City, New Jersey, 07310 USA

August 29, 2024

VIA Federal E-Rulemaking Portal: http://www.regulations.gov
Docket Number FINCEN-2024-0013
Financial Crimes Enforcement Network
Policy Division
P.O. Box 39
Vienna, VA 22183

RE: Request for Comment on Proposed Amendments to the AML/CFT Program Requirements

To Whom It May Concern:

Financial Crime Intelligence & Insights, Inc. (FCi²)[1] appreciates the opportunity to comment on the Financial Crimes Enforcement Network (FinCEN) Notice of Proposed Rulemaking pursuant to the Anti-Money Laundering Act of 2020 (AML Act) to strengthen and modernize financial institutions' anti-money laundering and countering the financing of terrorism (AML/CFT) programs (the "FinCEN Notice").

FCi² is dedicated to the use of advanced technology to provide insight into potential AML/CFT, fraud, sanctions, and cyber-crime activities through advanced peer-to-peer and public to private information sharing approaches and methodologies. Developed in consultation with law enforcement, FCi² 's work is intended to transform the fight against financial crime from reactive to proactive, exposing illegal activity at a much earlier stage of development, and providing more informed and almost immediate investigative results.

FCi² strongly supports FinCEN's work to modernize and strengthen programs for the prevention and detection of money laundering and terrorist financing which are essential in the fight against financial crime.

Recommendations

As discussed in additional detail below, we commend FinCEN's effort with this proposal to give financial institutions greater ability to focus resources on higher risk areas as identified by their risk assessments and to ensure that government and private sector anti-money laundering and terrorist financing priorities are aligned.

However, we believe the proposed changes do not do enough to encourage innovation or peer-to-peer information sharing. While the proposals will improve AML/CFT efforts by those financial institutions that may

[1] FCi² is a wholly owned subsidiary of the Global Association of Risk Professionals, Inc. (GARP), the world's leading professional organization for risk managers, offering the Financial Risk Manager (FRM)® certification as well as the Sustainability and Climate Risk (SCR)® and Risk and AI (RAI)™ certificates globally. GARP also sponsors the GARP Benchmarking Initiative (GBI) which provides analysis and confidential reporting for over 100 financial institutions around the world on bank capital and other financial industry studies. FCi² was established in the United States to provide a secure automated information sharing hub for participating financial institutions to proactively identify and fight financial crime.

not presently conduct risk assessments or appropriately incorporate FinCEN priorities into their AML/CFT programs, it is only addressing what is occurring within the financial institution itself. Financial crime takes place across organizations and geographies. Without attaining a wider field of view, illicit actors will continue to be able to use the financial system to conceal and fund criminal activities by scattering accounts and transactions among financial institutions and relying on their current lack of information sharing.

Financial institutions can share information with other financial institutions on suspected money laundering or terrorist financing activities under the safe harbor provided by Section 314(b) of the USA PATRIOT Act. Unfortunately, many financial institutions are not availing themselves of the safe harbor or are not fully sharing information even though it leads to a more complete analysis about the activity or actor, better SAR filings, and better risk management.

There are a number of reasons financial institutions do not share information, but a primary rationale is that information sharing under Section 314(b) is voluntary, and there are no current regulatory incentives to either compel or encourage broad-based information sharing.

The voluntariness of the current AML/CFT regime results in uneven participation, slow and potentially incomplete information sharing and suboptimal use. This, together with the lack of regulatory incentives "encouraging" financial institutions to readily and efficiently share information with other financial institutions to detect and prevent financial crime, has enabled bad actors to take advantage of the siloed view of financial institutions and for financial crime to proliferate.

There are also differing views on the scope of information that can appropriately be shared under the regulation. For example, the reluctance of some financial institutions to allow for the sharing of suspected fraud because they are unsure whether fraud falls within the information sharing safe harbor inhibits, or chills information flows.[2] As a result, financial institutions requesting information do not know what type of, or if any response will be received.

The combination of all the above factors can lead to, among other things, delays in AML investigations and SARs filings that only reflect part of the picture.

Financial institutions that choose to respond to requests for information from other financial institutions take on additional risk, and additional workloads. Because they may be alerted to an issue they were previously unaware of, they are now required to look into the activity and determine whether to take action. They then may face regulatory scrutiny with respect to those actions or inaction, without receiving any "credit" for participating in the information sharing effort.

The changes proposed in the request for comment are essential and should be welcomed by all. However, we respectfully recommend that thought be given to improving the financial crime information sharing regime in

[2] The FinCEN Section 314(b) Fact Sheet (December 2020) www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf The Section 314(b) Fact Sheet provides specific guidance relating to the activities financial institutions may share under the 314(b) safe harbor, including the specified unlawful activities ("SUAs") listed in 18 USC §1956 that are predicate crimes applicable to money laundering. Despite the fact that the Fact Sheet specifically indicates that fraudulent activities, including fraud against individuals, organizations, or governments, computer fraud and abuse, and other crimes are included in those covered by the safe harbor, the guidance is not legally binding, and therefore some financial institutions are unwilling or unable to rely on it.

its entirety, taking into consideration technological advances and innovations in privacy enhancing technologies, machine learning and artificial intelligence that allow for the fast, secure data sharing and analysis necessary to enable a strong, effective, modernized approach to fighting money laundering and terrorist financing. As bad actors become more sophisticated in their use of technology and better at leveraging the siloed views of financial institutions, we must do more to shrink their advantage by incentivizing innovation, facilitating the adoption of new technology, and promoting information sharing.

Specific Responses to Questions Presented

Question 5.

We believe that a risk assessment is a necessary element in establishing an effective AML/CFT program. However, to successfully identify, manage and mitigate illicit finance activity risks a financial institution should also maintain an awareness of activities outside of its organization.

One way to do this is to incorporate the AML/CFT priorities into its risk assessment process, as FinCEN is proposing. However, additionally, we believe that for any program to be effective, it must also require the sharing of, or accessing, even in some cases real time, information on an activity or persons creating a suspicion of money laundering or terrorist financing.

Because financial crime occurs across financial institutions it is often hard to identify or proactively address illicit activity at an early stage. Section 314(b) provides financial institutions with an invaluable tool for viewing a broadscale of activity and gaining insight into suspicious activities taking place through multiple financial institutions. Therefore, along with the distribution of the AML/CFT priorities, it should be made clear that any activities listed in those priorities are permitted to be shared in accordance with Section 314(b). FinCEN should be clear that best practices for identifying and mitigating financial crime includes information sharing.

Question 12.

We agree that the BSA reports filed by financial institutions pursuant to 31 CFR Chapter X, especially SARs reports, contain important information that should be assessed, analyzed and carefully reviewed. However, we believe this review would be more effective if it was done with respect to all SARs filings, an undertaking that now, given technology, including artificial learning methodologies, can be readily done. That way connections could be made between actors or activities that could not be identified by viewing the activities taking place at one financial institution. Once analyzed, that information should be made available to financial institutions frequently, or even in real-time, utilizing technology to its fullest.

We also agree that if financial institutions are seeing the same threat patterns, they should affirmatively consider whether adjustments to their internal policies, procedures and internal controls should be made.

In addition, it would be useful to track SAR filings that lead to subpoenas. We do not believe, however, that a review by a financial institution of its own BSA reports will be sufficient to materially minimize defensive SARs filings.

It is our understanding, from our many conversations with professionals representing numerous and varied financial institutions, that reducing the number of non-useful SARs is something all of them would relish. SARs filings require a lot of time, effort, and resources, from conducting the investigation, gaining internal insights

and management input, to drafting the report. There is a sense that many are filed and never reviewed. Most financial institutions have a strong desire to know whether their filing was helpful and whether they truly identified a bad actor or illicit activity and provided adequate support information. However, unless they receive a subpoena from law enforcement, they have virtually no information whatsoever to act on or use to assess the quality or value of their reports, including whether the activity was truly illicit or part of a broader scheme.

We recommend a more robust system of review and feedback on BSA reports be developed and implemented so that financial institutions can better calibrate their transaction monitoring systems and improve their reporting procedures.

Questions 14 and 18.

Question 14 asks how often a financial institution's risk assessment should be undertaken and Question 18 asks how a financial institution would demonstrate that its AML/CFT program is effective, risk based and reasonably designed. We have chosen to respond to these questions together because they are interrelated.

Often, regulations promulgated with the best intentions result in check-the-box exercises that lose sight of the underlying purpose. We understand the purpose of this proposed provision to be the development of a program that detects, manages, and mitigates illicit financing risks effectively and efficiently, with greater focus directed towards higher risks and produces reports that are useful to law enforcement. The frequency of the risk assessment process should directly relate to the effectiveness of the program.

While good "hygiene" necessitates reviewing policies and procedures regularly, this function should be assessed in terms of good compliance and not specified in this proposed rule which would likely lead to the assessment becoming a check the box function. Instead, we suggest that FinCEN place more emphasis on whether the purpose of the rule is being fulfilled.

This proposal refers to a June 2019 Senate Banking hearing summarizing the results of an empirical study of 19 financial institutions which found that they employed 14,000 individuals, spent $2.4 billion, and used more than 20 different technology systems in their AML/CFT compliance programs. The same study found that 17 financial institutions reviewed 16 million AML alerts identified by their transaction monitoring systems and filed over 633,000 SARs, with an aggregate conversion rate of 4%.[3] We assume, based on feedback from financial institutions regarding SARs filings, out of that 4%, a significant portion could be considered defensive SARs, meaning that an even smaller percentage of those filings are of value to law enforcement.

The amount of resources being spent by financial institutions should also be considered when assessing the current financial crime regimes' impact. A recent reporting in the *Wall Street Journal* stated that over $480 billion was lost to bank fraud schemes globally in 2023 as The United Nations Office on Drugs and Crime report cited by the *Wall Street Journal* said that approximately $2 trillion or 2% to 5% of global gross domestic product is laundered annually. It is estimated that in 2024, globally, financial institutions spent approximately $230 billion on financial crime compliance and fraud prevention technology and operations.[4] An objective

[3] See footnotes 36 and 61 of the Financial Crimes Enforcement Network (FinCEN) Notice of Proposed Rulemaking pursuant to the Anti-Money Laundering Act of 2020 (AML Act). *Federal Register Vol. 89, No. 128 (July 3, 2024) 55428 at 55431 and 55434.*

[4] Telis Demos, "Fighting Financial Crime Could Pay for Nasdaq", *Wall Street Journal,* Aug 28, 2024. https://www.wsj.com/finance/stocks/fighting-financial-crime-could-pay-for-nasdaq-704c165e

assessment of these statistics alone, leads to the conclusion that what is currently being done with great effort and at great expense to fight and deter financial crime, is not as effective as intended. The growing gap between illicit activities and the ability to deter and detect it points to an acute need to make changes. In that regard, we recommend greater collaboration between law enforcement, regulators, and financial institutions, better more secure information sharing mechanisms, and more encouragement with regulatory incentives for the testing and implementation of new approaches and solutions for fighting financial crime.

Risk assessments are useful tools, but they result only in an educated guess on behalf of the financial institution about where to dedicate its attention. It may be more effective to shift the focus and a significant portion of the resources of financial institutions towards the priorities of law enforcement, effectively and efficiently collaborating in their efforts. Allocating resources toward law enforcement priorities may also result in a significant reduction of SARs filings, eliminating a material number of defensive and non-relevant filings.

Financial institutions must now engage in activities that are more properly within law enforcement's areas of expertise. They are being asked to determine whether an activity may be sufficiently problematic under the law (e.g., a suspicious activity) to require a SAR filing. Law enforcement has the expertise for these determinations, financial institutions activities should be directed toward providing supporting information based on law enforcement's priorities and advice. This shift, coupled with regulatory incentives and a move away from a check-the-box approach to assessing the effectiveness of an adequate internal financial crime fighting apparatus, would result in a more proactive and flexible approach to fighting financial crime.

Question 25.

We commend FinCEN's consideration of new approaches for soliciting and providing feedback from law enforcement about useful BSA reports submitted by financial institutions. We would also recommend several changes, especially with respect to SAR filings.

First, a notice to the financial institution that the SAR was received could assure the institution that it was properly filed. Second, in situations where it would not jeopardize an investigation, law enforcement could allow a notification to be sent to a financial institution when a SAR is being reviewed. Finally, law enforcement could provide feedback on those SARs that are missing information, hard to understand, or are clearly defensive, if a secure and easy to use mechanism for doing so was available. Given the vast amount of data being submitted daily, using artificial intelligence and other advanced technological tools should be prioritized with the objectives of discerning trends, identifying changing typologies, and providing an advanced and real-time information sharing mechanism to inform financial institutions and law enforcement. Too often both operate in an information vacuum when the tools and capabilities for more informed information flows exist and are permissible under current regulation.

Questions 38, 39 and 40.

We agree that innovative approaches should be permitted to help financial institutions more effectively comply with the BSA and fight financial crime. Considering the statistics noted in our response to Questions 14 and 18 above, we urge FinCEN to fully support innovation, flexibility and the use of technology to its fullest. The fight against financial crime requires collaboration between FinCEN, regulators, law enforcement, fintech, and financial institutions. We commend FinCEN's use of notices and other outreach efforts to communicate information to financial institutions. We would advocate for continued collaboration and a greater focus on

opportunities to encourage financial institutions to evaluate new innovations. This will require regulators to provide incentives and allow for trial-and-error approaches without penalties, FinCEN to provide guidance to financial institutions, and a willingness by law enforcement to provide appropriate feedback to financial institutions. Fighting financial crime is a shared interest and requires cooperation and coordination.

We also recommend that when considering innovative measures to fight financial crime, additional scrutiny be given so that any adopted approach avoids the unintended consequence of creating more siloes. When viewed holistically, information sharing is essential to the detection and prevention of financial crime and should be a component of any innovation incorporated into an AML/CFT program.

It is our general understanding that financial institutions are hesitant to consider investing in and adopting new technology to fight financial crime for a variety of reasons, including, among other things, resource allocation, risk averseness, fear of regulatory scrutiny, or lack of incentives.

Every financial institution we've spoken with has stated unequivocally they want to better detect, mitigate, and prevent financial crime. And they have invested a lot of time and money trying. However, doing more of the same without addressing the basic underlying issues of cooperation, information flows and incentives, will not reduce the expanding gap between illicit activities and the financial services industry's ability to respond. There must be a transition into a more proactive and collaborative effort utilizing advanced technology to fight financial crime. Regulators, and law enforcement, are immensely important to this transition. In coordination with the financial services industry, regulators and law enforcement need to affirmatively "encourage" innovation, quickly share more information, and commit to using new technology. Innovation must be viewed positively in audit and regulatory findings and regarded as a valuable customer protection measure.

Conclusion

FCi^2 appreciates the opportunity to provide this response to FinCEN's Notice of Proposed Rulemaking and Request for Comment on Proposed Amendments to the AML/CFT Program Requirements. We understand the difficulty in drafting rules to protect the financial system from being used as a tool to further criminal activity, especially when financial criminals are becoming more and more sophisticated every day.

We believe the best way to combat financial crime is through the smart use of technology, with flexibility, and scalability, which provides for the quick exchange and analysis of information in a secure and transparent way. Allowing financial institutions to alert each other about suspicious activity, using as much of a flow-through information sharing system as possible, with automated learnings derived from SAR analysis and law enforcement input, will arm financial institutions and law enforcement with more complete information. The ability to share and collaborate quickly is an important tool in detecting criminal activity, protecting customers from fraud, and the banking system from abuse.

Respectfully submitted,

/s/Richard Apostolik
_____
Richard Apostolik
President & CEO
Rich.Apostolik@fci2.com

/s/Rachel Lerner
_____
Rachel Lerner
General Counsel
Rachel.Lerner@fci2.com