INDEPENDENT COMMUNITY BANKERS of AMERICA®

Robert M. Fisher, *Chairman*
Brad M. Bolton, *Chairman-Elect*
Gregory S. Deckard, *Treasurer*
Tim R. Aiken, *Secretary*
Noah W. Wilcox, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

February 14, 2022

Via Electronic Submission

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

RE: Docket Number FINCEN–2021–0008 - Review of Bank Secrecy Act Regulations and Guidance

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] appreciates the opportunity to respond to the Financial Crimes Enforcement Network's ("FinCEN's") Request for Information ("RFI") to solicit comments on ways to streamline, modernize, and update the anti-money laundering and countering the financing of terrorism ("AML/CFT") regime of the United States. This RFI also supports FinCEN's ongoing formal review of Bank Secrecy Act ("BSA") regulations and guidance required by Section 6216 of the Anti-Money Laundering Act of 2020 ("the AML Act"), enacted into law as part of the National Defense Authorization Act for Fiscal Year 2021 ("NDAA").[2]

[1] *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

With nearly 50,000 locations nationwide, community banks constitute roughly 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding nearly $5.9 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org

[2] 31 U.S.C. § 5336.

Background

Section 6216 of the AML Act requires FinCEN to undergo a formal review to ensure that BSA regulations and guidance continue to safeguard the U.S. financial system from threats by various forms of financial crime, and that reporting and recordkeeping requirements continue to be highly useful. The review is intended to help FinCEN identify regulations and guidance that are not useful, outdated, redundant, or do not promote a risk-based AML/CFT compliance regime for financial institutions. In consultation with specified stakeholders, FinCEN will make appropriate changes to regulations and guidance to improve their efficiency. In addition, the formal review will assist FinCEN in identifying recommendations for administrative and legislative changes.

Executive Summary

In today's rapidly ever-changing world, it is imperative that financial institutions ("FIs") and law enforcement work together to combat and prevent financial crime, money laundering, and terrorist financing. Community bankers are committed to supporting balanced, effective measures that will prevent the financial system from being used to fund criminal activities and prevent money launderers from hiding the proceeds of criminal activities. However, anti-money laundering, combatting the financing of terrorism, and BSA programs have increasingly charged community banks with complying with outdated, inefficient, and redundant requirements that consume a growing share of community banks' scarce resources.

Since the inception of anti-money laundering laws in 1970 and anti-terrorist financing laws in 2001, the burdens placed on FIs increasingly create an environment where FIs are essentially tasked with identifying, investigating, policing, stopping, and reporting potential criminal activity. Each year, community banks must invest more time, money, and resources to combat this threat. Yet, the current outdated framework is more of a robotic exercise of submitting forms, maintaining records, and responding to examination demands. This outdated framework is not only ineffective, but also diminishes community banks' ability to attract capital, support the financial needs of their customers, and contribute to their local economies as many do not have dedicated legal and compliance departments focused on BSA.

Modernization and reform of the BSA will produce more useful information for law enforcement while alleviating one of the most significant and costly sources of community bank compliance burdens. Rather than having banks devote their resources to tasks that are inefficient or redundant, a more efficient and technologically advanced framework would better serve law enforcement and enable community banks to utilize their resources more effectively. BSA modernization will allow FIs to deploy compliance resources more efficiently and will render more useful information to law enforcement.

ICBA has called for BSA modernization for many years. This RFI, the subsequent report to Treasury, and potential rulemaking is an opportunity for FinCEN to heed the input of FIs, specifically community banks, and work diligently to improve the current AML/CFT regime. In

response to this RFI, ICBA urges FinCEN to take the following actions to streamline, modernize, and update the AML/CFT regime:

- Undertake a holistic review of financial crime taking place outside of the traditional banking system;
- Increase reporting requirement thresholds for suspicious activity reports ("SARs") and currency transaction reports ("CTRs");
- Withdraw beneficial ownership collection and verification requirement from banks but allow them to rely on their risk-based monitoring procedures;
- Abandoned plans to decrease the current record-keeping and Travel Rule thresholds;
- Provide flexibility for FIs to deploy resources to areas that impact their specific institution;
- Issue frequent reports that inform FIs on local, regional, and national trends, financial crime patterns, and threats; and
- Provide more robust assurances for the use of new technologies.

ICBA Comments

Emerging Financial Crime Threats, Vulnerabilities, or Risks

The RFI seeks input on threats, vulnerabilities, or risks that the Treasury may be unaware of or is not responding to with sufficient and appropriate safeguards. FIs are on the front lines defending against all matters of financial crime threats. They take their role in protecting customers, their respective institutions, and securing data and personal information very seriously. This role also gives them insight into threats and patterns afoot, and on the horizon.

An area of significant concern for community banks pertains to entities that are not subject to BSA regulations and other non-regulated entities. ICBA urges FinCEN to undertake a holistic review of financial crime that includes a focus on non-bank entities that handle or have access to financial data and personally identifiable information. This can take the form of unregulated companies and financial technology companies ("fintechs") that employ screen scraping technologies to harvest a customer's information, or non-bank companies that require the customer's banking login credentials to use their service. The financial sector is an eco-system and when banking and customer information is accessed by non-bank or unregulated entities, it puts the customer's data at risk and opens the door to financial criminals.

Retailers, technology companies, and other parties that process or store consumer financial data are not subject to the same federal data security standards and oversight as FIs. Subjecting FIs to the most strenuous requirements for securing and monitoring data is of limited value if it remains exposed at the point-of-sale and other processing points. To effectively protect customer data from criminal access, all participants in the payments system, and all entities with access to customer

financial information, should be subject to the monitoring and reporting requirements under the BSA.

Community banks significantly rely on third party technology and service providers to support their systems and business activities. While community banks are diligent in their management of third parties, mitigating sophisticated cyber threats against them can be challenging, especially when they have connections to other institutions and servicers. FinCEN must be aware of the significant interconnectivity of these third parties and collaborate with them to mitigate financial crime risk. FinCEN should evaluate the concentration risk of service providers to FIs to understand the depth of BSA/AML exposure and areas of vulnerability.

Reporting or Recordkeeping Requirements

Suspicious Activity Reports

Suspicious activity reporting ("SARs") is the cornerstone of the BSA system and was established as a way for banks to provide leads to law enforcement. Because community banks have a strong incentive to file SARs as a defensive measure to protect themselves from examiner criticism, SARs are filed in increasing and vast numbers without a commensurate benefit to law enforcement. As the government combats money laundering and terrorist financing, ICBA strongly recommends an emphasis on quality over quantity when filing SARs. ICBA recommends reforming the SAR process by increasing the reporting thresholds, which have not been adjusted since becoming effective in 1992, and by emphasizing those instances in which an institution may rely on risk-based reporting.

In the current regulatory environment, community banks undertake a cumbersome process to ensure they are protected, and no mistakes are made in preparation for examiner review. For each transaction the bank identifies as suspicious, a thorough investigation is conducted that typically includes monitoring and reviewing all documentation and account activity, interviewing appropriate personnel, a review of the investigation by a BSA-trained employee, and sometimes a second review by either a compliance or BSA committee, BSA officer, or senior level staff. The investigation is documented, with documents retained on transactions for which a SAR is filed, as well as for investigations for which a SAR is not filed. If a SAR is not filed, banks must document and subsequently justify to their examiner why a flagged transaction did not result in a filed SAR. This is done for every suspicious transaction no matter how minor or severe the potential offense. The process is time consuming, and labor intensive and community banks are skeptical that the method by which SARs are completed provides commensurate value to law enforcement.

Notwithstanding this arduous process, FIs are questioned on the number of SARs filed in relation to the number of accounts and transactions initially identified as suspicious rather than the quality of the bank's monitoring system or investigative process. Additionally, bankers are questioned on the total number of SARs filed since the last examination as though a quota is required. As a result, bank employees often file SARs as a defensive measure. The current focus

is also a daunting task for community banks because it usurps resources by requiring significant time monitoring for thresholds (quantity) and less time focused on actual suspicions (risk).

SAR Thresholds
The archaic and labor-intensive nature of the SAR process makes the SAR regime ineffective and cumbersome. As stated previously, community banks follow the same SAR procedure for every suspicious transaction no matter how minor the potential offense. This approach leaves community banks skeptical that SARs have real value to law enforcement. As such, ICBA recommends the current SAR threshold should be raised from $5,000 to $10,000, which will modernize thresholds by emphasizing quality over quantity and enable community banks to provide more targeted and valuable information to law enforcement.

There is a lack of visibility into the thresholds that trigger FinCEN or law enforcement to investigate a financial crime. SARs and even direct contact to law enforcement often go unanswered. Banks have ample examples of fraud and other financial crimes where even after they filed a SAR, continued to file SARs on a specific matter, and contacted law enforcement, there was no follow-up. This leaves community banks with a sense that reporting potential or actual financial crimes that are unanswered is a waste. Essentially law enforcement does not investigate fraud until the dollar amount is high enough to warrant the attention of law enforcement agents. Along with providing some sense of progress on investigations, it would be helpful if the triggers that would initiate an investigation were known to community banks so that they could incorporate that into their risk-based approach. It is unnecessary and ineffective to put the burden on community banks to collect this information if no action is taken, or justice is not provided to victims.

Currency Transaction Reports
Reporting thresholds are significantly outdated and capture far more legitimate transactions than originally intended. The currency transaction report ("CTR") threshold, set in 1970, should be raised from $10,000 to $30,000 with future increases linked to inflation.

CTRs are intended to collect information for investigations into tax evasion, money laundering, terrorist financing and other financial crimes. However, the overwhelming percentage of CTRs relate to ordinary business transactions, which create an enormous burden on FIs that is not commensurate with financial crime investigations. While the BSA provides banks with the ability to exempt certain customers from CTR reporting, a higher threshold would produce more targeted, useful information for law enforcement.

Beneficial Ownership Rule
The CTA amended the BSA by imposing new beneficial ownership requirements and calling for the creation of a FinCEN registry. The CTA requires FinCEN to issue rules mandating reporting

companies to submit certain information to FinCEN about their beneficial owners;[3] requires FinCEN to maintain this information in a confidential, secure, and non-public database;[4] and authorizes FinCEN to disclose the information to FIs to facilitate compliance with customer due diligence ("CDD") requirements.[5] The CTA also provides for the issuance and use of identifiers assigned by FinCEN that persons may submit to FIs to satisfy certain beneficial ownership reporting requirements.[6] The CTA requires the promulgation of regulations prescribing procedures and standards for beneficial ownership reporting and FinCEN identifiers by January 1, 2022. The CTA also requires the Treasury to revise its existing CDD rules to reduce any burdens on FIs and legal entity customers that are unnecessary or duplicative.[7]

Because FinCEN is mandated to collect beneficial ownership information ("BOI") directly from reporting companies, ICBA strongly urges FinCEN to withdraw its requirement that banks also collect BOI and rely instead on their risk-based monitoring procedures. From the onset of the CDD rule's development, ICBA's position has been and continues to be that if the government has an interest in collecting and maintaining records of beneficial owners of private legal entities, such information should be collected and verified at the time a legal entity is formed, rather than requiring FIs to collect this information.

According to FinCEN, entities are at times used to obfuscate ownership interests and used to engage in illegal activities such as money laundering, corruption, fraud, terrorist financing, and sanctions evasion. Criminals have exploited the anonymity that legal entity ownership can provide to engage in a variety of crimes, and often take advantage of shell and front companies to conduct such activity. Making legal entities more transparent by requiring identifying information of natural person owners would likely hinder such abuses. However, placing the responsibility and oversight of collecting this information to the private sector, specifically FIs, is misguided and ineffective.

The CTA requires Treasury to ensure its new CDD rules reduce burdens on FIs. Requiring both FinCEN and FIs to collect the same information on the same entities is ineffective, duplicative, unnecessary, costly, and highly useless. This exercise is also extremely burdensome to both legal entities and banks because the onerous task of confirming BOI has already taken place and is on file. To do so each time a new account is opened adds no benefit whatsoever to law enforcement.

The drafters of the CTA mandated the Secretary of the Treasury to revise the final CDD rule to **"**reduce any burdens on FIs and legal entity customers that are, in light of the enactment of this division and the amendments made by this division, unnecessary or duplicative."[8] ICBA strongly urges FinCEN to execute its directive from Congress by withdrawing the requirement that

[3] CTA § 6403 (b)(1)(C)
[4] CTA § 6402(7)
[5] CTA § 6403(b)(1)
[6] CTA § 6403 (b)(3)
[7] CTA § 6403 (d)(1)(C)
[8] Ibid

regardless of risk, legal entities provide to FIs, and FIs collect BOI, as we believe it is the only way to best implement the CTA and will reflect this current modernization effort.

Record-Keeping and Travel Rule

Under BSA rules, banks must collect and retain information on certain funds transfers and transmittals of funds ("recordkeeping rule")[9] as well as include certain information on funds transfers and transmittals of funds sent to other banks or nonbank financial institutions ("travel rule").[10] The current threshold for both rules is $3,000. In December 2020, FinCEN and the Federal Reserve Board (collectively, the "Agencies") issued a joint notice of proposed rulemaking to decrease both the recordkeeping and travel rule (collectively, "the rules") thresholds to $250. ICBA opposes a threshold decrease.

While community banks are eager to do their part to protect the U.S. financial system pursuant to the BSA, the cumulative impact of these regulations places a burden on community banks that is often disproportionate to the benefits of any additional regulatory requirements. Decreasing the threshold from $3,000 to $250 will deepen the cumulative impact. The impact includes the cost for new technologies needed to comply, additional personnel and time to collect information, costs associated with creating new or adjusting processes, and costs associated with retention and transmission. The ripple effect of this change will make payment services less affordable for those legitimately transferring smaller dollar amounts abroad.

Additionally, lowering the threshold will be counterproductive. The Agencies cite a benefit to national security and law enforcement[11] as justification for lowering the threshold. The proposal states that "malign actors are using smaller-value cross-border wire transfers to facilitate or commit terrorist financing, narcotics trafficking, and other illicit activity, and that increased recordkeeping and reporting concerning these transactions would be valuable to law enforcement and national security authorities."[12] However, criminals find new ways to avoid detection, such as conducting transactions underground, in order to achieve unlawful goals. Their ability to outmaneuver detection-related regulations makes it difficult to track the activity, and yet banks are left saddled with the additional burdens. Piling on additional BSA obligations, by decreasing the threshold, reinforces the notion that banks are effectively deputized to identify, investigate, and report on criminal activity, and maintain records that may never be requested. The Agencies' belief that "there has been an increase in the ability of small institutions to rely on third-party vendors to reduce their costs of handling compliance with a revised threshold"[13] is an assumption that does not always bear out because reliance on vendors comes with additional costs. Additionally, institutions remain obligated for the vendors' oversights. A significant swath of small community banks continues to rely on manual in-house processes because of their limited

[9] 31 CFR 1020.410(a)
[10] 31 CFR 1010.410(f)
[11] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201023a.pdf p.8-9
[12] Ibid
[13] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201023a.pdf p.16

resources. ICBA is a staunch advocate for efficient regulatory requirements that effectively support law enforcement. This is why we oppose this threshold decrease.

Changes to BSA Regulations and Guidance to Improve Efficiency

Flexibility

Section 6216 of the Act requires FinCEN to make changes to regulations and guidance to improve the efficiency of those provisions. Allowing FIs to deploy resources to areas that impact their specific institutions (while not ignoring national priorities) will improve efficiency. BSA requirements should be flexible and easily applied. ICBA firmly believes that an effective and efficient AML program would provide FIs with greater flexibility to reallocate resources away from practices that are not required by law or regulation, that are mechanical, defensive and "check-the-box," in nature, that respond to examiner demand, and render little to a FI's overall risk management objective. Freeing up these resources away from activities that are low priority and reallocating them to address areas of higher risk priorities within an institution's risk determination is the surest way to achieve an effective and efficient AML program.

Future rulemaking should not only consider this notion of reallocation for FIs but must also make clear that examiners should conduct examinations pursuant to those reallocated resources, and not penalize a FI's decision to refocus their AML priorities.

Effective and Targeted Communication

Communication and cooperation are critical to an effective working partnership among the government, law enforcement, and FIs. Community banks seek most recent information from the federal government to better understand what specific methods of terrorist financing and money laundering they are helping to mitigate. This enables FIs to more readily identify and report truly suspicious transactions. To improve efficiency, ICBA recommends that FinCEN provide secure monthly or quarterly reports that inform on local, regional and national trends, financial crime patterns, and threats. Faster and more proactive releases of information will provide an option for FIs to align or reallocate resources more effectively and allow them to identify truly suspicious transactions and provide more useful information to law enforcement. Creating reports might be time consuming for FinCEN, but that amount of time would then be saved across 5,000 banks while also providing FinCEN with a mechanism to highlight patterns that it feels are important for financial crime reporting.

Updating or Amending Regulatory Processes

Other ways FinCEN can improve efficiency is by:

- Streamlining the online SAR form such that -
  - certain fields could auto or pre-populate; and
  - information from previous SARs could be added to new and similar SARs without significant report building required;
- Updating SAR and CTR thresholds;

- Expanding CTR exemptions;
- Improving the BSA E-Filing System by working with a company with specific expertise in enhancing data entry automation and simplifying user interfaces.
- Creating an EZ SAR form that reduces the amount of data that needs to be collected for smaller offenses and when suspicious activity thresholds are not met;
- Eliminating the requirement to file SARs every 90 days but encourage a risk-based approach for decisions to continue filing; and decreasing or removing the narrative section;
- Updating the *Suspicious Activity Information* section on the SAR form based on both national and international financial crime trends to enable FIs to get the basic information to those reviewing the report more quickly and prior to reading the narrative section;
- Revising the 314(a) process by posting lists on a monthly basis versus every two weeks; and
- Communicating measurements for what will trigger a financial crime investigation.

Innovation

The RFI seeks information on whether BSA regulations or guidance should account for technological advancements and whether regulations and guidance sufficiently allow FIs to incorporate innovative and technological approaches to BSA compliance. ICBA supports balanced and flexible regulations that facilitate bank exploration of new technologies. ICBA firmly believes that BSA guidance should account for new technologies and offer guidance to FIs using them. However, ICBA does not support regulations that would require such use.

On December 3, 2018, FinCEN and the federal banking agencies issued a joint statement (the "Joint Statement") encouraging banks to consider, evaluate and implement innovative approaches to meeting their BSA/AML compliance obligations, including by deploying emerging technologies to identify and address vulnerabilities and threats.[14] The effort is intended to foster innovation without fear of criticism and includes exceptive relief, upon request, to the extent necessary to facilitate the development of new technologies and other innovations. Yet, four years after the release of the Joint Statement, many community banks have not been comfortable enough to take advantage of the gesture.

As technologies and innovation continue to evolve, many FIs lack the comfort level needed to implement and utilize these technologies. Community banks have expressed that their hesitancy stems from concern that regulators and examiners do not allow FIs the space to experiment and make errors when utilizing these technologies, their use will result in exam criticisms and findings, and regulations impede their ability to implement new technologies.

[14] The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration and the Office of the Comptroller of the Currency ("OCC") (together, the "Agencies") issued a Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018).

Conclusion

ICBA appreciates the opportunity to provide comments in response to this request. If you have any questions, please do not hesitate to contact me at Rhonda.Thomas-Whitley@icba.org or (202) 821-4451.

Sincerely,

/s/

Rhonda Thomas-Whitley
Vice President and Regulatory Counsel