Statement by

Himamauli Das

Acting Director

Financial Crimes Enforcement Network

United States Department of the Treasury

before the

Committee on Financial Services

U.S. House of Representatives

April 28, 2022

Good morning. My name is Him Das, and I am the Acting Director of the Financial Crimes Enforcement Network (FinCEN). Chairwoman Waters, Ranking Member McHenry, and distinguished Members of the Committee. Thank you for the invitation to appear before you today to provide an update on FinCEN's implementation of the Anti-Money Laundering Act of 2020 (AML Act), including the Corporate Transparency Act (CTA). This morning, I hope to demonstrate the value FinCEN adds to the nation's regulatory, law enforcement, and national security infrastructure, and the critical role it has played, and continues to play, in transforming our nation's anti-money laundering (AML) regime from post-9/11 to post-pandemic; from al-Qaida to artificial intelligence and digital assets.

Until recently, the overarching legal foundation of the U.S. anti-money laundering/combating the financing of terrorism (AML/CFT) regime reflected the post-9/11 moment. Just as earlier iterations of the Bank Secrecy Act (BSA) were focused on countering the dominant policy concerns of their times—such as combating drug-related financial flows—the updates made to the BSA by the USA PATRIOT Act after 9/11 emphasized disrupting the money flows of terrorist organizations such as al-Qaida through the traditional banking system.

The AML Act has helped put FinCEN in the position to address today's challenges, such as illicit use of digital assets, corruption, and kleptocrats hiding their ill-gotten gains in the U.S. financial system, including through American shell companies and real estate. It also highlights FinCEN's unique tools and expertise to combat both longstanding threats, as well as new ones, such as ransomware and other cyber-enabled threats and the use of the dark web to engage in illicit activity, such as the online exploitation of children.

The AML Act also provides tools to approach innovations in a way that recognizes not only the opportunities they present, but the risks that they pose. One of the purposes of the AML Act is to encourage technological innovation and the adoption of new technology by financial institutions to make the AML/CFT framework more effective. And, it directs FinCEN to "streamline, modernize, and update the AML/CFT regime of the United States." It also placed by statute national security front and center in FinCEN's mandate.

Current events often make clear the importance of an AML/CFT framework that is well designed and effective in preventing bad actors from exploiting the financial system. As the pandemic began to unfold in 2020, FinCEN pivoted its efforts to focus on the effects COVID-19 was having on a range of illicit finance threats around the world. FinCEN issued guidance, advisories, and information about trends and red flags to provide feedback to financial institutions on COVID-19 medical fraud, imposter scams, cyber-enabled crime, and the defrauding of the unemployment insurance system. FinCEN also assisted law enforcement and financial institutions in the recovery of funds stolen via fraud and other COVID-19 related crimes.

In 2021, FinCEN placed a spotlight on ransomware—a scourge that continues to affect schools, hospitals, the U.S. energy grid and oil supplies, and large and small companies around the United States. In October 2021, FinCEN published its first Financial Trends Analysis (FTA) as required

by section 6206 of the AML Act. This report shared with the public ransomware trends and typologies gleaned from financial intelligence provided to FinCEN by financial institutions.[1] FinCEN also published an advisory and hosted a FinCEN Exchange, as required by section 6103 of the AML Act, on ransomware to alert financial institutions to red flags associated with the crime. FinCEN continues to work closely with law enforcement and develops investigative tips and leads based on suspicious activity reporting and blockchain analysis.

Now, the ongoing situation in Ukraine places a renewed spotlight on the importance of an effective AML/CFT regime in providing key insights and information to law enforcement and national security agencies.

Ongoing Situation in Russia/Ukraine

Since the further invasion of Ukraine began, the United States and our international partners have imposed unprecedented financial pressure on the Russian Federation and its leadership. FinCEN is bringing all BSA authorities to bear in support of U.S. government efforts and multilateral efforts. FinCEN has issued two Russia-related alerts to provide financial institutions with information about typologies and red flags. The first alert focused on sanctions evasion,[2] and the second highlighted channels through which oligarchs hide and launder corrupt proceeds.[3] These channels include shell companies, real estate, and the purchase of luxury goods and high-end art.

Additionally, FinCEN is continuing robust engagement with financial institutions through its public-private partnership FinCEN Exchange program, to explore typologies and share best practices. These exchanges enable the private sector to better identify corrupt proceeds of elites, oligarchs, and their proxies, and provide FinCEN and law enforcement with critical information to track, freeze, and seize their assets. We are sifting through suspicious activity and other reports filed by financial institutions to trace beneficial owners of shell companies established by oligarchs, locate hidden assets, and uncover efforts to evade sanctions.

Finally, on March 16, 2022, FinCEN led the effort by the financial intelligence units (FIUs) of Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, the United Kingdom, and the United States in issuing a statement of intent to form an FIU Working Group on Russia-Related Illicit Finance and Sanctions.[4] The FIUs affirmed the need to identify

---

[1] *See* FinCEN, "FinCEN Issues Report on Ransomware Trends in Bank Secrecy Act Data," https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data

[2] *See* FinCEN, "FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts," (March 7, 2022), https://www.fincen.gov/index.php/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions

[3] *See* FinCEN, "Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members," (March 16, 2022), https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Elites%20High%20Value%20Assets_508%20FINAL.pdf

[4] *See* Financial Intelligence Units of Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, the United Kingdom, and the United States, "Russia-Related Illicit Finance and Sanctions FIU Working

concrete actions that Working Group members can take to enhance financial intelligence on sanctions-related matters; expedite and increase sharing of financial intelligence in sanctions-related matters; discuss FIU best practices, and lessons learned, and identify opportunities for actions and partnerships to combat the threat caused by Russia's unprovoked invasion of Ukraine. The Working Group will also strengthen and facilitate working relationships among FIUs, appropriate public authorities and the private sector addressing that threat, including by engaging with the international Russian Elites, Proxies, and Oligarchs Task Force.

Targeting Corruption

The ongoing tragic events in Ukraine underscore the urgent need to provide transparency to combat corruption. The Biden Administration is aggressively targeting corruption, and recently identified corruption as a core U.S. national security interest. Central to the effort to combat corruption globally is targeting corrupt actors who rely on vulnerabilities in the United States and international financial systems to obscure ownership of assets and launder the proceeds of their illicit activities.

In support of the first-ever U.S. Strategy on Countering Corruption and the Administration's commitment to supporting and bolstering democracy, FinCEN is taking several actions to fight corruption and prevent it from undermining democratic institutions. These actions include implementing beneficial ownership requirements, better addressing money laundering risks in the real estate market, and identifying ways to enhance transparency for investment advisers.

One of Treasury's most significant contributions to the fight against corruption is through the implementation of the CTA, which will establish a beneficial ownership reporting regime to assist law enforcement in unmasking shell companies used to hide illicit activities. Access to beneficial ownership information reported under the CTA would significantly enhance the U.S. government's and law enforcement's ability to protect the U.S. financial system from illicit use. It would also impede malign actors from abusing legal entities to conceal proceeds from criminal acts that undermine U.S. national security, such as corruption, human smuggling, drug and arms trafficking, and terrorist financing. For example, beneficial ownership information can add valuable context to financial analysis in support of law enforcement and tax investigations. It can also provide essential information to the intelligence and national security professionals who work to prevent terrorists, proliferators, and those who seek to undermine our democratic institutions or threaten other core U.S. interests from raising, hiding, or moving money in the United States through anonymous shell companies.

Until the enactment of the CTA in 2021, Treasury had limited ability to identify and collect information about the beneficial owners of certain companies formed in the United States. The CTA requires specified legal entities to submit beneficial ownership information to FinCEN, and for FinCEN to provide timely access to this information to law enforcement, financial institutions, and other authorized users, under specific conditions, to help combat corruption,

---

Group Statement of Intent," (March 16, 2022), https://www.fincen.gov/news/news-releases/russia-related-illicit-finance-and-sanctions-fiu-working-group-statement-intent

money laundering, terrorist financing, tax fraud, and other illicit activity, and to help protect national security. This information must be accurate, complete, and highly useful to authorized government users while minimizing burdens on reporting companies.

In December 2021, FinCEN published in the Federal Register a Notice of Proposed Rulemaking (the "Reporting Rule NPRM") that proposed regulations to implement the beneficial ownership reporting requirements of the CTA, and in particular, defined core terms that will affect the scope of the regulations. This is the first of three proposed regulations that will fully implement the statutory requirements of the CTA. FinCEN received over 240 comments on this first proposal. Commenters weighed in on the breadth of issues considered in the context of the NPRM both in support of and to express concerns with aspects of the Reporting Rule NPRM. The timing of the final rule is not clear yet. It is a complex rulemaking that we need to get right—both for law enforcement and because of the effect that it will have on stakeholders such as small businesses and financial institutions.

FinCEN is currently developing a second NPRM that will propose regulations governing access to beneficial ownership information by law enforcement, national security agencies, financial institutions, and others specified in the statute (the "Access Rule NPRM"). We intend to publish this proposed rule this year.

The final rulemaking to implement the CTA is the revision to the Customer Due Diligence (CDD) regulation for financial institutions, which must be issued no later than one year after the effective date of the final reporting rule. The CTA directs that the revisions should bring the CDD regulation into conformance with the beneficial ownership rules under the CTA and reduce unnecessary or duplicative requirements, among other things. We are considering all options as we develop the Access Rule NPRM, and look forward to receiving public comments on our proposal when it is issued.

In concert with the rulemaking effort, FinCEN is developing the backbone of the beneficial ownership database—the Beneficial Ownership Secure System (BOSS). FinCEN has gathered initial requirements and is completing system engineering, architecture, and program planning, and the initial build of the cloud infrastructure and development environments are in progress. Data security is of the utmost importance, which is why the BOSS is being implemented to meet the highest Federal Information Security Modernization Act (FISMA) level (FISMA High) to secure the beneficial ownership information. The ability to search and access beneficial ownership information will be controlled and tailored by the users' purpose and role. All users will use strong authentication methods to access the information.

The goal of the CTA—and the proposed regulations to implement the CTA—is to combat the proliferation of anonymous shell companies that facilitate the flow and sheltering of illicit money in the United States. These beneficial ownership reporting obligations will make our economy—and the global economy—stronger and safer from criminals and national security threats.

To further implement the President's anti-corruption strategy, addressing the gaps in our anti-money laundering framework that allow the exploitation of the U.S. real estate market is another key area of focus. On December 6, 2021, FinCEN announced the issuance of an Advance Notice of Proposed Rulemaking (ANPRM) to solicit comments from the public to assist in crafting a rule to address money-laundering vulnerabilities in the real estate market. This ANPRM represented the next step in FinCEN's long-running fight to protect the real estate market from exploitation by criminals and corrupt officials. As highlighted in the ANPRM, the current Real Estate Geographic Targeting Order (GTO) program requires title insurance companies to file reports concerning non-financed purchases above $300,000 of residential real estate by certain legal entities in 14 metropolitan areas of the United States.

FinCEN issued these GTOs to ensure that law enforcement and national security agencies have relevant information concerning the approximately 25 percent of residential real estate transactions that proceed without financing from a bank or similar financial institution with full AML/CFT program requirements. FinCEN first issued the real estate GTOs in January 2016 and our law enforcement partners have consistently assessed that the GTOs produce valuable information that helps them target illicit activity. Against the backdrop of requests from law enforcement, FinCEN has renewed the GTOs, and when doing so has periodically expanded the covered geographic areas and lowered the reporting price threshold, based on feedback from law enforcement, as well as our own analysis.

FinCEN is carefully studying the 150 comments we received in response to the real estate ANPRM. These comments will help us move toward the next step, a proposed rule to address the illicit finance threats to the real estate market. While it is still too early to identify the scope of any NPRM or final rule, we are working to ensure that the requirements would be carefully crafted to result in valuable information for law enforcement, regulators, and the intelligence community, as well as to help the real estate sector protect itself from abuse by corrupt and other bad actors.

FinCEN continues to assess the illicit finance risks related to non-bank types of financial institutions that are not subject to comprehensive AML/CFT requirements to determine whether additional AML/CFT measures would be appropriate. As highlighted in the 2022 National Money Laundering Risk Assessment, the lack of a comprehensive AML/CFT regulatory framework for investment advisers may create vulnerabilities that illicit actors may be able to exploit.[5] In 2015, FinCEN issued a NPRM on investment advisers, but did not issue a final rule.

FinCEN, in coordination with the Treasury's Office of Terrorist Financing and Financial Crimes, is engaged in several lines of effort to better understand the nature of any AML/CFT risks presented by investment advisers and the specific channels through which those risks are transmitted. FinCEN's ongoing efforts include engaging with law enforcement, the Securities and Exchange Commission, and the Financial Industry Regulatory Authority. We are also

[5] See Treasury, "National Money Laundering Risk Assessment," (February 2022), https://home.treasury.gov/news/press-releases/jy0619

exploring how to use FinCEN's information collection authorities to enhance transparency in this sector, including regarding how Russian elites, proxies, and oligarchs may use hedge funds, private equity firms, and investment advisers to hide their assets.

This work is critical to scoping a potential rule to address the AML/CFT risks associated with investment adviser activity and to avoid duplicating regulatory efforts or placing undue burdens on small businesses. Even though investment advisers in the United States are not expressly subject to AML/CFT requirements under BSA regulations, investment advisers may fulfill some AML/CFT obligations in certain circumstances. For example, investment advisers may perform certain AML/CFT functions because they are part of a bank holding company, are affiliated with a dually-registered broker-dealer, or share joint customers with a BSA-regulated entity such as a mutual fund.

Further, as with any regulatory framework, it is important that sufficient resources are dedicated to outreach and engagement with newly covered financial institutions, coupled with effective examination and enforcement, in order to foster compliance. FinCEN will need to further consider the resource implications of a possible rule imposing AML/CFT obligations on investment advisers that could result in substantial additional supervisory and examination responsibilities.[6]

Effective Anti-Money Laundering Programs

We must ensure that the AML/CFT regime reflects modern national security needs, attacking threats as they exist in 2022 and as they continue to evolve. Effective AML/CFT programs are an invaluable tool in preventing current threats such as ransomware, stopping Paycheck Protection Program fraud, and rooting out corrupt Russian oligarchs, among other financial crimes. The AML Act imposes more than 40 requirements on FinCEN that are designed to make the AML/CFT framework more effective. It also recognizes that an effective and reasonably designed AML/CFT program is the cornerstone of a financial institution's ability to support law enforcement efforts to combat illicit finance. To support efforts by financial institutions to better understand U.S government priorities, and to incorporate those priorities into their AML/CFT programs, FinCEN published the first government-wide list of national AML/CFT priorities in June 2021.[7] The AML/CFT priorities confirm a broad range of threats to the integrity of the U.S. financial system and our national security, in addition to the financing of terrorism. We will update these priorities regularly, and that will help us keep pace with the shifting threat landscape.

---

[6] *See* North American Securities Administrators Association (NASAA) "2021 Investment Adviser Section Annual Report," (April 2021) at p. 1. *See also* Investment Adviser Association Report, "Investment Adviser Industry Snapshot 2021: Revolution Imagined," (July 2021, Second Edition) at p. 3, and SEC's Information About Registered Investment Advisers and Exempt Reporting Advisers.

[7] *See* FinCEN "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," (June 30, 2021),
https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

The AML Act describes certain factors that FinCEN is required to take into account as we consider minimum standards for AML/CFT programs and work toward new regulations that would require financial institutions to incorporate the national AML/CFT priorities. These include the private and public costs and benefits of AML/CFT programs, the need to extend financial services to the underbanked while preventing criminal abuse, the role of "effective" AML/CFT programs in protecting national security and preventing illicit finance, and that AML/CFT compliance programs should be "risk-based" and "reasonably designed to assure and monitor compliance."

The AML Act further incentivizes feedback loops among financial institutions, regulators, and law enforcement in other ways. It emphasizes and codifies public-private information sharing, in which FinCEN engages through FinCEN Exchanges and Innovation Hours. We have held FinCEN Exchanges to share information among FinCEN, law enforcement, and financial institutions on ransomware,[8] on suspicious activity report (SAR) reporting with a regional focus,[9] and on environmental crimes.[10] These have been productive exchanges, and we will be holding more. Typically, a FinCEN Exchange session includes participants from law enforcement, financial institutions and, as appropriate, other private sector entities, for the purpose of sharing information regarding typologies, threats, and vulnerabilities. This increases visibility and transparency for participants, and also informs internal BSA compliance and risk management processes. It also strengthens the financial intelligence received back from stakeholders through suspicious activity reporting, which in turn assists law enforcement and enhances FinCEN's development of analytical products such as advisories and public notices.

Another key feedback loop in the AML Act is the requirement that FinCEN at least twice a year publish threat pattern and trend information derived from suspicious activity reports to provide feedback to financial institutions regarding the use and value of these reports. In accordance with Section 6206, FinCEN published two of these FTA reports last year. As previously mentioned, the first FTA focused on ransomware. In December 2021, FinCEN published the second FTA focused on environmental crimes. FinCEN will publish additional FTA reports this year as required by the AML Act, and we expect that at least one of them will again focus on ransomware.

We continue to engage actively in the Bank Secrecy Act Advisory Group (BSAAG), which allows financial institutions, regulators, and law enforcement to engage directly to find ways to improve the AML/CFT framework. In May 2021, FinCEN launched the BSAAG Innovation and Technology Subcommittee, as required by Section 6207 of the AML Act, and the BSAAG Information Security and Confidentiality Subcommittee, as required by Section 6302. We have

[8] *See* FinCEN, "FinCEN Holds Second Virtual FinCEN Exchange on Ransomware," (August 10, 2021), https://www.fincen.gov/news/news-releases/fincen-holds-second-virtual-fincen-exchange-ransomware

[9] *See* FinCEN, "FinCEN Exchange Brings Together Public and Private Stakeholders to Discuss Bank Secrecy Act Suspicious Activity Reporting Statistics," (November 9, 2021), https://www.fincen.gov/news/news-releases/fincen-exchange-brings-together-public-and-private-stakeholders-discuss-bank-0

[10] *See* FinCEN, "FinCEN Holds FinCEN Exchange on Environmental Crimes and Related Financial Activity," (November 16, 2021), https://www.fincen.gov/news/news-releases/fincen-holds-fincen-exchange-environmental-crimes-and-related-financial-activity

a wide range of participants in these two new Subcommittees including representatives from the federal functional regulators, state banking supervisors, law enforcement agencies, and a variety of financial industry participants, such as depository institutions, casinos, money services business, securities, FinTechs, and digital asset service providers.

These two new Subcommittees are tackling important issues. The Innovation and Technology Subcommittee is focused on innovation themes related to digital identity, the coverage of payment processors under current regulations, and banking relationships with FinTech entities. The Information Security and Confidentiality Subcommittee priorities are looking at third-party vendor relationships and current information security technologies. We are working with the Subcommittees so that they can advise the BSAAG plenary in ways that can help shape our thinking on these important areas.

Another enhancement to FinCEN's feedback mechanism was the establishment of Domestic and Foreign FIU Liaisons in the AML Act to expand engagement with financial institutions and foreign partners. FinCEN has not had the resources to create either the Office of Domestic Liaison—to be led by a Senior Executive Service official overseeing at least six geographically dispersed senior FinCEN employees—or to hire at least six Foreign FIU Liaisons, as required by Sections 6107 and 6108 of the AML Act, respectively. We have requested FY23 appropriations to realize the legislative vision embodied in these two provisions.

Domestic Liaisons would allow FinCEN to improve significantly on the FinCEN-to-financial-institution segment of the feedback loops envisioned by Congress. These Domestic Liaisons will be located in financial centers around the country and will engage directly with regional financial institutions to not only provide those institutions with insights on what's effective in their reporting, but also to hear input and provide feedback on an ongoing basis about how FinCEN can execute its mission even more effectively.

Foreign FIU Liaisons will play a critical role in enhancing international information sharing and the efficiency of international cooperation to combat money laundering. We have seen that the presence of foreign liaisons can create incredible opportunities. FinCEN's one overseas liaison today is at Europol, and that liaison has played a crucial role leveraging existing relationships to organize the FIU Working Group supporting our efforts to enhance information sharing to respond to the threats posed by Russia's invasion of Ukraine. We look forward to achieving similar objectives in key jurisdictions globally.

The AML Act also requires annual training for bank examiners to enable them to better understand risk profiles and warning signs that an examiner may encounter during examinations. The training requirement reflects concerns that financial institutions have long expressed about how examiners evaluate AML/CFT programs and the degree to which those programs are effective and guard against money laundering. Options are largely dependent on funding: considerations include the need for human capital for ongoing design, updating, monitoring, and delivery of the annual training program, as well as technology for delivery and tracking.

The AML Act also places the modernization of the AML/CFT framework—and the role of innovation in that modernization effort—front and center. As required by the legislation, we are working to find ways not only to revise or eliminate regulations that are "outdated" or "redundant," but also to identify ways to provide opportunities for financial institutions to adopt innovative technologies that help them enhance their compliance programs.

Last December, we issued a Request for Information (RFI) pursuant to section 6216 of the AML Act.[11] That RFI sought public input on ways in which FinCEN can streamline, modernize, and update the AML/CFT framework so that it can continue to protect U.S. national security and prevent illicit finance in a way that promotes an efficient allocation of resources.

We received 140 comments, and are carefully reviewing every comment with the goal of developing a report and recommendations on ways to modernize the AML/CFT regulatory framework. In doing so, we will continue to consult with government, private sector, and civil society stakeholders. Our goal is also to take good, practical ideas and to find ways to implement those ideas as we continue to work on the overall report and recommendations. This information will inform the report to Congress required by Section 6216, as well as in other rulemakings and efforts in the coming months.

In parallel, we are spending considerable time on innovation and its implications for the AML/CFT regulatory framework. New technologies, automation of compliance efforts, and other innovations can all help to enhance implementation of AML/CFT programs. Our limited experience suggests that they may also allow financial institutions to allocate resources more efficiently and to engage in more high value, resource intensive investigative work that provides greater value to law enforcement.

For nearly three years, FinCEN has been using public-private engagement opportunities, such as our Innovation Hours program, to talk to financial institutions and FinTech or RegTech companies that are building innovative solutions.[12] These Innovation Hours allow FinCEN staff to learn about innovative solutions, better understand the degree to which financial institutions are deploying those solutions, and to ask questions about their regulatory implications.

We also continue to explore the creation of structured pilot programs. These can be frameworks for institutions to pilot the use of innovative technologies through exceptive relief authority. They do not have to be technology focused. For example, in accordance with Section 6212, we issued draft regulations on January 24, 2022, seeking comment on a pilot program for financial institutions to share SARs with their foreign affiliates: we received 17 comments.[13] In the

[11] *See* FinCEN, "FinCEN Seeks Comments on Modernization of U.S. AML/CFT Regulatory Regime," (December 14, 2021), https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime

[12] *See* FinCEN, "FinCEN Announces Its Innovation Hours Program," (May 24, 2019), https://www.fincen.gov/resources/fincens-innovation-initiative,

[13] *See* FinCEN, "FinCEN Issues Proposed Rule for Suspicious Activity Report Sharing Pilot Program to Combat Illicit Finance Risk," (January 24, 2022), https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-suspicious-activity-report-sharing-pilot-program

technology space, we can envision consideration of efforts involving artificial intelligence or machine learning-driven transaction monitoring, dynamic approaches to customer risk rating and institutional risk assessment, digital identity tools and utilities, and automating the adjudication and filing of SARs related to certain types of activity.

Enforcement and Compliance

Another cornerstone of our efforts to foster effective and efficient AML/CFT programs is enforcement and compliance. FinCEN is expanding its enforcement and compliance team and working closely, or in parallel, with the Federal Functional Regulators and law enforcement on compliance and enforcement efforts. Compliance examinations and enforcement actions play a critical role in driving broad compliance with the BSA.

As part of potentially extending and supplementing FinCEN's existing tools for regulatory guidance and relief, FinCEN is implementing the AML Act's no-action letter provision. This provision required FinCEN, in consultation with other agencies and officials, to conduct an assessment on whether to establish a process for the issuance of no-action letters in response to inquiries concerning the application of AML/CFT laws and regulations to specific conduct. It also required the Secretary, in coordination with others, to submit a report (the Report) to Congress, and propose rulemaking, if appropriate, to implement the findings.

FinCEN submitted and published the Report on June 28, 2021.[14] The Report concluded that FinCEN should undertake a rulemaking to establish a no-action letter process to supplement the existing forms of regulatory guidance and relief that may currently be requested from FinCEN. We aim to begin that rulemaking by publishing an ANPRM in the Federal Register this summer to solicit public comment on questions pertinent to the implementation of a no-action letter process at FinCEN.

FinCEN is also implementing the AML Act's whistleblower provisions, which are designed to pay awards to eligible individuals who have voluntarily provided FinCEN or the Department of Justice (DOJ) with original information about BSA violations. Funding constraints have slowed our efforts, but FinCEN has taken several steps to implement the whistleblower provisions. For example, in FY 2021, FinCEN created a new Office of the Whistleblower within its Enforcement and Compliance Division. We hired key personnel to build and lead the program. The office will eventually be staffed with a cadre of enforcement officers who will assess and investigate, where appropriate, whistleblower tips and information and process applications for awards.

FinCEN is actively reviewing tips and referring appropriate matters for investigation while drafting regulations to implement the whistleblower provisions of the AML Act in a way that encourages whistleblowers to step forward when they see or suspect BSA violations. These efforts include developing an online tip intake system and award application process. We are in the early stages of this effort, but we are very excited about it and look forward to the public

[14] *See* FinCEN, "FinCEN Completes Assessment on the Use of No-Action Letter," (June 30, 2021), https://www.fincen.gov/news/news-releases/fincen-completes-assessment-use-no-action-letters

comment following the publication of a Notice of Proposed Rulemaking, and working with Congress to further enhance this program.

Resources

While the AML Act made significant improvements to the AML/CFT framework, these improvements come at a cost. FinCEN employs a team of about 300 dedicated employees, including intelligence analysts, investigators, AML/CFT policy strategists, enforcement and compliance officers, outreach specialists, data analysts, regulators, and economists.

We appreciate the Fiscal Year (FY) 2022 appropriations to support the development of the beneficial ownership IT infrastructure and our efforts to support the U.S. response to Russian aggression. Nonetheless, FinCEN has significant staffing requests that remain unfunded. These include, but are not limited to, personnel needed to implement the beneficial ownership framework under the CTA, Foreign FIU Liaisons, Domestic Liaisons, BSA Innovation and Information Security Officers, enforcement officers for the new Whistleblower Office, other Enforcement and Compliance Division personnel, innovation experts, information security experts, data scientists and emerging technology experts, among other critical positions. Many of these positions are requirements of the AML Act.

The FY 2023 President's Budget request for FinCEN is $210.3 million—an increase of $49.3 million from the FY 2022 enacted levels. This request provides critical funding for AML Act and CTA implementation, including the full-time employees necessary to support on-going requirements from the AML Act, including the CTA, and FinCEN's Office of Chief Counsel more broadly.

Conclusion

In closing, timely and effective implementation of the AML Act, which includes the CTA, is a top priority. The FinCEN team is working diligently with law enforcement and regulatory stakeholders to promulgate rules and take other steps under the legislation that will further the national security of the United States and promote a more transparent financial system.

That said, limited resources have presented significant challenges to meeting the implementation requirements of our expanded mandate under the AML Act, including the CTA's beneficial ownership requirements. As you are aware, we are missing deadlines, and we will likely continue to do so. FinCEN's budget situation has required prioritization across the board, but we are working hard to meet our obligations. Congressional support for our FY 2023 budget request is critical to FinCEN's success in meeting AML Act requirements and general mission obligations.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you may have.