Prepared Remarks of FinCEN Acting Director Himamauli Das During NYU Law's Program on Corporate Compliance and Enforcement

March 25, 2022

Prepared Remarks

Himamauli Das

Acting Director

Financial Crimes Enforcement Network

NYU Law's Program on Corporate Compliance and Enforcement (PCCE)

March 25, 2022

Good morning and thank you for inviting me to be a part of your discussions this year. I want to start by thanking Jennifer Arlen and the staff at NYU's Program on Corporate Compliance and Enforcement for focusing on the effectiveness of corporate compliance programs.

Current events often make clear the importance of compliance programs that are 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 that COVID-19 was having on a range of illicit finance threats around the world. We issued guidance and advisories to advise financial institutions of trends that we were seeing related to COVID-19 medical fraud, imposter scams, cyber-enabled crime, and the defrauding of the unemployment insurance system. And, we assisted law enforcement and financial institutions in the recovery of stolen funds 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). This report -- for the first time -- shared with the public ransomware trends and typologies gleaned from financial intelligence provided to FinCEN by financial institutions. FinCEN also published an advisory and hosted a FinCEN Exchange 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 – and tragic – situation in Ukraine places a renewed spotlight on the importance of effective compliance programs that are able to provide insights and information to law enforcement and national security agencies. We have established task forces to track, freeze, and seize oligarch assets – both within the

U.S. government and with our international partners. FinCEN has now issued two alerts – on typologies and red flags related to sanctions evasion (https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf) and channels through which oligarchs hide and launder corrupt proceeds (https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Elites%20High%20Value%20Assets_508%20FINAL.pdf) … shell companies, real estate and the purchase of luxury goods and high-end art. We are working through public-private efforts to ensure that law enforcement and financial institutions can share information on ways in which the Russian government and its enablers may try to evade sanctions. And, we are sifting through the information submitted by financial institutions to trace beneficial owners of shell companies established by oligarchs, hidden assets, and efforts to evade sanctions.

Background

Before discussing FinCEN's work on effective compliance programs, I would like to take a moment to discuss FinCEN's mission and what we do. I hope that it will provide a helpful backdrop for our discussion today.

FinCEN administers the Bank Secrecy Act, or the BSA, which is the United States' primary regulatory regime to combat money laundering and to counter terrorist financing. In this role, FinCEN receives reports from financial institutions about suspicious financial transactions, which we then analyze and make available to law enforcement, intelligence, national security, and regulatory agencies. FinCEN is also the financial intelligence unit of the United States – and in this capacity, we work with similar FIUs in foreign governments to share information internationally about suspicious transactions and to share best practices. These efforts help us – and law enforcement – get a full picture of the ways in which bad actors hide and move funds across financial institutions and across borders.

FinCEN employs a team of about 300 dedicated employees, including intelligence analysts, investigators, anti-money laundering/countering the financing of terrorism (AML/CFT) policy strategists, enforcement and compliance officers, outreach specialists, data analysts, regulators, and economists. In comparison, our counterpart regulators are significantly larger – for example, the Office of the Comptroller of the Currency (https://www.occ.gov/about/what-we-do/key-data-and-statistics/index-occ-and-federal-banking-system-at-a-glance.html) has about 3,500 staff, the Federal Deposit Insurance Corporation (https://www.fdic.gov/news/board-matters/2021/2021-12-14-notice-dis-a-mem.pdf) has around 5,800, and the New York Department of Financial Services (https://www.budget.ny.gov/pubs/archive/fy21/exec/agencies/appropdata/FinancialServicesDepartmentof.html) has more than 1,300.

FinCEN regulates a broad swath of financial institutions for AML/CFT purposes. These range from banks and traditional depository institutions to brokers and dealers in securities; insurance companies; money services businesses; casinos and card clubs; and dealers in precious metals, stones, or jewels. These institutions present different risks; range vastly in size and scope; and have different experiences with compliance programs and efforts.

Our regulations impose recordkeeping and reporting requirements on financial institutions that are designed to elicit highly valuable information to combat illicit finance. The two most common reports are the Currency Transaction Report, known as the CTR, and the Suspicious Activity Report, or the SAR. CTRs must be filed on all cash transactions exceeding $10,000. In 2021, there were over 18 million CTRs filed by financial institutions around the country. In the case of a suspicious activity report, a financial institution must file a SAR if it "knows, suspects, or has reason to suspect" that a transaction is suspicious. Generally speaking, the transaction must involve $5,000 or more in a single transaction, or in the aggregate. Last year, financial institutions filed over 3 million SARs with FinCEN. These reports often include additional account information, dollar amounts, the nature of the transactions, and other information that were suspicious to the financial

institution. These reports can provide valuable information about transactions that might be linked, for example, to terrorism financing, corruption, ransomware attacks, transnational crime, drug trafficking, and massive fraud schemes.

In 2021, Congress enacted the Anti-Money Laundering Act of 2020. That legislation amended the Bank Secrecy Act – FinCEN's foundational statute – and substantially enhanced FinCEN's mandate, added to its responsibilities, and emphasized certain factors that FinCEN needs to take into account in prescribing the AML/CFT compliance framework. The legislation defines FinCEN's mission, among other things, to prevent money laundering and terrorist financing through the establishment by financial institutions of reasonably designed risk-based AML/CFT compliance programs.

Effectiveness

In the whole, the AML Act sets out over 40 requirements on FinCEN – all designed to make the AML/CFT framework work better.

The AML Act reflects concepts and programs that were being discussed between regulators, law enforcement, and financial institutions to improve the overall AML/CFT framework at the time. In September of 2020, for example, FinCEN released an Advanced Notice of Proposed Rulemaking (https://www.fincen.gov/index.php/news/news-releases/fincen-seeks-comments-enhancing-effectiveness-anti-money-laundering-programs), or "ANPRM," on effectiveness. The ANPRM sought public comment on incorporating an "effective and reasonably designed" AML program component to empower financial institutions to allocate resources more effectively. The potential regulatory amendments described in the ANPRM were intended to make clear that an "effective and reasonably designed" program is one that:

- assesses and manages risk as informed by a financial institution's own risk assessment process, including consideration of AML priorities to be issued by FinCEN,
- provides for compliance with BSA requirements, and
- provides for the reporting of information with a high degree of usefulness to government authorities.

We asked a number of questions, like: How do we achieve, measure, and examine for, effectiveness in our AML regime? How do we work together to adequately provide the flexibility that industry needs to allocate resources according to risk and priorities to help government authorities with actionable information? How do we communicate our needs and information to each other and feel confident that something will come of it?

FinCEN received 108 comments. Many expressed the view that compliance with AML requirements has become inefficient and falls short of serving law enforcement needs. Commenters noted that financial institutions are spending a lot of time and money on technical compliance, exercises that "check the box," but may not necessarily be doing much to combat the actual risks of financial crime. That's not the intended purpose of AML/CFT programs. Rather, effective AML/CFT programs should safeguard national security and the financial system from illicit use by preventing and detecting the abuse of our financial system.

I think we can all agree that an effective and reasonably designed AML/CFT program is an important cornerstone for a financial institution. But, in many ways, an effective AML/CFT framework requires a partnership. It's an effort that goes in two directions. The AML Act reflects this.

An important step toward building that partnership was FinCEN's release in June 2021 of the first government-wide list of national AML/CFT priorities (https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf). This list reflects extensive consultations within the Treasury Department, with Federal and State banking regulators, as well as law enforcement and national security agencies.

The AML Act also incentivizes feedback loops between financial institutions, regulators, and law enforcement in other ways. It emphasizes and codifies public-private information sharing, which FinCEN engages in through FinCEN Exchanges and Innovation Hours. We have held FinCEN Exchanges to share information between

FinCEN, law enforcement, and financial institutions on ransomware, on SAR reporting with a regional focus, and on wildlife trafficking. These have been productive exchanges. We will be holding more. The AML Act also requires FinCEN to publish twice a year analyses of SARs filed by financial institutions – the Financial Trends Analysis that I mentioned earlier. We issued two reports last year – analyzing SAR reporting on ransomware (https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf) and on wildlife trafficking (https://www.fincen.gov/sites/default/files/2021-12/Financial_Threat_Analysis_IWT_FINAL%20508_122021.pdf). We also continue to engage actively in the Bank Secrecy Act Advisory Group – which allows financial institutions, regulators, and law enforcement to engage directly to find ways to improve the AML/CFT framework.

The AML Act requires annual training for bank examiners so that they 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 and auditors evaluate AML/CFT programs and the degree to which those programs are effective and guard against money laundering.

And, the AML Act defines certain factors for FinCEN to take into account as it considers minimum standards for AML/CFT programs and works towards new regulations that require financial institutions to incorporate the national AML/CFT priorities and risk assessments into their programs. 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."

FinCEN is committed to working with financial institutions, law enforcement, and other stakeholders to ensure that the AML/CFT framework is effective. Through this process, we will ensure that financial institutions are able to focus resources where it counts and get credit for effective programs. This is also how we will ensure that the BSA continues to protect the integrity of the U.S. financial system and the national security of the United States in a cost-effective and efficient manner.

Modernization and Innovation

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) (https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime) under section 6216 of the AML Act. 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.

The comment period closed on February 14. We received 140 comments during the comment period. We are carefully reviewing every single 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.

In general, the comments – which are available publicly – urged FinCEN to enhance existing public-private information sharing mechanisms, to foster innovative approaches to BSA compliance, and to consider various changes to existing recordkeeping and reporting obligations.

Some themes emerged in the comments. For example, financial institutions want FinCEN to adopt risk-based and effective AML program obligations that permit them to allocate resources based on their individual risk assessments. Financial institutions have also noted concerns about examination incentives that result in resource-intensive "check the box" compliance exercises and defensive filings that may not provide the information that's most valuable to law enforcement in preventing money laundering or other illicit finance.

These are important concerns – and ones that we have been working on with financial institutions over the past few years. We will continue to be focused on these issues as we work to develop 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 innovative efforts can all help to enhance implementation of AML/CFT programs. Our experience – albeit limited – suggests that it may also allow financial institutions to allocate resources more efficiently and to address high value, resource intensive investigative work that provides greater value to law enforcement.

Financial institutions are also applying new technologies like artificial intelligence and machine learning in the compliance space. As they seek to transition from wholly rules-based transaction monitoring or KYC systems to systems that rely to a greater degree on machine learning, questions will arise with respect to the efficacy with which newer systems detect suspicious activities in relation to existing systems. How the machine learning based system works and provides results. Whether there is bias in the system. It is important to recognize that neither system is perfect. Both require trade-offs, impose different costs, and have different benefits.

For more than two years now, 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. 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 the regulatory implications.

We are also continuing to explore the creation of regulatory sandboxes or structured pilot programs. These can be a series of interim, but formal, frameworks for institutions to pilot the use of innovative technologies or isolated programs through the use of exceptive relief authority to permit a financial institution to test an innovative approach. It does not have to be technology focused. For example, we recently issued draft regulations for comment regarding a pilot program for financial institutions to share SARs with their foreign affiliates (https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime). In the technology space, we can envision 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.

If we could stand up these sandboxes tomorrow, we would. We know there's a lot of interest in something like this, and we're going to move as quickly as possible. We need more staff and budget to help build the program, and we are working on that.

An important component for these efforts to work is communication – or in the framework of a sandbox or pilot program, a mechanism for oversight. Communication and appropriate oversight and reporting will not only allow regulators and law enforcement to better understand both the comparability of the outputs of new and existing technologies, but also the trade-offs and efficiencies. This can be done through a range of metrics or factors – the number of alerts or SARs filed or omitted, the number of "false positives" or non-productive alerts, how resources are allocated across the compliance team, and others. At root, law enforcement and regulators need to have confidence that the new system will continue to provide information that is highly useful to law enforcement and will guard against money laundering.

We know that innovation will only happen if the private sector feels it has latitude to innovate. At FinCEN, we're committed to ensuring that the space to innovate is as large and as safe as it has to be. Three years ago, we issued a joint statement (https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf) together with the Federal Reserve, the OCC, FDIC, and NCUA encouraging financial institutions to adopt innovative approaches, including the use of AI, to meet their obligations under the BSA. We said that we wouldn't penalize financial institutions for failing to innovate along these lines, but we wanted to support those that did. FinCEN is working with other regulators and moving forward with what that support actually looks like.

Compliance and Enforcement

This brings me to another cornerstone of our efforts to foster effective and efficient AML/CFT programs: enforcement and compliance.

Financial institutions need to implement reasonably designed and effective AML programs. The Bank Secrecy Act says so. But instead, over the years, our enforcement and compliance teams have seen a number of financial institutions with "paper programs." By that, I mean AML programs that look functional, but which do not allow an institution to identify and generate meaningful reporting of a significant amount of suspicious activity flowing through the institution. This often arises when financial institutions put growth before compliance and think about compliance as only a cost center.

That's why FinCEN is expanding its enforcement and compliance team and working closely, or in parallel, with the Federal banking regulators, the securities regulators, and law enforcement on compliance and enforcement efforts. Compliance examinations and enforcement actions are a critical part of the toolkit through which we communicate compliance expectations.

FinCEN takes strong enforcement action where there are willful violations of the BSA, or where there is an egregious disregard of requirements to implement and maintain an AML program that reasonably guards against money laundering and terrorist financing, or to identify and report suspicious activity to FinCEN.

Just this month, FinCEN imposed a $140 million fine (https://www.fincen.gov/news/news-releases/fincen-announces-140-million-civil-money-penalty-against-usaa-federal-savings) against a financial institution, together with the OCC, for the bank's failure to maintain an effective and reasonably designed anti-money laundering program, and failing to file at least 3,783 suspicious activity reports, over a 5-year period. At root, the program failed to guard against money laundering, as required by the Bank Secrecy Act. And last August, FinCEN assessed a $100 million fine (https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures) against BitMEX, one of the oldest and largest virtual currency derivative exchanges, for operating without a compliant AML program and for facilitating more than $200 million in transactions involving known darknet markets or unregistered money services businesses.

I think the message here is clear: our enforcement office does not tolerate paper programs.

I know that there is interest in the FinCEN whistleblower program. Whistleblower referrals will translate into greater transparency on enforcement and compliance priorities because employees are not only financially incentivized to bring non-compliance issues directly to FinCEN, they are also protected from retaliation by their employers for communicating those issues directly with FinCEN.

FinCEN's Enforcement and Compliance Division is implementing the AML Act's whistleblower provision. The Whistleblower Program is designed to pay awards to eligible individuals who have voluntarily provided FinCEN or the Department of Justice (DOJ) with original information about BSA violations. We're in the early stages of this effort, but we're very excited about it.

Financial institutions often say they have three lines of defense—their lines of business, their compliance departments, and their auditors. In some ways, FinCEN's whistleblower program will be a 4th line. We anticipate the whistleblower program will incentivize individuals to share valuable information and

significantly contribute to FinCEN's compliance and enforcement efforts.

There are a number of statutory guardrails for the Whistleblower Program. To be eligible for an award, the whistleblower's information must lead to a successful enforcement action by FinCEN or DOJ. Additionally, the statute requires FinCEN and the DOJ to preserve the confidentiality of whistleblowers, but also affords the government the ability to share the whistleblower's information with our law enforcement and regulatory partners.

The AML Act also prohibits any form of retaliation or discrimination by employers against individuals who provide FinCEN or DOJ with information about potential BSA violations. The protections afforded a whistleblower are quite robust, and include the right to bring a cause of action before the Department of Labor or in court where a whistleblower can seek compensatory damages, reinstatement, and two times the amount of any back pay they are owed. Our partners at the Department of Labor will be responsible for administering and implementing these retaliation protections. These guardrails are important because they provide whistleblowers with the confidence and protection they need to come forward and blow the whistle when they see or suspect BSA violations.

The AML Act calls for Congress to fund the whistleblower program through congressional appropriations, and we continue to work constructively with Congress on this point. We are hopeful for continued progress over the course of the year. The lack of funding has slowed our efforts, but despite budgetary challenges, FinCEN has taken several steps to implement the whistleblower provisions:

- FinCEN recently created a new Office of the Whistleblower.
- We hired key personnel to build and lead the program. The office will be staffed with enforcement officers who will assess and investigate, where appropriate, whistleblower tips and information.
- We are accepting whistleblower tips while we work towards the development of a more formal tip intake system.
- And, we are actively drafting rules to implement the whistleblower provision of the AML Act.

FinCEN looks forward to creating a robust whistleblower program and will welcome public comment following the publication of a Notice of Proposed Rulemaking.

In closing today, I want to thank you all for being a part of the dialogue and keeping these issues at the front and center of the work we are doing in the compliance space. I do believe that whether you are on the corporate side or approaching these issues as a regulator that we are all working towards the same goals. I look forward to an ongoing partnership with you all as we move forward together.

###

Newsroom (/news-room)

Contract Opportunities (/about/contract-opportunities)

Get News Updates (https://service.govdelivery.com/accounts/USFINCEN/subscriber/new)