Remarks by Under Secretary for Terrorism and Financial Intelligence Brian Nelson at SIFMA's Anti-Money Laundering and Financial Crimes Conference

May 25, 2022

As Prepared for Delivery

Good morning—thank you, Ira, for the warm welcome, and thank you to SIFMA for inviting me to speak with you today.

Compliance plays a critical role in protecting the integrity of the financial system, and no one appreciates that more than me and my colleagues at the Treasury Department. I know that many of you have been working around the clock these past few months to ensure that your institutions' compliance programs keep pace as Russia's war has revealed new risks and meaningfully expanded sanctions obligations. Please know that the U.S. government greatly values these efforts. Our ability to address Russian illicit finance—and illicit finance in general—is truly a partnership.

I am going to start this morning with the issue that is top of mind for us all—Russia's unprovoked and brutal invasion of Ukraine. Then, I will turn to some of the biggest illicit finance risks facing the United States and provide an overview of the priorities laid out in Treasury's recently released National Illicit Finance Strategy. Finally, I'll highlight one of those priorities—our ongoing work to understand and address the anti-money laundering and countering the financing of terrorism, or AML/CFT, risks related to investment advisers.

Since Russia's invasion began in February, the United States and our international partners have responded swiftly and decisively by using extraordinary financial measures to impose severe economic costs on the Russian Federation and its leadership.

I'd like to share the latest on our efforts as well as the direct impact they're having on the Kremlin's ability to fund its war effort and project power.

First, we have targeted Russia's financial sector and the key sources of revenue that sustain Putin's war machine. We've sanctioned Russia's largest financial institutions and restricted dealings with banks representing approximately 80 percent of the Russian banking sector.

We've immobilized assets of the Central Bank of Russia and have prohibited Russia from making debt payments using funds within the United States. We've also imposed new sovereign debt prohibitions, restrictions related to new debt and equity of major Russian state-owned enterprises and large privately - owned financial institutions, and full blocking sanctions on two Russian state investment funds. These actions have made it harder for Russia to raise capital to fund its war of aggression.

Second, we have focused on degrading Russia's defense sector and other critical sectors feeding its military industrial complex. We recently designated more than 80 individuals and entities associated with Russia's defense sector and weapons manufacturing. We've targeted major Russian defense enterprises for their direct involvement in the war in Ukraine and blocked key state-owned enterprises that act as a source of revenue for the Kremlin and produce the weapons and technology used to wage this horrific war. We are closely monitoring where these defense firms get their critical inputs and will work to degrade their supply chains. As the Russian military finds itself in need of resupply—thanks to the heroic efforts of Ukraine's defenders—they will find that the technology they rely on is increasingly difficult to obtain. Already, Russia's two major tank facilities have halted production because of a lack of foreign components. We, along with our partners, are undercutting Russia's capacity to build and maintain the tools of war.

And third, we know that many Russian oligarchs and elites are attempting to evade sanctions, and we are working tirelessly to prevent sanctions evaders from exploiting financial loopholes to hide and move their wealth. In March, Treasury and the Department of Justice joined with the G7, Australia, and the European Commission to launch the Russian Elites, Proxies, and Oligarchs, or *REPO*, Task Force. The work of this multilateral body has resulted in the freezing of assets controlled by sanctioned Russian elites and oligarchs around the world. In parallel, the Financial Crimes Enforcement Network (FinCEN), a Treasury bureau, issued a joint statement with an array of foreign Financial Intelligence Units to form a Working Group on Russia-Related Illicit Finance and Sanctions. This working group of financial intelligence units will identify opportunities for actions and partnerships to combat the threat caused by Russia's unprovoked invasion of Ukraine. As part of these multilateral efforts, we are prioritizing attention on the tools and networks that Russian elites and enablers use to obfuscate their wealth. We will go after their assets wherever they are. We will not stand by if others assist in sanctions evasion schemes. Individuals or entities that do so will expose themselves to sanctions and, as appropriate, civil or criminal enforcement.

Our goal has been to impose economic costs squarely on Russia, and to minimize any impact on other economies—including our own. We have carefully crafted wind-down provisions and general licenses to allow for an orderly exit from affected markets and to ensure the continued flow of transactions critical to the global economy, including in energy and agriculture.

In all of this, we greatly value our partnership with the private sector as we seek to promote private-sector compliance. We are doing this through guidance, outreach, and enforcement.

First, we issue extensive guidance. We want to ensure the private sector has as much clarity as possible about OFAC's sanctions. We recognize the sanctions imposed on Russia are complex. To help industry understand its obligations, OFAC has issued ninety (90) new and seventy-six (76) amended frequently asked questions since February, published a fact sheet explaining authorizations related to humanitarian, medical, and NGO transactions, and processed hundreds of requests for licenses and interpretive guidance. Additionally, 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. The second highlighted channels that oligarchs may use to hide and launder corrupt proceeds. We encourage you to review these resources.

Second, we conduct outreach. Our team has directly engaged with affected industries and companies on a regular basis, providing guidance as quickly as possible. Conferences like this are very important to us—we want to know what the compliance challenges are and where additional guidance or clarity would be useful. Over the course of the conference, representatives from both OFAC and FinCEN will be speaking on various panels, and I encourage you to engage with them. Even if we cannot answer the question immediately, this engagement helps us consider how we may adjust or issue additional guidance. As a reminder, OFAC runs a "Compliance Hotline," which receives thousands of calls a year—90 percent of which we respond to within 24 hours.

Third, as appropriate, we will take enforcement actions. Enforcement is one of the tools we use to promote compliance, and this is particularly important in the context of our Russia sanctions program. We will take enforcement actions against institutions or individuals that evade, avoid, cause a violation of, or conspire or attempt to violate OFAC regulations. OFAC encourages anyone who may have violated OFAC regulations to voluntarily disclose the apparent violation to OFAC. Voluntary self-disclosure is considered a mitigating factor by

OFAC in enforcement actions, and under OFAC's Enforcement Guidelines it will reduce the base amount of any proposed civil penalty.

We view the private sector as a partner in all of these efforts. We welcome actionable information from you. Treasury recently launched the Kleptocracy Asset Recovery Program, which offers monetary rewards for information leading to seizure, restraint, or forfeiture of assets linked to Russian government corruption. We have an "oligarch tip line" and an e-mail inbox.

In short, this is a historic effort made possible in large part by the collaboration we have with the compliance community. We understand some of our recent actions in Russia and elsewhere have been novel and technically complex. We also understand this has generated numerous demands on the compliance community over the last few months. That's why we so greatly appreciate the collaboration with the private sector as we work to impose severe economic costs on the Russian Federation and its leadership.

Russia's war against Ukraine—supported by decades of endemic corruption by Putin and his cronies—underscores the broader principle that illicit finance is a major national security threat.

At the Treasury Department, we are committed to taking the steps necessary to curb illicit finance. I'd like to call attention to some recently published Treasury reports that provide insight into how we are approaching these issues.

First, in early March, Treasury released the 2022 National Risk Assessments on Money Laundering, Terrorist Financing, and Proliferation Financing. These assessments reflect a whole-of-government effort to understand the risks facing our financial system. The assessments highlighted an array of illicit finance risks—including the abuse of legal entities, the complicity of professionals that misuse their positions or businesses, small-sum funding of domestic violent extremism networks, the effective use of front and shell companies, and the exploitation of the digital economy. I would encourage you to use these assessments to evaluate the specific risks facing your institutions as you seek to develop and maintain a risk-based compliance program.

Second, earlier this month, Treasury published the 2022 U.S. Illicit Finance Strategy, a report that outlines how Treasury plans to target illicit financial activity. The strategy provides a roadmap to close loopholes that can be exploited by criminals and corrupt actors.

Our strategy prioritizes actions to improve financial transparency. It includes multiple lines of effort in support of the Administration's Anti-Corruption Strategy. To highlight a few examples:

FinCEN is implementing the Corporate Transparency Act by establishing a beneficial ownership reporting structure to assist law enforcement in unmasking shell companies that criminals use to hide their illicit activities.

FinCEN is crafting a rule to address money-laundering vulnerabilities in the real estate market to ultimately reduce anonymity in these transactions.

Internationally, Treasury is working with the Financial Action Task Force or FATF to improve global beneficial ownership standards.

Last June, FinCEN published the first government-wide list of national AML/CFT priorities, and we expect that later this year FinCEN will issue regulations that will specify how all covered institutions should incorporate these priorities into their risk-based AML programs.

We view illicit finance as a core national security issue, and we're focused on addressing these threats. The compliance community is an integral partner in that endeavor. Accordingly, we ask that financial institutions work to understand their own risk profiles and take a risk-based approach to compliance.

I'd like to conclude today by focusing in on the money laundering risks associated with investment advisors.

As the National Money Laundering Risk Assessment noted, certain financial intermediaries, such as investment advisers, are not subject to comprehensive AML/CFT regulations. While investment advisers are subject to multiple federal and state regulatory requirements, those requirements primarily focus on consumer protection. The Risk Assessment highlighted some core risks related to the lack of AML/CFT obligations:

First, while some investment advisers may fulfill some AML/CFT obligations in certain circumstances, the lack of consistent standards across the industry can incentivize regulatory arbitrage. At the moment, investment advisers may *voluntarily* perform certain AML/CFT functions or comply with AML/CFT obligations of an affiliated entity. But inconsistencies in AML/CFT obligations across segments of the market create a vulnerability that illicit actors can exploit. In particular, the lack of consistent requirements to identify and report suspicious transactions can be detrimental to our national security.

And second, aspects of the investment adviser industry are segmented, which can limit transparency. For example, a broker-dealer executing a trade at the direction of an adviser may not know the identity of the adviser's client. The same is true for a prime broker that holds assets in custody on behalf of a hedge fund. The prime broker may hold the assets and execute trades on the fund's behalf, but the broker lacks clarity about the ultimate investors in the hedge fund.

Given these vulnerabilities, money launderers may see some investment advisers as a low-risk way to enter the U.S. financial system. The FBI has indicated that threat actors likely place funds in private investment companies, including hedge funds and private equity funds, to launder money and thereby circumvent traditional AML/CFT compliance programs. Additionally, according to industry data, there is a growing shift in the securities industry: an *increase* in the number of registered investment advisers and a *decrease* in the number of registered broker-dealers, which face more stringent AML/CFT requirements. There may be many benign reasons for this shift, but it could also reflect an attempt by entities to move into an industry with fewer AML compliance requirements. We are continuing to monitor and scrutinize this issue.

While the Money Laundering National Risk Assessment provides us with an initial *overview* of some of the risks facing the investment adviser business, Treasury is engaged in additional analysis to identify the best ways to enhance transparency for investment advisers. In 2015, FinCEN issued a Notice of Proposed Rulemaking (NPRM) on investment advisers, but did not issue a final rule. To better understand the extent and nature of any AML/CFT risks and determine whether action is appropriate, my team is focused on a few lines of effort.

First, we are engaging with law enforcement, the SEC, and FINRA to further understand their view of the risk landscape.

Second, we are engaging with industry to understand your assessment of the vulnerabilities and risks.

And third, we are thinking through ways to gather information that will enhance our visibility into 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 information-gathering effort will help us understand whether a rulemaking is necessary and, if so, how to design it to ensure that it is appropriately tailored.

As with all measures, we are carefully considering risks before identifying which steps would be appropriate—the same way that we advise all of you to understand the risks you face so that you can effectively implement the risk-based approach.

I want to thank you all for the continued collaboration and for your daily vigilance to safeguard the financial system. As I discussed today, we see the securities industry as a priority in our ongoing work to enhance transparency in the financial system. At this critical juncture, the compliance community is an indispensable partner in our efforts to respond decisively to Russia's unprovoked war against Ukraine. Your work is vital to our national security, and for that you have my sincere gratitude. Thank you again for the opportunity to speak to you this morning.