

Oversight of the Office of Terrorism and Financial Intelligence (TFI) and the Financial Crimes Enforcement Network (FinCEN)
House Financial Services Committee
February 14, 2024
Under Secretary Brian E. Nelson
U.S. Department of the Treasury
Written Testimony

Introduction

Good afternoon, Chair and Ranking Member, and distinguished members of the committee. Thank you for the opportunity to speak with you once again about the important work of the Treasury Department's Office of Terrorism & Financial Intelligence ("TFI"). Since I was last here ten months ago, TFI has made important strides on anti-money laundering and countering the financing of terrorism ("AML/CFT"), and safeguarding the United States and international financial systems.

Today I would like to take the opportunity to discuss the threats to the U.S. financial system, as well as the approaches that we are taking both in countering threats abroad, in cyber space, and closer to home. I will walk you through the efforts that our team, working closely with our colleagues in the interagency, are tackling.

Threats to the United States Financial System

Russia/Ukraine

At the start of Russia's illegal invasion of Ukraine, President Biden laid out a comprehensive strategy to support Ukraine, which includes making use of the full range of our economic tools. Since then, Treasury has used its authorities to target a broad range of harmful Russian activities, ensuring sustained pressure on the Kremlin and its proxies. This includes the rigorous application of sanctions targeting Russian actors and their financial support networks as they continue to pose a threat to U.S. national security amid their brutal war against Ukraine.

Our Russia sanctions have two core objectives that we continue to pursue, in coordination with the G7: 1) limiting Russia's ability to fund its war by taking steps to restrict its revenues from energy and its access to the global financial system; and 2) restricting Russia's access to items critical to its military-industrial base.

Since February 22, 2022, Treasury's Office of Foreign Assets Control ("OFAC") has issued over 3500 new, and 750 amended sanctions listings. Over 250 new and amended FAQs, 5 executive orders, 5 new and amended Directives and responded to over 7,000 specific licenses or requests for interpretive guidance.

Our actions are forcing the Kremlin to use its limited resources to prop up Russia's economy at a time when they would rather be investing every dollar in their war machine. Combined with

domestic structural and war-related constraints, these efforts are limiting Russia's medium-to-long term economic growth potential.

Restricting Russia's Revenues

We designed the novel price cap policy to pursue seemingly contradictory goals: to maintain a reliable supply of crude oil and petroleum products to global market while reducing the revenues the Russian Federation earns from oil. The price cap, which covers both crude oil and petroleum products of Russian Federation origin, has been achieving these goals—with Russian revenues falling sharply as the Kremlin accepted a significant discount for its oil relative to global prices. Russian oil tax revenue was down nearly 30% in 2023 compared to 2022.

Treasury and our Price Cap Coalition partners have demonstrated resolve to address evasion of the price cap and hold accountable those who attempt to circumvent our sanctions. We have pursued multiple, successive rounds of sanctions against actors who violated the price cap, including shipping companies, vessel owners, and opaque traders, without causing significant oil market volatility.

We are also working diligently to target and enforce sanctions against actors, like those in the so called "Ghost Fleet," choosing to employ these deceptive tactics as a means of circumvention of U.S. sanctions. Through regular engagements and the issuance of an alert on price cap evasion tactics, we have emphasized the importance of monitoring vessel behavior for common and dangerous deceptive shipping practices, doing due diligence to ensure vessels meet appropriate quality and safety standards, and ensuring vessels are adequately covered by insurance in the case of a maritime accident.

Finally, Treasury has also updated its price cap guidance and documentation requirements for industry, implementing changes to strengthen the attestation and recordkeeping processes for certain covered service providers.

These actions have had a measurable effect to support the price cap's credibility by highlighting increased risk associated with shipping above the price cap. At the same time, the discount on Russian oil that the Kremlin has been forced to accept to sell its oil has increased. All the while, we have carefully calibrated our actions to have a significant impact on Russia's ability to finance its illegal war in Ukraine, while also preventing major disruptions to the global oil markets keeping costs stable for everyday Americans.

Combatting Circumvention

One of the ways we know our approach is working is that the Kremlin has been actively seeking ways to circumvent sanctions, tasking its intelligence services with finding ways to get around them and looking to work with international businesses to work with.

In response, we have launched a push to crack down on sanctions evasion and the provision of goods and services for Putin's war machine. On December 22, President Biden issued a new Executive Order, which further targets Russian sanctions evasion and solidifies the U.S.

commitment to the G7 Leaders' Statement, making clear to foreign financial institutions that facilitating significant transactions relating to Russia's military-industrial base may expose them to U.S. sanctions.

Treasury is working closely with the private sector, especially financial institutions, to ensure the effective implementation of U.S. sanctions targeting Russia's unprovoked war in Ukraine, including targeting evasion networks that the Russia regime has created to source components for its military industrial base.

We have also continued to use our authorities to bring together public and private sector stakeholders to combat this threat, hosting a series of FinCEN Exchange events on Russia's sanctions and export control evasion activity alongside our Commerce Bureau of Industry and Security (BIS) colleagues.

Finally, FinCEN co-leads a multilateral group of 19 financial intelligence units (FIUs) focused on combating Russian illicit finance and sanctions evasion. Since its inception following the Russian invasion of Ukraine in February 2022, FinCEN has received hundreds of tips from fellow members, which it has securely disseminated to partners in OFAC and U.S. law enforcement agencies to support their sanctions, enforcement actions, and investigations.

Our actions are leading banks around the world to exercise enhanced due diligence when facilitating payments for dual-use goods or for the benefit of entities suspected of operating in Russia's aerospace, construction, defense, manufacturing, or technology sectors. This will increase the costs we impose on the operation of complex evasion networks that are supporting Russia's war machine and reduce the space in the financial sector for these illicit actors to operate in.

Middle East

While the events of October 7 have caused us to redouble our focus on countering terrorist financing in the Middle East, the Treasury Department has consistently targeted Iran and its proxies for decades. Since 2021, the Biden-Harris Administration has administered 47 separate Iran sanctions rollouts targeting 465 individuals and entities. Seven of these rollouts have targeted Iran's energy sector and include over 160 designations.

We are also targeting with sanctions Iran's procurement of critical parts for its drone and missiles programs, which are directly destabilizing the region and are also enabling Russia's indiscriminate targeting of civilians and aggression in Ukraine. We continue to take disruptive designation actions against Iran's revenue generation activities that it uses to fund its destabilizing regional activities and support of multiple regional proxy groups, including Hamas and Hizballah.

Hamas

Disrupting Hamas's financing operations is not new to us; we have done this work for many years. Treasury is implementing a sustained, global campaign against Hamas financing that includes our full suite of tools, including sanctions designations, public alerts and advisories, the convening of public-private partnerships, and use of our regulatory authorities. Treasury's goal is to ensure that Hamas cannot raise or move funds through the international financial system in support of acts of terror. Since 9/11, the United States has sanctioned numerous Hamas--affiliated individuals and entities across the globe.

Since the October 7th attacks, Treasury has issued five tranches of 45 Hamas-related designations targeting key Hamas terrorist group members, operatives, and financial facilitators. Many of these targets have been involved in Hamas's secret investment portfolio, which we have been targeting since May 2022. We have also targeted sham charities that hold themselves out as legitimate but provide funds to families of Hamas and Palestinian Islamic Jihad (PIJ) terrorists. In effect, the funding serves as a recruiting tool for these groups.

We are also keeping an eye on how these groups are adapting, including using new methods or technologies, to raise and move funds. While we continue to assess that terrorists' use of digital assets remains a small fraction of more established mechanisms to move money, we recognize that terrorist groups have and may continue to turn to digital assets to raise, transfer, and store their illicit proceeds. That is why we are focused on disrupting these groups' ability to leverage digital assets, such as our recent multilateral action against several of Hamas's funds transfer networks that relied on several key exchanges to funnel proceeds to the group. You will continue to see us target Hamas-related financing going forward.

Treasury's actions to designate entities, freeze funds, and exert targeted financial pressure are only the start of our overall strategic work. Disrupting Hamas's international financial networks requires collective action, and to this end we need sustained action from our foreign counterparts. In the wake of Hamas's attack, Treasury reached out to our foreign counterparts to share information and press them to expand their own efforts.

Our outreach to partners in Australia, the G7 and the European Union has led to complementary sanctions actions by Australia, the EU, Japan, and the UK, to designate Hamas-related targets through their own domestic authorities. FinCEN engaged FIU counterparts across the world to enhance and expedite information sharing efforts. This has led to the formation of an international task force of FIUs from Australia, Canada, Estonia, France, Germany, Israel, Liechtenstein, Luxembourg, the Netherlands, New Zealand, Switzerland, the UK, and others, that will enable partners to better work with their respective law enforcement authorities to identify and stop terrorist funding channels.

In October, I traveled to Saudi Arabia for an emergency session of the Terrorist Financing Targeting Center to discuss with our Gulf partners the need to intensify efforts to investigate and prosecute terrorist financing. I also traveled late last year to Qatar, Oman, and Türkiye, as well as the UAE just two weeks ago, to discuss the urgent need for domestic action to freeze

Hamas's funds and to stress the importance of addressing terrorist financing vulnerabilities in their respective jurisdictions.

We are also concerned by the humanitarian crisis in Gaza. The Administration strongly supports the delivery of humanitarian assistance to the Palestinian people, and we want to make clear that U.S. sanctions do not stand in the way of these life-saving efforts. Neither Gaza nor the West Bank are subject to jurisdiction-based sanctions by OFAC. OFAC has authorizations for limited transactions with blocked persons to the extent such dealings are ordinarily incident and necessary to certain humanitarian activity. To ensure that humanitarian organizations adequately understand Treasury's humanitarian general licenses across our sanctions programs, I have hosted five roundtables in the last year and my team regularly engages with the humanitarian sector and financial institutions on these issues.

Houthis

We are closely following the situation in Yemen and are increasingly concerned with the growing number of Houthi attacks against vessels in the Bab al Mandab Strait. We cannot risk further regional escalation and are thus committed to deterring further Houthi aggression and halting the sources of their funding for the weapons which continue to threaten international commerce.

Sanctions have the capacity to disrupt, deter, and prevent actions that undermine U.S. national security - like these acts of terrorism. Cutting off the financial flows that feed terrorism is an important duty of my office. That is why the Administration is designating Ansarallah, also known as the Houthis, as a Specially Designated Global Terrorist ("SDGT") effective on February 16.

At the same time, we recognize the grave humanitarian situation in Yemen. We know that 17 million people are food insecure in the country. And we know that the rate of child malnutrition in Yemen is among the highest in the world. That is why we are also taking actions to mitigate unintended humanitarian impacts on the people of Yemen by adopting new general licenses in the Global Terrorism Sanctions Regulations. The general licenses allow for the provision of agricultural commodities, medicine, and medical devices; telecommunications, mail, and internet-based communications, personal remittances, refined petroleum products in Yemen; and commercial shipments into Yemeni ports and airports, which the people of Yemen rely on for food, medicine, and fuel. We are taking these steps to preserve lifesaving humanitarian aid and commercial trade efforts. In fact, in late January, I met with over 200 humanitarian actors, including representatives of NGOs and international organizations to discuss the forthcoming Ansarallah SDGT designation and respond to questions about Treasury's new general licenses. Treasury continues to meet with key stakeholders, including banks, insurers, and humanitarian aid groups. Our robust outreach also includes commercial shippers, who deliver critical supplies to Yemen to ensure they understand these broad humanitarian carveouts and continue to deliver essential food, medicine, and fuel to the Yemeni people.

China

As Secretary Yellen has stated, our approach to the People’s Republic of China (PRC) in the national security context is clear: we will safeguard our priority interests, along with those of our allies and partners, and will protect human rights. Our aim is to take specific, targeted action where our concerns have been clearly communicated and it becomes necessary to defend our vital national interest, and not to seek competitive economic advantage. Within that frame, TFI is focused on identifying and, where appropriate, taking action to respond to a range of illicit financial risks emanating from the PRC, including trafficking of fentanyl, state-sponsored cyber threats, violations of human rights, and facilitating the evasion of our sanctions. We have and will continue to engage our PRC counterparts directly on these concerns, as we believe the best way to address many of these threats is through direct communication, such as through the recently re-established bilateral Financial and U.S.-China Counternarcotics Working Groups. However, we will continue to take public action when necessary, such as our designation of a large China-based network involved in the manufacturing and distribution of illicit narcotics in October, as well as our designation of two PRC government officials for ongoing serious human rights abuse in Xinjiang in December. TFI will continue to evaluate the illicit finance and national security risks emanating from the PRC, and work diligently across the Department and with our interagency colleagues to address them.

Domestic and other International Efforts

We are continuing to work on the implementation of the important authorities that Congress gave to us in 2020 on a bipartisan basis through the Anti-Money Laundering Act (“AMLA”). The bipartisan Corporate Transparency Act (“CTA”) is vital to closing a massive loophole in the U.S. financial system. Small businesses are the backbone of America’s thriving communities, and allowing anonymous criminal companies to operate within our borders substantially disadvantages law-abiding business owners.

The goal of the CTA is to protect U.S. economic and national security, and we are not interested in hitting America’s small businesses with unnecessary fines, penalties, or burdens. We continue to encourage everyone to comply with their obligations under the law, but we will not be taking “gotcha” enforcement actions against small businesses doing their best to comply.

FinCEN has made tremendous progress in implementing the CTA, from opening the database for filing last month to finalizing the framework for law enforcement and others authorized by the law to access beneficial ownership information (“BOI”). As you know, FinCEN successfully launched its BOI registry on January 1st and in the first week alone, more than 100,000 companies successfully filed their beneficial ownership information.

To minimize the burden on small businesses that need to report BOI, we are working to facilitate several options to file, including the option for reporting companies to work through a service provider that has established connectivity to the reporting platform via an application program interface (“API”) to efficiently submit BOI.

Full implementation of the CTA will be a powerful deterrent and will help ensure that money launderers, tax evaders, criminals, and other illicit actors cannot hide their ill-gotten gains in the United States with anonymity and impunity. The launch of the beneficial ownership registry represents a substantial step forward in our efforts to close what has long been identified as a gap in the United States' AML/CFT regime.

Last week, we published three risk assessments on Money Laundering, Terrorist Financing, and Proliferation Financing. This work highlights the most significant illicit finance threats, vulnerabilities, and risks the United States faces detailing recent significant updates to the U.S. AML/CFT framework and explain changes to the illicit finance risk environment, including the ongoing fentanyl crisis, surge in foreign and domestic terrorist attacks and related financing, increased potency of ransomware attacks, the growth of professional money laundering, and continued digitization of payments and financial services. We hope that both the public and the private sectors can use these updated risk assessments to better understand the current illicit finance environment and inform their own risk mitigation strategies.

Fentanyl

The Treasury Department has long recognized the threat from money laundering linked to drug trafficking. We are key implementers of the President's National Drug Control Strategy ("NDCS"), which identifies counter illicit finance as a critical pillar to degrade and disrupt transnational criminal organizations ("TCOs") that traffic these drugs.

Treasury is pursuing a multi-pronged strategy against these threats that encompasses: (1) understanding risks and mapping TCO financial networks; (2) imposing preventative measures on financial institutions that include reporting suspicious activity, which directly generates lead information for law enforcement; (3) encouraging public-private partnerships to facilitate robust information-sharing, including through an ongoing series of regional FinCEN Exchanges that has included events in San Antonio, Cincinnati, and Los Angeles; (4) using targeted financial sanctions to identify and cut off TCOs, their members, and enablers from the international financial system; (5) closing outstanding regulatory gaps; and (6) working with international partners.

With our interagency partners, Treasury is escalating narcotics sanctions across the global supply chain to prevent the transfer of precursor chemicals and machinery that transnational criminal organizations in Mexico require to produce illicit synthetic opioids for U.S. markets. With our international partners, Treasury is working to strengthen multilateral efforts to combat fentanyl-related financial flows through the North American Drug Dialogue, the result of a commitment made by the heads of government from the United States, Canada, and Mexico at the 2016 North American Leaders Summit and the principal mechanism for our three countries to address current and emerging drug threats in North America.

We are also working to increase our internal Treasury coordination on this issue. In December, Secretary Yellen announced the creation of a Counter Fentanyl Strike Force, co-chaired by IRS Criminal Investigations Chief Jim Lee and myself. The Strike Force will focus on strengthening

the partnership between TFI and IRS-CI by unifying the many existing lines of effort across Treasury. Additionally, the Strike Force will help TFI and IRS-CI enhance information sharing, supporting both law enforcement investigations as well as potential sanctions designations.

Investment Advisers

Yesterday, FinCEN issued a proposed rule to combat illicit finance activity in the investment adviser sector. The exploitation of this sector poses both an illicit finance and national security challenge. We have identified instances where sanctioned persons, corrupt officials, tax evaders, and other criminal actors have used IAs as an entry point to invest in U.S. securities, real estate, and other assets. We have also seen U.S. adversaries use investments, including through venture capital funds, in early-stage companies to access sensitive information and technology held by these companies involving the development of strategic and emerging U.S. technologies, often without detection.

Investment advisers have never been subject to comprehensive AML/CFT regulations in the United States. Right now, there is patchwork AML/CFT coverage in the sector, with certain adviser implementing some AML measures, sometimes based on affiliation with a bank or broker-dealer. This allows legitimate or illicit investors to “shop around” for an adviser who does not need to inquire into their source of wealth. The proposed rule would significantly improve efforts to protect the U.S. financial system, provide highly useful information to law enforcement authorities and national security agencies, and safeguard the investment adviser sector against illicit activity.

In developing this proposed rule, we worked to minimize the potential business burden as much as possible. We’ve been careful to ensure we’re not piling on additional or redundant requirements for investment advisers. We’ve also designed the proposal to be risk-based, meaning the cost of the requirements largely correlates with the size of an investment adviser portfolio, such as the number of customers and transactions, along with the risk level of its advisory activities and customers.

Residential Real Estate Notice of Proposed Rulemaking

Illicit actors undermine the national security of the United States when they launder money through residential real estate. In addition to facilitating illicit activity, this abuse of the real estate market can distort the market, drive up prices, and when left unchecked make it more difficult for law-abiding Americans to buy and sell homes.

Last week, FinCEN issued a proposed rule that would enhance transparency for residential real estate purchases. This proposed rule is designed to shed light on the 20% of residential real estate transfers that do not involve a financial institution that is required to have an AML program. The proposed rule would require reports for residential real estate transfers that are associated with a high risk of money laundering. Purchases of homes by individuals would not be reported, and other exceptions would apply.

The illicit finance risk in the real estate sector has been a focus of the Treasury Department of

years. Treasury first advanced its efforts to prevent the misuse of this sector by issuing Geographic Targeting Orders (GTOs) to collect information about certain residential real estate transactions in the United States. We then issued an advanced notice of proposed rulemaking in December 2021 to gather information from the public on how best to cover this sector. Taking all of this into account, the proposed rule part of the Bank Secrecy Act (“BSA”) that specifically identifies real estate transactions as subject to regulation, but we’ve designed this proposal to minimize unnecessary burdens on the industry. The information to be reported is streamlined, only one form would be filed for any given transfer, and the real estate businesses involved in the closing process would be able to decide who files the form. The resulting reports would be available for use by Treasury, law enforcement, and national security agencies in combatting money laundering through real estate and prosecuting associated crimes.

Both proposed rules meet a key vulnerability identified in our risk assessments as well as in the Administration’s U.S. Strategy on Countering Corruption.

De-Risking

I know that Treasury’s April 2023 De-Risking Strategy has been of great interest to many of you. This strategy reflects the Biden-Harris Administration’s priority to shape a safer, more transparent, and more accessible financial system, while at the same time maintaining a robust framework to protect the U.S. financial system from illicit actors and bolstering national security. Many of these recommendations have a long-time horizon, which may not immediately bear fruit. We are working closely with both domestic and international partners to advance them, and we will continue to engage with interested parties on the Hill and elsewhere, and work together to address specific concerns.

Evolving Threats

Treasury is deeply concerned about the use of virtual assets for all illicit financial activity. We have been working for over a decade on implementing an AML/CFT framework for digital assets that mitigates illicit finance risks while promoting responsible innovation. One key element of this work is assessing illicit finance risks associated with virtual assets.

The recently published risk assessments each have substantive sections on virtual assets. They detail how various threat actors, including ransomware cybercriminals, Democratic People’s Republic of Korea (“DPRK”) cyber actors, scammers, terrorist groups, and other illicit actors misuse virtual assets.

They also outline the vulnerabilities that enable them to use virtual assets to profit from their illicit activity, including jurisdictional arbitrage and financial institutions that fail to comply with their AML/CFT obligations.

Importantly, we have tools to address some of these vulnerabilities, such as using our authorities to hold accountable firms that fail to comply with their Bank Secrecy Act and sanctions obligations. For example, in November, Treasury reached historic settlements for BSA and sanctions violations with the largest virtual asset service provider in the world, Binance.

We also use our tools, sometimes in novel ways, to disrupt illicit actors' ability to use virtual assets. To illustrate, Treasury on October 19, 2023 took a critical step to reduce the anonymity that virtual currency mixing can afford illicit actors, including terrorists and DPRK cyber actors, by finding convertible virtual currency (CVC) mixing within or involving a jurisdiction outside of the United States as a class of transactions of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act, and proposing new reporting requirements for transactions involving mixing. This action seeks to increase transparency in the virtual asset ecosystem and assist U.S. government efforts to mitigate these illicit finance risks by requiring covered financial institutions to report on transactions involving mixing. It builds upon other actions that we have taken at Treasury to address risks related to mixers, including designations of mixers used to launder funds by DPRK cyber actors.

However, to root out illicit finance by players in virtual asset markets and forums, we need additional tools and resources. That is why we are eager to work with Congress to adopt common-sense reforms that update our tools and authorities to match the evolving challenges we face today.

Conclusion

I would like to conclude by thanking the hard-working and committed men and women of TFI. I am proud of the work that we have done this year, but also all that TFI has accomplished over its existence so far – in fact, this year TFI will celebrate its twentieth anniversary. With that, I look forward to your questions.