Testimony of Sigal Mandelker

Under Secretary, Terrorism and Financial Intelligence

U.S. Department of the Treasury

Senate Committee on Banking, Housing, and Urban Affairs

Wednesday, January 17, 2018

Introduction

Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, as the Under Secretary for Treasury's Office of Terrorism and Financial Intelligence (TFI), I am honored to appear before you today to discuss the critical work that TFI does to safeguard the United States and international financial systems.

The offices I lead are tasked with deploying our financial intelligence, expertise, and economic authorities to combat terrorist financing, money laundering, weapons proliferators, rogue regimes, human rights abusers, and other national security threats to the United States and our allies.

In 2004, Congress and the Executive Branch had the tremendous vision to combine under one roof a broad range of powerful economic tools, including sanctions, anti-money laundering (AML) measures, enforcement actions, foreign engagement, intelligence and analysis, and private sector partnerships, among others. We are the only country that combines these economic authorities within one office, which has proven invaluable in combating some of the most serious illicit finance and national security threats we face today.

Terrorist groups such as ISIS, al-Qaida, Hizballah, and others seek to infiltrate the financial system to finance their activities and threaten our national security.

Rogue regimes in Iran, North Korea, and Venezuela continue to assault the integrity of the financial system, including by using deceptive financial practices to advance their corrupt, criminal, or terrorist aspirations. Russia continues to occupy Crimea and destabilize Ukraine, in violation of international norms of sovereignty.

These regimes, and many more, engage in human rights abuses and corruption, putting their own interests above the well-being of their people. That is why we are also targeting human rights abusers and the corrupt through authorities like the Global Magnitsky Human Rights Accountability Act. Simply put, the United States will not allow our financial system to be compromised by human rights abusers and corrupt actors who exploit innocent people around the world.

Transnational criminal organizations, drug kingpins, cyber criminals and others likewise seek out vulnerabilities in the global financial system, including by looking to use emerging technologies such as virtual currencies to launder their ill-gotten gains and advance their malicious enterprises.

These and other malign actors cannot operate without funding. Cutting off their access to the financial system requires calibrating our economic tools in strategic and complementary ways. TFI integrates our authorities and expertise across components, deploying the tools best suited to

each challenge and achieving significant impact. The foundation of our economic authorities is a strong and robust anti-money laundering/combating the financing of terrorism (AML/CFT) regime.

Many of our efforts to identify and disrupt terrorist financiers, weapons proliferators, rogue regimes, and other illicit finance threats depend on financial institutions implementing the laws and regulations designed to protect the financial system. Financial intelligence reported to us by financial institutions serves as a key component of our efforts to target illicit actors.

One of my top priorities as Under Secretary for TFI is to ensure that the AML/CFT framework remains strong and effective. My testimony today will focus on both the threats that we face and the efforts we are undertaking to strengthen the AML/CFT framework in order to counter those challenges.

Threats to Our Financial System

We bring enormous economic power to bear against an array of law enforcement and national security threats. Below are just a few of the challenges we have been combating.

For example, North Korea uses covert representatives as well as front and trade companies to disguise, move, and launder funds that finance its weapons programs. The regime's illicit financial activity is not just conducted in dollars, nor is it limited to a handful of jurisdictions. Once a North Korean trade or financial representative successfully accesses a nation's financial system, illicit funds can flow indirectly through global banks, who may be unwittingly conducting currency clearing operations for North Korea.

We are laser-focused on detecting and disrupting these networks as part of the Administration's strategy to impose maximum pressure on North Korea. We are deploying the full range of our economic authorities to combat the North Korean threat. Treasury has a cadre of analysts, including in the Office of Intelligence and Analysis (OIA) and the Financial Crimes Enforcement Network (FinCEN), who are mapping out these networks so that we can target and disrupt them.

There are now six North Korea-related executive orders, in addition to robust congressional authorities, that we use to target key North Korean financial middlemen and others who support the regime. Over the last year, Treasury's Office of Foreign Assets Control (OFAC) designated over 100 individuals and entities related to North Korea as part of our concerted effort to pressure the regime. Our recent action under Section 311 of the USA PATRIOT Act against Bank of Dandong, a Chinese bank facilitating North Korean money laundering and sanctions evasion, highlights our resolve to target key nodes of financial support for North Korea.

We are also warning financial institutions both here and abroad about the deceitful ways in which North Korea abuses the international financial system. In November 2017, FinCEN issued an advisory to alert financial institutions about North Korea's attempts to use front companies to launder money and evade sanctions. This information helps the private sector detect and report such activity, which in turn supports our efforts to target those persons and entities that help the regime fund its weapons program.

Our focus on depriving North Korea of its ability to earn and move revenue through the international financial system means that we must work with other countries to achieve this goal. Not only do we work bilaterally with key partners to coordinate our domestic sanctions programs, the Secretary, myself, and others within TFI engage with leaders across the world to stress the importance of implementing United Nations Security Council Resolutions (UNSCRs). We also work bilaterally with governments and through the Financial Action Task Force (FATF) and the G7 Financial Experts Group to ensure that countries have the regulatory framework in place to detect and freeze assets linked to North Korea. I raise these concerns in virtually every engagement I have with my foreign counterparts and with many financial institutions, and will do so again in my upcoming trip to Asia next week.

Iran is another rogue regime that seeks to subvert the financial system. It is the leading state sponsor of terrorism and finances terrorist groups such as Hizballah and Hamas, the brutal regime of Bashar al-Assad, and a host of Shi'a militant groups in Bahrain, Iraq, Syria, and Yemen.

Like North Korea, Iran uses deceptive financial practices to generate revenue. As just one example, in November, we sanctioned an Islamic Revolutionary Guards Corps-Qods Force (IRGC-QF) network involved in a large-scale scheme to counterfeit Yemeni bank notes to support its destabilizing activities. This network employed deceptive measures to circumvent European export control restrictions and procured materials to print counterfeit bank notes potentially worth hundreds of millions of dollars.

In addition to Iran's financing of terrorism and other destabilizing activities, the IRGC has an extensive presence in Iran's economy, including in the energy, construction, mining, and defense sectors. In our engagements both here in the United States and abroad, we have made clear that companies doing business in Iran face substantial risks of transacting with the IRGC or IRGC-linked entities.

This risk is heightened by the lack of transparency in the Iranian economy, which is one of the least transparent in the world. Indeed, Iran is on the FATF's blacklist precisely because it has failed to address such systemic deficiencies in its controls to combat terrorist financing and money laundering. This has led the FATF to highlight for the past decade the terrorist financing risk emanating from Iran and the threat that it poses to the international financial system. Thus far, Iran has failed to fulfill its commitments to the FATF in addressing its weak controls.

We will continue to take action to protect the international financial system and to combat Iran's relentless campaign to support terrorism, destabilize the region, and abuse its own people. Over the last two weeks, OFAC designated 19 individuals and entities in connection with serious human rights abuses and censorship in Iran, and for assisting designated Iranian weapons proliferators. As Secretary Mnuchin stated when announcing last week's sanctions, the United States will not stand by while the Iranian regime continues to engage in human rights abuses and injustice.

In Venezuela, the Maduro regime's systematic destruction of democracy, as well as its endemic corruption, also pose a threat to the international financial system. Under Maduro,

embezzlement, graft, and fraud have become the regime's de facto economic policy, aimed at maintaining the loyalty of the security apparatus to keep Maduro and his cronies in power. In August 2017, the President issued an Executive Order carefully calibrated to deny the Maduro dictatorship a critical source of financing to maintain its illegitimate rule and protect the U.S. financial system from complicity in Venezuela's corruption and in the impoverishment of the Venezuelan people, while still allowing for the provision of humanitarian assistance.

In September, FinCEN issued an advisory to alert financial institutions of widespread public corruption in Venezuela and the methods that senior political figures and their associates may use to move and hide proceeds of their ill-gotten gains, at the grave expense of the Venezuelan people. Combined with our powerful sanctions, this advisory put financial institutions on watch for possible illicit fund flows.

Endemic corruption also undermines the U.S. and international financial systems, perpetuating violent conflict and damaging economic markets. In the past year, we have imposed sanctions, issued financial advisories, and undertaken diplomatic engagements to counter corruption across the globe. Building on the Global Magnitsky Act, which Congress passed just over one year ago, the President signed an Executive Order on December 20, 2017, declaring a national emergency with respect to human rights abuses and corruption globally and enabling Treasury to impose financial sanctions on malign actors engaged in these activities.

In this Executive Order, the President imposed sanctions on 13 serious human rights abusers and corrupt actors, and OFAC simultaneously imposed sanctions on an additional 39 affiliated individuals and entities under the newly-issued Order. Since this action, we have seen public reports regarding the notable impact of these sanctions, with some of the designated individuals being cut off from lucrative business arrangements, while others face investigation by their home governments.

TFI has also been deploying its authorities against transnational criminal organizations, fraud, cybercriminals, human trafficking networks, and other law enforcement priorities in which our economic tools have had a meaningful impact. In recent years, for example, we have issued geographic targeting orders (GTOs) aimed at combating tax refund fraud and sophisticated trade-based money laundering schemes orchestrated by drug trafficking networks and their money launderers.

To mitigate the money laundering vulnerabilities associated with luxury real estate, in 2016 we issued GTOs to identify the beneficial owners behind shell companies used to pay all-cash for high-end residential real estate in certain U.S. cities. In 2017, following the enactment of the Countering America's Adversaries through Sanctions Act, FinCEN revised the GTOs to capture a broader range of transactions and include transactions involving wire transfers. The information gathered from the GTOs supports law enforcement and helps inform our broader approach to mitigating the money laundering vulnerabilities in the real estate sector.

Strengthening the AML/CFT Framework

As we employ our economic tools to address these challenges, we must continue to increase the transparency and accountability in the financial system, which underpins much of our economic statecraft. A strong and effective AML/CFT framework keeps illicit actors out of the financial

system, and allows us to track and target those who nonetheless slip through. This framework must address the evolving forms of illicit finance threats that we face.

As such, we are taking a hard look not only at the Bank Secrecy Act (BSA) but also at the broader AML/CFT regime. We need to continuously upgrade and modernize our system – a statutory and regulatory construct originally adopted in the 1970s – and make sure that we have the right framework in place to take us into the 2030s and beyond.

Incentivizing Innovation

In particular, we must make sure that financial institutions are devoting their resources towards high value activities and are encouraged to innovate with new technologies and approaches. In recent years, for example, financial institutions have become more proactive in their AML/CFT approach, in some cases building sophisticated internal financial intelligence units devoted to identifying strategic and cross-cutting financial threats. Financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and machine learning. Institutions are also working together to share information on suspicious activities, enabling them to identify and report activity that would not otherwise be visible or concerning to a single institution.

We laud and encourage these innovations. These initiatives advance the BSA's underlying purpose. We are working closely with our counterparts at the Federal Banking Agencies (FBAs) to discuss ways to further incentivize financial institutions to be innovative in combating financial crime. We have also been speaking with many in the financial community to understand their perspectives.

Public-Private Partnerships

Deploying our tools for maximum impact requires proactive dialogue and information sharing with financial institutions. They are on the front lines, detecting and blocking illicit financing streams, combating financial crimes, and managing risk. The safeguards employed by the private sector, and the information reported about terrorist financiers, weapons proliferators, human rights abusers and traffickers, and cyber and other criminals, help prevent malign actors from abusing our financial system.

Enhancing public-private partnerships that reveal and mitigate vulnerabilities is one of our top priorities. To make these partnerships work, we are arming the private sector with information that enhances their ability to identify and report suspicious activity. We have also been issuing advisories to warn financial institutions about illicit finance risks.

I have heard from my outreach with financial institutions here and abroad how this information helps them better prioritize targets and utilize their limited resources. That is why last month I announced the launch of FinCEN Exchange, a new public-private information sharing program led by FinCEN.

FinCEN Exchange brings financial institutions, FinCEN, and law enforcement together to facilitate greater information sharing between the public and private sectors.

Information sharing should be a two-way street. As part of FinCEN Exchange, we are convening regular briefings – at least once every 6-8 weeks – with law enforcement, FinCEN, and financial institutions to exchange targeted information on priority illicit finance threats. In close coordination with law enforcement, our goal is to provide information to support specific matters through Section 314(a) of the USA PATRIOT Act and other authorities, and also to provide financial institutions with broader typologies to help them identify illicit activity. These types of exchanges enable the private sector to better identify risks and provide FinCEN and law enforcement with critical information to disrupt money laundering and other financial crimes.

I have seen firsthand the immense value of this public-private partnership. Information provided by financial institutions in connection with public-private briefings has helped us map out and target weapons proliferators, sophisticated global money laundering operations, human trafficking and smuggling rings, and corruption and trade-based money laundering networks, among others. This also creates a positive feedback loop in which we can share with the broader financial community the typologies learned from these exchanges, enabling other financial institutions to identify and report similar activity.

Through FinCEN Exchange, we are increasing public-private information sharing, which will include financial institutions of all types and sizes across the country.

We are also discussing BSA reform with the private sector, including in the Bank Secrecy Act Advisory Group (BSAAG). The BSAAG, chaired by FinCEN, is comprised of members from financial institutions, trade groups, and state and Federal regulators and law enforcement. The topics addressed in the BSAAG include identifying metrics for determining effective financial reporting, streamlining the reporting of money laundering "structuring" transactions, and more efficient ways for industry to report cash transactions.

Promoting Information Sharing Among Financial Institutions

Public-private partnerships are even more effective when financial institutions share information with each other. Money launderers are sophisticated. They move across borders and financial institutions, and financial institutions are better able to keep pace and effectively combat them when they communicate with each other.

Some institutions have started forming consortia to share information more dynamically under Section 314(b) of the USA PATRIOT Act, which provides safe harbor for financial institutions to voluntarily share information related to money laundering or terrorist activities. We are highly encouraged by, and supportive of, the private sector's willingness to engage in this type of exchange. By working together, these groups of financial institutions are directly assisting our efforts to identify and disrupt streams of financing for North Korea and other top illicit finance threats.

Evolving Threats

Part of our effort to update the AML/CFT regime includes staying ahead of evolving threats. We lead the world in mitigating the illicit finance risks of emerging technologies, such as the use of

virtual currencies. We stand at the regulatory and supervisory forefront of this emerging industry. Currently, the United States, Japan, and Australia are among the few countries regulating virtual currency payments/exchange activities, including in particular decentralized convertible virtual currency, for AML/CFT purposes.

To ensure that virtual currency providers and exchangers know the rules and follow them, FinCEN has prioritized engagement with – and examination of – these entities, focusing both on the approximately 100 that have registered with FinCEN as money transmitters as required, as well as those that have not. As part of the examination process, FinCEN, working with delegated Internal Revenue Service (IRS) examiners, has recommended virtual currency providers and exchangers take certain actions to improve their compliance activities.

The effectiveness of this structure depends on compliance by the regulated entities, and so we aggressively pursue virtual currency exchangers and others who do not take these obligations seriously. In July 2017, for example, FinCEN assessed a $110 million fine against BTC-e, an Internet-based, foreign-located money transmitter that exchanges fiat currency as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. At the time of our action, it was one of the largest virtual currency exchanges by volume in the world and facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. FinCEN also assessed a fine against Russian national Alexander Vinnik, one of the operators of BTC-e, for his role in the violations.

This action sends a very powerful message that we will hold accountable virtual currency exchangers that violate our AML laws, wherever they are located. We will do so in conjunction with our law enforcement partners and foreign counterparts.

We understand that the EU is finalizing its amendments to its anti-money laundering directive, which will put in place a requirement for EU members to regulate virtual currency exchangers, a significant step. Even with these advancements, there is still a major gap in regulating these entities globally and we are actively engaged with other countries, bilaterally and multilaterally, to encourage them to apply international AML/CFT standards to virtual currency payments.

We also prioritize increasing the transparency of shell companies in the U.S. financial system. To that end, we have strengthened one of the fundamental components of our AML/CFT regime: customer due diligence. Treasury's customer due diligence rule, which takes effect this May, requires covered financial institutions to identify and verify the identity of the beneficial owners of companies at the time of account opening. We look forward to working with Congress on the important issue of enhancing the transparency of beneficial owners.

As we call upon the private sector to enhance its systems, we at TFI are doing the same. Financial intelligence is central to our efforts to combat the national security threats I outlined above. As such, I have directed my staff to work innovatively on employing new tools to analyze and use information more effectively. Last month, I established a Technology Council, which, among other things, is implementing new technologies to further enhance our analytic capabilities.

Conclusion

I am grateful for this Committee's leadership and support, both of which are essential to combating the threats we face and ensuring the continued success of TFI. I look forward to working with this Committee and other Members of Congress as we seek to fulfill our shared responsibility to keep Americans safe and secure. I look forward to your questions.