CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Committee on Financial Services
Subcommittee on National Security, International Development, and Monetary Policy

Schemes and Subversion

How Targets of Sanctions Undermine and Evade Sanctions Regimes

ERIC B. LORBER

Senior Director
Center on Economic and Financial Power
Foundation for Defense of Democracies

Managing Director
K2 Integrity

Washington, DC
June 16, 2021

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

I. Introduction[1]

Chairman Himes, Ranking Member Barr, and distinguished members of the committee, I am honored to appear before you today to discuss how bad actors and foreign governments undermine and evade sanctions regimes.

I come before this committee as an economic sanctions and compliance professional, having worked at the U.S. Department of the Treasury and advised financial institutions, corporations, humanitarian organizations, and individuals on ensuring they operate in compliance with U.S., EU, and UN sanctions obligations. I have spent countless hours studying, assessing, and countering methods by which illicit actors try to evade our sanctions.

My testimony today will focus on the importance of countering sanctions evasion, which can undermine our successful use of these powerful tools of economic statecraft. Indeed, without effective efforts to counter evasion, our sanctions programs are less impactful, less likely to achieve U.S. national security objectives, and more likely to cause pain to innocents. I will provide an overview of the different types of sanctions used by the United States and then discuss the importance of countering efforts to evade these programs. I will then focus on certain key areas of sanctions evasion we have observed in the last few years, including how illicit actors have tried to circumvent our prohibitions, as well as future areas to watch. Finally, I will turn to how best to counter sanctions evasion, and what Congress, the administration, and the private sector can do to detect and disrupt evasion activity.

II. Understanding the Different Types of Sanctions

While the use of economic statecraft to achieve national security and foreign policy objectives is as old as the republic itself, over the last two decades, the United States has increasingly turned to economic sanctions and statecraft as a tool of first resort in addressing critical national security challenges.[2] Over the last four administrations, the Treasury Department, the State Department, and other executive agencies, along with Congress, have significantly increased both the number of countries and illicit actors subject to our sanctions, as well as the sophistication of these tools. In recent years, the United States has used these tools more and more. During the Trump administration, for example, the U.S. government – led by the Treasury Department's Office of Foreign Assets Control (OFAC) – designated more than 1,000 targets per year.[3]

Beyond new targets and ramped-up programs, successive administrations have imposed new and sophisticated types of sanctions to change target state behavior and prevent terrorist organizations, weapons proliferators, corrupt actors, human rights abusers, and many others from accessing the

[1] The views expressed in this testimony are my personal views and do not represent the views of the Foundation for Defense of Democracies, K2 Integrity, or the Treasury Department. Pursuant to legal and ethical obligations, I cannot discuss internal deliberations that occurred during my tenure at the Treasury Department.
[2] Juan Carlos Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York City: PublicAffairs, 2015). (https://www.publicaffairsbooks.com/titles/juan-zarate/treasurys-war/9781610391160)
[3] "2020 Year-End Sanctions Update," *Gibson Dunn*, February 5, 2020. (https://www.gibsondunn.com/wp-content/uploads/2021/02/2020-year-end-sanctions-and-export-controls-update.pdf)

international financial system. The United States now employs a range of sanctions to protect its national security interests, including:

- **Comprehensive Jurisdictional Sanctions.** Often referred to as embargoes, comprehensive sanctions prohibit U.S. persons from broadly transacting with certain countries or territories, often as a means to pressure the regime in that country. The United States currently maintains comprehensive sanctions programs on Iran, Cuba, Syria, and North Korea as well as the Crimean Peninsula.

- **Conduct/List-Based Sanctions.** List-based sanctions focus on individuals and entities engaged in illicit activity such as terrorism, weapons proliferation, drug trafficking, or malicious cyber activity, among many other illicit activities. These persons are added to the Specially Designated Nationals And Blocked Persons (SDN) List, and U.S. persons are required to block their assets. These sanctions are generally imposed to cut these persons off from legitimate financial and business markets.

- **Regime-Based Sanctions.** These are list-based sanctions that target members of current or former regimes engaged in corruption, human rights abuses, or other malign activity. These programs are not full, comprehensive programs but nevertheless target specific regimes. Examples include the U.S. sanctions programs on Libya, Burma, and Zimbabwe.

- **Sectoral Sanctions.** First employed against Russia following its annexation of Crimea and destabilizing activities in eastern Ukraine, sectoral sanctions were developed to impose costs on target companies in situations where designating those companies as SDNs was viewed as too escalatory or to have too many negative collateral consequences. Whereas SDN designations prohibit U.S. persons from engaging in any transaction with the target, sectoral sanctions prohibit *certain* transactions with the target, including prohibitions on transacting in new debt over a certain tenor or equity. The Russia sectoral sanctions program was subsequently expanded pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA). The Trump administration likewise imposed sectoral sanctions in the Venezuela program. Most recently, the Biden administration imposed sectoral sanctions on China when it issued Executive Order 14032, which prohibits U.S. persons from purchasing or selling securities of 59 Chinese companies as well as any person determined to operate in the defense or surveillance technology sectors of the Chinese economy.[4]

- **Secondary Sanctions.** Secondary sanctions extend U.S. coercive leverage to non-U.S. persons who knowingly engage in significant transactions with SDNs or in prohibited sectors (such as Iran's oil or shipping sector). Secondary sanctions authorities threaten persons who engage in such activities with being cut off from U.S. markets (including

[4] Executive Order 14032, "Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China," June 3, 2021. (https://home.treasury.gov/system/files/126/eo_cmic.pdf). For a discussion of these restrictions, see: "Biden Revises Ban on U.S. Investors Buying Certain Chinese Securities," *K2 Integrity*, June 7, 2021. (https://www.k2integrity.com/en/knowledge/policy-alerts/biden-revises-ban-on-us-investors-buying-certain-chinese-securities)

financial markets), among a number of additional penalties. Designed to pressure non-U.S. persons to cease engaging in unwanted activity with adversaries, they are often controversial with allies and partners given their so-called "extraterritorial" nature. Currently, the United States has secondary sanctions authority in the Iran, Syria, North Korea, Russia, terrorism, and Hizballah programs.

- **Non-Sanctions Economic Authorities.** In addition to sanctions, U.S. regulatory and enforcement agencies have a range of economic authorities to protect the international financial system and pressure our adversaries, including USA PATRIOT Act Section 311 identifications of institutions or jurisdictions as primary money laundering concerns; private-sector outreach and guidance through advisories issued by OFAC and Treasury's Financial Crimes Enforcement Network (FinCEN); and robust diplomacy to garner support for coordinated action with our allies and partners.

Important to note here is that these tools are not used in isolation. Congress and the executive branch frequently use overlapping authorities to target particular countries or entities. For example, the U.S. sanctions program on Russia combines a list-based program (such as Executive Orders 13660, 13661, and 14024) targeting particular Russian persons; a comprehensive jurisdictional program targeting Crimea; secondary sanctions for knowingly conducting significant financial transactions with SDNs and in certain sectors of the Russian economy; and sectoral sanctions targeting transactions in new debt or equity of certain Russian companies.

III. The Purpose of Sanctions

That these tools are used with increasing frequency should come as no surprise: They can often seem to be the best possible option from a range of suboptimal choices and can be impactful in a number of ways, including:

1. **Denying Illicit Actors Access to Global Markets and Significantly Degrading Their Capabilities.** A key objective of sanctions is to deny terrorists, human rights abusers, weapons of mass destruction (WMD) proliferators, and others access to global markets in order to make it more difficult for them to engage in malign activity. For example, successive administrations have used targeted sanctions against terrorist organizations and Islamic State leaders to degrade their capabilities and make it more difficult for them to move money and earn illicit revenue. Along with military force, the Obama and Trump administrations' efforts to constrict the Islamic State's access to the international financial system and to global markets greatly constricted the group's ability to finance its operations.[5]

2. **Imposing Economic Pain to Change Behavior.** Another key objective of sanctions policy is to compel targets to change undesirable behavior. The United States routinely uses its broad economic authorities to ramp up costs on the governments of Iran, Russia, North

[5] Assistant Secretary for Terrorist Financing Marshall Billingslea, *Testimony before House Committee on Financial Services Subcommittee on Monetary Policy and Trade*, November 30, 2017. (https://www.treasury.gov/press-center/press-releases/Pages/sm0227.aspx)

Korea, Cuba, and Venezuela to force changes in their behavior. For example, in the Russia context, the United States has used a combination of sectoral, list-based, comprehensive jurisdictional, and secondary sanctions to impose costs on Russian President Vladimir Putin and his cronies for interfering in U.S. elections, annexing Crimea, destabilizing eastern Ukraine, supporting the Assad regime in Syria, and using chemical weapons. In the case of Iran under the Obama administration, sanctions, including those mandated by Congress, are widely credited with pressuring Iran to come to the negotiating table to discuss its nuclear program, leading to the Joint Comprehensive Plan of Action (JCPOA).

3. **Deterring Unwanted Activities.** A third key purpose of employing sanctions is deterrence. Congress and the executive branch have made clear that sanctions can serve as a key deterrent against malign activities.[6] In the case of Russia, for example, United States in April imposed sanctions and threatened further sanctions to, among other objectives, deter Moscow from engaging in additional destabilizing activities, including aggressive cyber activities and election interference.[7] While deterrence is always difficult to measure, there was some evidence to suggest that previous sanctions on Russia in 2014 did create a deterrent impact. At the time of Russia's annexation of Crimea and invasion in eastern Ukraine, it was reportedly planning on increasing the scope of its overt military support in order to wrestle key cities and territories away from Ukrainian government control, but thought twice after biting sectoral sanctions took effect.[8]

IV. The Importance of Countering Sanctions Evasion

While sanctions can be a powerful tool for achieving U.S. foreign policy objectives, our adversaries are continually developing and implementing strategies and tactics to blunt their impacts. These adversaries use a range of sanctions evasion techniques – many of which rely on obfuscation and opacity – to surreptitiously move funds and goods across the world, frustrating the impact of U.S. sanctions programs. Countering these efforts is critical to ensuring that U.S. sanctions remain effective in pressuring terrorist organizations, rogue regimes, human rights abusers, and the corrupt.

Indeed, sanctioned regimes have developed sophisticated evasion techniques that undermine the impact of economic pressure. For example, in the case of North Korea, the Kim regime has relied

[6] The 2015 National Security Strategy notes that U.S. "use of targeted sanctions and other coercive measures are meant not only to uphold international norms, but to deter severe threats to stability and order at the regional level." The White House, "National Security Strategy," February 2015, page 23. (https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf)

[7] "Biden Ramps Up Russia Sanctions Pressure," *K2 Integrity*, April 19, 2021. (https://www.k2integrity.com/en/knowledge/policy-alerts/biden-ramps-up-russia-sanctions-pressure)

[8] See, for example: Nigel Gould-Davies, "Sanctions on Russia Are Working: Why It's Important to Keep Up the Pressure," *Foreign Affairs*, August 22, 2018. (https://www.foreignaffairs.com/articles/russian-federation/2018-08-22/sanctions-russia-are-working). See also: Eric Lorber, "Assessing U.S Sanctions on Russia: Next Steps," *Testimony Before Senate Banking, Housing, and Urban Affairs Committee*, March 15, 2017. (https://www.banking.senate.gov/imo/media/doc/Lorber%20Testimony%203-15-17.pdf)

on a range of evasion tactics, including deceptive shipping practices, the use of front[9] and shell[10] companies to access the global financial system, and state-sponsored cyberattacks on financial institutions and cryptocurrency exchanges, to counter one of the most restrictive sanctions regimes in the world.[11] Using these multifaceted and complex evasion efforts, the regime has successfully resisted the global pressure campaign aimed at forcing Pyongyang to give up its nuclear weapons.

Detecting and disrupting sanctions evasion is often a game of cat and mouse. Financial institutions, the intelligence community, law enforcement, and others try to detect efforts by North Korea, Iran, or Hizballah to mask their true identifies through the use of front or shell companies, renamed vessels, anonymous digital assets, or a range of other methods. Oftentimes, these schemes are detected and disrupted.[12]

But sanctions evaders have certain significant advantages. First, they choose the time and place of the evasion attempt. For example, in the case of North Korea, the Kim regime has used many different front and shell companies to try and access global financial markets.[13] While certain front and shell companies are identified and shut down by law enforcement or have their efforts thwarted by financial institutions, the North Koreans can simply set up new front organizations to try to illicitly access markets using different financial institutions or different routes. In effect, the financial system and those trying to prevent sanctions evasion have to cover a wide range of possible vulnerabilities, while sanctions evaders can pick and choose how they try to infiltrate the system.

Second, and relatedly, it is often inexpensive and easy to set up evasion mechanisms. For example, establishing a front company in Singapore or Hong Kong does not require a significant investment – often just a paper registration and an address that is home to hundreds of such companies. If these front companies are engaged in illicit activity and are detected and shut down, it can be

[9] Front companies are functioning businesses that combine illicit proceeds with earnings from legitimate operations, obscuring the source, ownership, and control of the illegal funds. U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Updated Advisory on Widespread Public Corruption in Venezuela," May 3, 2019. (https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf)

[10] Shell companies are typically non-publicly traded corporations or limited liability companies that have no physical presence beyond a mailing address and generate little to no independent economic value. See: U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018. (https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf)

[11] See, for example, UN Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)," S/2021/211, March 4, 2021. (https://undocs.org/S/2021/211). See also: James Byrne, Joseph Byrne, Lucas Kuo, and Lauren Sung, "Black Gold: Exposing North Korea's Oil Procurement Networks," *Royal United Services Institute and C4ADS*, 2021. (https://c4ads.org/black-gold)

[12] See, for example: U.S. Department of the Treasury, Press Release, "Treasury Targets Iran's Central Bank Governor and an Iraqi Bank Moving Millions of Dollars for IRGC-Qods Force," May 15, 2018. (https://home.treasury.gov/news/press-releases/sm0385)

[13] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)

straightforward and inexpensive to establish another front company or series of front companies in a matter of days or weeks.

V. How U.S. Adversaries Evade Our Sanctions

While U.S. adversaries have developed myriad approaches for evading sanctions, over the last few years the U.S. government has focused on a number of key circumvention methods, including in the maritime, financial, and cryptocurrency sectors. As discussed above however, even in situations where authorities generally understand the high-level of evasion risks, illicit actors are always innovating and finding new ways to get around our sanctions regimes.

At its core, sanctions evasion is about hiding the identity of the sanctioned parties involved. Many companies and individuals understand that they are prohibited from conducting transactions with sanctioned persons or in sanctioned jurisdictions and face significant risks for doing so. As a result, sanctions evaders undertake substantial efforts to hide their identities and, in doing so, are able to surreptitiously access global markets.[14]

a. Maritime Sanctions Evasion

Shipping has been described by a former senior U.S. government official as a "key artery to evade sanctions."[15] As 90 percent of global trade involves maritime transportation, sanctioned individuals and jurisdictions are constantly seeking ways to exploit the global supply chain and adapt to new restrictions.[16] As of 2019, the total value of annual world shipping trade has reached more than $14 trillion,[17] and the global commercial fleet maintains over 100,000 vessels.[18]

Since 2018, OFAC has put a spotlight on the growing use of deceptive tactics in the shipping industry by issuing maritime-related advisories, aggressively sanctioning persons in the maritime

[14] Note that this description of sanctions evasion does not include efforts by U.S. adversaries – and in some cases partners and allies – to insulate themselves from U.S. sanctions pressure. For example, following the U.S. withdrawal from participation in the JCPOA, certain European countries established the Instrument in Support of Trade Exchanges (INSTEX), a special purpose vehicle designed to facilitate trade with Iran. INSTEX was designed to create a trade channel between European countries and Iran that the United States would not sanction, but it was not an effort to evade U.S. sanctions through obfuscation or deception. Likewise, potential Chinese efforts to establish a People's Central Bank of China-backed digital currency that could serve as an international medium of exchange – thus limiting exposure to the U.S. dollar and, by extension, U.S. sanctions pressure – likewise does not rely on deception. Rather, these methods are more straightforward approaches to blunting the impact of U.S. sanctions.

[15] Jonathan Saul, "U.S. sets sights on shipping companies for sanctions evasions," *Reuters*, November 6, 2019. (https://www.reuters.com/article/us-shipping-usa-sanctions/u-s-sets-sights-on-shipping-companies-for-sanctions-evasions-idUSKBN1XG2CH)

[16] U.S. Department of Commerce, National Oceanic and Atmospheric Administration, Office for Coastal Management, "Fast Facts: Ports," accessed June 11, 2021. (https://coast.noaa.gov/states/fast-facts/ports.html)

[17] "Shipping and world trade: driving prosperity," *International Chamber of Shipping*, accessed June 11, 2021. (https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-driving-prosperity/#:~:text=For%20an%20economic%20region%20such,than%2014%20trillion%20US%20Dollars)

[18] Michael Horwitz, "Revealing risk through insights into ship-to-ship cargo transfers," *Windward*, accessed June 11, 2021. Revealing risks through insights into ship-to-ship cargo transfers, Windward. (https://www.wnwd.com/blog/identifying-risk-through-ship-to-ship-cargo-insights)

sector, and engaging with stakeholders in the maritime sector to ensure they understand their due diligence obligations.

Tactics deployed by sanctions evaders often include:

- Frequent changes to the names of vessels;
- Frequent changes to vessel ownership and management;
- Utilizing large barges and bulk-carrier vessels to reduce the number of ship-to-ship transfers;
- Disabling or manipulating a vessel's automatic identification systems (AIS);
- Ship-to-ship transfers;
- Voyage irregularities;
- False flags and flag hopping;
- Falsifying cargo and vessel documents;
- Physically altering vessel identification; and
- Complex ownership or management.

Such tactics can be seen through the well-known *Grace 1* case. In July 2019, Gibraltar authorities seized the *Grace 1*, a Panamanian-flagged oil tanker, for breaching international sanctions. The *Grace 1* was carrying 2.1 million barrels of Iranian crude oil to Syria. The vessel was impounded for 43 days, and the U.S. Department of Justice (DOJ) issued a seizure warrant and forfeiture complaint against the vessel and cargo.[19]

DOJ alleged that several front companies owned, operated, and managed the *Grace 1*, but that it was ultimately controlled by the Islamic Revolutionary Guards Corps (IRGC) and was used to conceal Iranian oil sales and transport. Between 2018 and 2019, the vessel would deactivate its AIS to load petroleum in Iranian ports and offload it in different locations, including by engaging in ship-to-ship transfers with vessels that previously engaged with Syrian ports. The complaint also described fraudulent documents and the use of multiple companies as intermediaries to obfuscate the participation of sanctioned Iranian persons and to circumvent U.S. sanctions on the Iranian energy sector. The seizure of the vessel highlighted the scope of sanctions evasion in the global shipping industry and challenges of enforcement.

As part of its efforts to disrupt sanctions evasion in the maritime sector, OFAC, along with the State Department and the Coast Guard, issued a global maritime sanctions advisory in 2020 that set compliance expectations for a range of actors operating in the shipping sector.[20] This advisory catalyzed compliance efforts in the sector, particularly by shipping companies, insurance companies, and port managers and operators, to significantly bolster their sanctions compliance programs.

---

[19] Verified Complaint for Forfeiture in Rem, *United States v. Oil Tanker – "GRACE l" (IMO 9116412), et al.*, 1:19-cv-1989-(JEB) (D.D.C., filed August 16, 2019). (https://www.justice.gov/opa/press-release/file/1196361/download)
[20] U.S. Department of the Treasury, U.S. Department of State, and U.S. Coast Guard, Advisory, "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities," May 14, 2020. (https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf)

But even now we are seeing innovative methods by illicit actors in the maritime sector to evade U.S. sanctions and move illicit cargo. For example, recent vessel tracking has revealed new, anomalous behavior that suggests sanctions evaders in the maritime sector are adopting new approaches to avoid detection. For example, earlier this year, the Cyrus-flagged oil tanker *Berlina* was transmitting its location near the Caribbean island of Dominica when, according to vessel tracking information, it stopped and within two minutes turned 180 degrees (likely impossible for a ship of its size). In addition, while the vessel's transponder indicated that it was in the Caribbean, around the same time it was spotted physically loading crude oil near Venezuela. This could be representative of a new sanctions-evasion approach and could be "one of the first instances of orchestrated manipulation in which vessels went dark for an extended period while off-ship agents used distant computers to transmit false locations."[21]

As the United States and its allies and partners aim to cut off sanctions evasion in the maritime sector, we can expect illicit actors to adopt new and sophisticated approaches to avoid these restrictions.

b. Financial Obfuscation

The U.S. dollar continues to play a large role in the global economy: About half of all international trade is invoiced in U.S. dollars. The dollar is involved in nearly 90 percent of all transactions in foreign exchange markets and comprises approximately 61 percent of global central bank reserves.[22] Even our adversaries under sanctions seek dollars to settle their transactions and need access to the U.S. financial system to settle dollar-denominated transactions. To do so, they use a number of financial obfuscation tactics and approaches to evade U.S. sanctions and access the U.S. financial system or sensitive U.S. goods. These tactics include using complex networks of businesses to layer illicit payments, with the goal of making transactions appear legitimate and obscuring the true originator, beneficiary, and purpose of the transactions. Two of our adversaries, in particular, make extensive use of these tactics: North Korea and Iran.

North Korea

North Korea relies on elaborate networks to circumvent U.S. and UN sanctions and to gain indirect access to the financial system and procure critical goods in support of its WMD program.[23] State-owned enterprises and banks use front and shell companies located abroad and a network of bank representatives and embassy personnel to conceal the true beneficiaries of transactions. According

[21] "Tanker's impossible voyage signals new sanction evasion ploy," *The Spokesman-Review*, May 28, 2021. (https://www.spokesman.com/stories/2021/may/28/tankers-impossible-voyage-signals-new-sanction-eva)
[22] Rebecca M. Nelson, James K. Jackson, and Martin A. Weiss, "The U.S. Dollar as the World's Reserve Currency," *Congressional Research Service*, December 18, 2020, page 1. (https://crsreports.congress.gov/product/pdf/IF/IF11707)
[23] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017, page 3. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)

to a 2021 report by the UN Panel of Experts on North Korea, Pyongyang also relies on corporate service providers in third countries to facilitate its sanctions evasion activities.[24]

One example of a typical North Korean sanctions-evasion practice is the export of coal to China-based companies,[25] which then send small payments to front, shell, or trading companies in Asia or in offshore jurisdictions. These companies will then sell the coal to other markets and use the proceeds to purchase goods on behalf of North Korea. In addition to selling coal, North Korean front companies often use companies in the shipping, import/export, textile, garment, fishery, and seafood sectors to conduct their business.

To obscure these front companies' ties to North Korea, North Korean diplomatic personnel and other overseas representatives establish bank accounts in foreign countries and set up front companies in jurisdictions with lax corporate registration practices. These companies will frequently share the same business registration address as other front companies, and different front companies with a shared address may make several payments to the same beneficiary.[26]

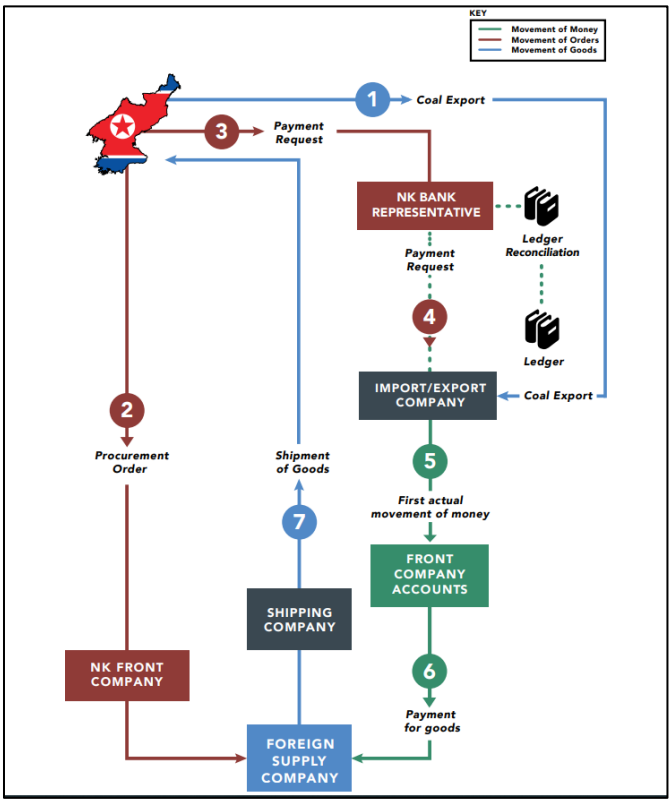
A recently unsealed 2018 DOJ indictment against a North Korean individual and his network of front companies for circumventing North Korea sanctions provides a case in point.[27] The indictment highlights the steps taken by the network to conceal its ties to North Korea, including the use of front companies by North Korean banks to process payments; using third-party companies to make payments; using bank accounts not in their own name; removing references to North Korea from wire transactions and transaction documents; and listing false end destinations on shipping documents that did not reference North Korea.[28]

Other countries help North Korea evade U.S. and UN sanctions as well, notably Russia and China. Between 2017 and 2018, a Russian financial services company, Russian Financial Society, helped North Korea access the international financial system by opening bank accounts for a North Korean company owned or controlled by the U.S.- and UN-designated Foreign Trade Bank (FTB).[29] As a result, North Korea gained access to the global financial system to generate revenue for its nuclear program. China similarly appears to assist – or at least tacitly condone – North Korean efforts to access the broader financial system. For instance, the 2021 UN Panel of Experts

---

[24] UN Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)," S/2021/211, March 4, 2021, page 418. (https://undocs.org/S/2021/211)
[25] Michael R. Gordon, "Covert Chinese Trade With North Korea Moves Into the Open," *The Wall Street Journal*, December 7, 2020. (https://www.wsj.com/articles/covert-chinese-trade-with-north-korea-moves-into-the-open-11607345372)
[26] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017, page 7. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)
[27] U.S. Department of Justice, Press Release, "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," March 22, 2021. (https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses)
[28] Indictment, *United States of America v. Mun Chol Myong*, 1:19-cr-00147-RC (D.D.C. filed March 22, 2021), page 9. (https://www.justice.gov/opa/press-release/file/1379211/download)
[29] U.S. Department of the Treasury, Press Releases, "Treasury Designates Russian Financial Institution Supporting North Korean Sanctions Evasion," June 19, 2019. (https://home.treasury.gov/news/press-releases/sm712).

report notes that FTB appears to continue to operate China-based accounts despite Beijing's claims to the contrary.[30]



Source: Financial Crimes Enforcement Network[31]

Iran

Central Bank of Iran Officials

Iran's regime has used a global network of front, shell, and trading companies[32] to gain access to the financial system to generate revenue and move money to support its malign activities, including human rights abuses, support for terrorist groups, and ballistic missile development. Notably, Iran has used senior officials of the Central Bank of Iran (CBI) and regional financial institutions to acquire hard currency and to conduct transactions in support of the Islamic Revolutionary Guards

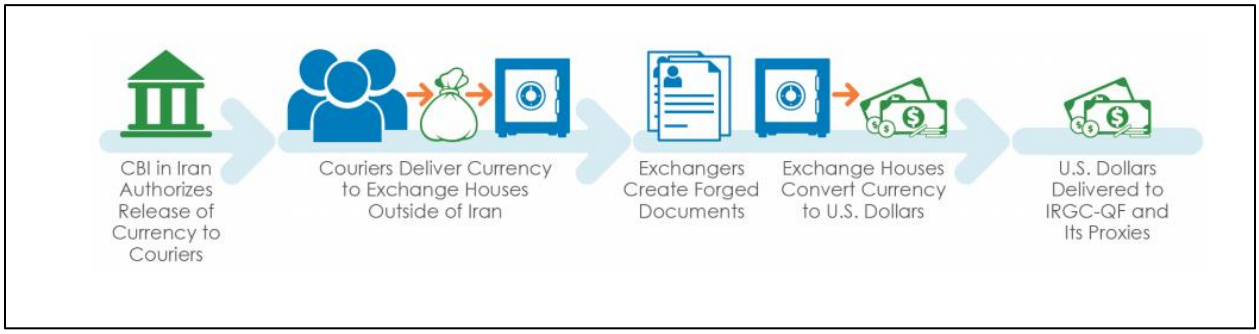
[30] United Nations Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)," March 4, 2021, (https://undocs.org/S/2021/211), p. 52.
[31] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on North Korea's Use of the International Financial System," November 2, 2017, page 4. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)
[32] Trading companies are entities that are not licensed to transmit funds but that in practice operate as exchange houses and rely upon their bank accounts to transmit funds on behalf of third parties. See: U.S. Department of the Treasury, Office of Foreign Assets Control, "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran," *Iranian Transactions and Sanctions Regulations*, January 10, 2013, page 1. (https://home.treasury.gov/system/files/126/20130110_iran_advisory_exchange_house.pdf)

Corps Qods Force (IRGC-QF), as demonstrated by the U.S. Treasury Department's May 2018 designation of the CBI governor.[33]

The IRGC-QF is also known to use front companies to retrieve funds from foreign bank accounts held by the CBI. In one documented case, the IRGC-QF used a front company it controlled to receive millions of dollars in transfers from the CBI.[34]

Currency Exchange Houses

Iran also uses currency exchange houses[35] in third countries and trading companies to hide the origin of funds and to procure U.S. dollars. For instance, in May 2018, the United States and the United Arab Emirates disrupted a currency exchange network operating in the United Arab Emirates that procured and transferred millions in dollar-denominated bulk cash to the IRGC-QF. To do so, this network established three front companies and forged documents to mask their true purpose of funding the Iranian regime.[36] Front companies and individuals and entities involved in this type of scheme will also seek to mask Iranian involvement by omitting Iranian addresses and names of companies and individuals from key documents and will use multiple exchange houses to avoid scrutiny.



Source: Financial Crimes Enforcement Network[37]

[33] U.S. Department of the Treasury, Press Release, "Treasury Targets Iran's Central Bank Governor and an Iraqi Bank Moving Millions of Dollars for IRGC-Qods Force," May 15, 2018. (https://home.treasury.gov/news/press-releases/sm0385)

[34] U.S. Department of the Treasury, Press Release, "Treasury Designates Vast Network of IRGC-QF Officials and Front Companies in Iraq, Iran," March 26, 2020. (https://home.treasury.gov/news/press-releases/sm957)

[35] Third-country exchange houses are financial institutions licensed to conduct foreign exchange and transmit funds on behalf of individuals and companies.
U.S. Department of the Treasury, Office of Foreign Assets Control, "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran," *Iranian Transactions and Sanctions Regulations*, January 10, 2013, page 1.
(https://home.treasury.gov/system/files/126/20130110_iran_advisory_exchange_house.pdf)

[36] U.S. Department of the Treasury, Press Release, "United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF," May 10, 2018.
(https://home.treasury.gov/news/press-releases/sm0383)

[37] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018, page 3.
(https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf)

Procuring Sensitive Goods

Iran also uses front and trading companies to skirt sanctions that would otherwise prevent it from acquiring sensitive goods or services, including dual-use equipment to aid its ballistic missile development goals and commercial aviation equipment to maintain its aviation industry. Iran has also used trading companies to gain access to critical U.S. and foreign-made inputs needed to further its missile development program.

One prominent example of Iran's use of these companies was revealed by Treasury's February 2017 action targeting a series of networks that used trading companies and intermediaries to procure dual-use and other goods for the regime in Iran. To obscure the true nature of these fund transfers, members of one targeted network used a group of China-based brokers and companies to assist in the procurement of dual-use goods for the ultimate benefit of the Iranian regime. In this scheme, the China-based brokers and companies would purchase dual-use goods from other suppliers based in China and arrange shipment of those goods to Iran in exchange for financial compensation.[38]

c. The Use of Cryptocurrency

Terrorist organizations and rogue regimes have likewise used different types of cryptocurrency to evade U.S. sanctions and finance their activities. While cryptocurrencies – and the blockchain on which they are often based – can provide a significant degree of transparency and the ability to trace and seize illicit funds transfers,[39] certain cryptocurrencies provide a degree of anonymity that can be exploited by terrorist organizations and rogue regimes. In recent months, we have seen a range of ways in which malign actors have exploited cryptocurrencies to evade sanctions.

Terrorist organizations have aggressively used cryptocurrencies to receive donations and evade sanctions. For example, in 2020, DOJ disrupted three separate campaigns by the al-Qassam Brigades, Hamas' military wing; al-Qaeda; and Islamic State. According to DOJ,

> In the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps. The al-Qassam Brigades boasted that bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor.[40]

[38] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Supporters of Iran's Ballistic Missile Program and Iran's Islamic Revolutionary Guard Corps – Qods Force," February 3, 2017. (https://www.treasury.gov/press-center/press-releases/Pages/as0004.aspx)
[39] David Uberti, "How the FBI Got Colonial Pipeline's Ransom Money Back," *The Wall Street Journal*, June 11, 2021. (https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981)
[40] U.S. Department of Justice, Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," August 13, 2020. (https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns)

Likewise, according to DOJ, al-Qaeda "operated a bitcoin money laundering network using Telegram channels and other social media platforms to solicit cryptocurrency donations to further their terrorist goals. In some instances, they purported to act as charities when, in fact, they were openly and explicitly soliciting funds for violent terrorist attacks."[41]

During and after the conflict between Israel and Hamas in late spring 2021, Hamas apparently received a significant uptick in donations in the form of bitcoin. According to a senior Hamas official, the group saw "a surge in cryptocurrency donations since the start of the armed conflict with Israel" last month, "exploiting a trend in online fundraising that has enabled it to circumvent international sanctions to fund its military operations."[42]

Likewise, Iran may be using bitcoin mining to circumvent sanctions. Despite the primary and secondary sanctions that prohibit or make sanctionable almost all activity in the Iranian energy sector, Iran has turned to bitcoin mining as one way to mitigate the impact of the restrictions on its oil sector. According to the cryptocurrency diligence firm Elliptic, up to 4.5 percent of worldwide bitcoin mining may take place in Iran.[43] While Iran cannot easily export its energy products because of the sanctions maintained by the United States, persons in Iran can use Iranian energy products to mine bitcoin, which is an energy-intensive process.[44]

Mining bitcoin provides a way for Iranians to earn revenue, and it is estimated that the amount of bitcoin mined in Iran could equal approximately $1 billion annually.[45] Iranian think tanks have recognized the potential for sanctions evasion, noting that bitcoin may not be traceable and can be used on international exchanges.[46] This extensive bitcoin mining raises clear compliance questions, including how bitcoin mined in Iran and inserted into international cryptocurrency markets can be identified or potentially overlooked by entities operating in these markets. Recent press reporting also suggests that Iran has cracked down on bitcoin mining in the country, in part because the extensive energy needs of mining have led to blackouts across the country.[47]

In addition, state actors such as North Korea have engaged in hacking operations of virtual currency exchanges to steal cryptocurrency. For example, in March 2020, DOJ charged two Chinese nationals with laundering over $100 million worth of cryptocurrency from a hacked

---

[41] Ibid.
[42] Benoit Faucon, Ian Talley, and Summer Said, "Israel-Gaza Conflict Spurs Bitcoin Donations to Hamas," *The Wall Street Journal*, June 2, 2020. (https://www.wsj.com/articles/israel-gaza-conflict-spurs-bitcoin-donations-to-hamas-11622633400)
[43] Tom Robinson, "How Iran Uses Bitcoin Mining to Evade Sanctions and 'Export' Millions of Barrels of Oil," *Elliptic*, May 21, 2021. (https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions)
[44] Ibid. China has reportedly established significant bitcoin mining farms in Iran.
[45] Ibid.
[46] Behnam Gholipour, "Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions," *IranWire*, March 2, 2021. (https://iranwire.com/en/features/9084)
[47] Shivam Vahia, "Iran is planning to introduce a legal framework for crypto even as Bitcoin mining activity remains restricted," Business Insider, June 10, 2021. (https://www.businessinsider.in/cryptocurrency/news/iran-is-planning-to-introduce-a-legal-framework-for-crypto-even-as-bitcoin-mining-activity-remains-restricted/articleshow/83396588.cms)

cryptocurrency exchange for the ultimate benefit of the North Korean regime.[48] The funds were then laundered through hundreds of automated cryptocurrency transactions aimed at preventing law enforcement from tracing the funds. The individuals circumvented compliance controls by submitting doctored photographs and falsified identification documentation, utilizing over 100 virtual currency accounts and addresses, and transferring over $1 million into prepaid iTunes gift cards.

One emerging area of concern in the cryptocurrency and blockchain space relates to decentralized financial products and services, known as DeFi. DeFi is a blockchain-based set of products and services that facilitates transactions directly between parties without the use of a centralized financial intermediary.

In many cryptocurrency transactions, the transaction will be intermediated by an exchange. In such a situation, the exchange likely has compliance obligations, including to ensure that the transacting parties are not sanctioned persons. Decentralized financial products do not rely on such an intermediary. Instead, individuals can buy and sell financial products directly with one another through smart contracts. Usually created by software developers, such smart contracts can trigger transactions when certain conditions obtain – for example, when the price for a certain cryptocurrency reaches a particular threshold. They generally allow people to lend or borrow funds from others, trade cryptocurrencies, and engage in a wide range of additional financial transactions.

Such decentralized products and services pose significant sanctions-compliance challenges. For example, determining whether a party to a particular one-to-one transaction is a sanctioned person may be complex, though this challenge could be mitigated depending on the transparency requirements specified in the smart contract or in the community governing its terms. Likewise, DeFi may pose risks that sanctioned parties are able to transact and receive items of value without their counterparties knowing that they are sanctioned or even being aware that they may be prohibited from transacting with such persons. (For example, an individual conducting a transaction may not understand that he or she cannot transact with a sanctioned person.) As a result, there may be significant risks that sanctioned parties can use these products and services to evade sanctions.

The nature of decentralized finance poses particular challenges to the effectiveness of U.S. sanctions programs and the Treasury Department's ability to extend its reach far beyond its resources. Treasury has a long history of focusing its regulations and enforcement actions on key gatekeepers in certain industries. For example, by ensuring that financial institutions understand and take their sanctions-compliance obligations seriously, Treasury can leverage its resources more effectively to root out illicit actors in the financial system. Likewise, in the case of the shipping industry, the Treasury and State departments focus on deputizing companies in this sector to target international trade prohibited under U.S. sanctions. Treasury and State do not have the resources to effectively regulate global financial transactions and commerce, but by ensuring that

[48] U.S. Department of Justice, Press Release, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack," March 2, 2020. (https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack)

key gatekeepers must comply with U.S. sanctions laws and regulations, they can have a far-outsized impact.

With centralized cryptocurrency exchanges, Treasury will likely continue to focus on their role as a key gatekeeper in this ecosystem and push to ensure they have effective sanctions-compliance programs in place (through a combination of guidance and enforcement activity). However, with DeFi, no clear gatekeeper exists. Indeed, in many ways, that is the impetus behind the creation and rise of DeFi products. This means that Treasury may need to find new and innovative ways to ensure that sanctioned parties do not attempt to widely exploit DeFi.

VI. Effectively Blunting Sanctions Evasion Requires a Defense-in-Depth Approach

The U.S. government, its allies and partners, and the private sector must adopt a multilayered, "defense-in-depth" approach to effectively counter sanctions evasion. Each layer of defense decreases the chances that a terrorist organization or rogue regime can access to global markets. And while each layer may not be foolproof, together they can pose a formidable obstacle. Elements of this defense-in-depth approach include:

- *Effective Intelligence Collection*. Key to effectively countering sanctions evasion activity is the ability to detect such activity in the first instance. The Treasury Department's Office of Intelligence and Analysis (OIA), along with other members of the intelligence community, as well as FinCEN, should be provided the tools necessary to identify sanctions evasion. A legislative proposal under consideration by this committee, the OFAC Fusion Center Act, could help achieve this. The law would create an interagency group designed to share data and allow for better detection and disruption of illicit networks, including sanctions evaders. While an OFAC Fusion Center may have broader responsibilities and authorities, the intelligence-collection component should be a major element. Note that Treasury has previously worked on related initiatives in sanctions program-specific contexts.

- *Aggressive Designation Activity*. OFAC should continue to aggressively target sanctions evaders. In particular, OFAC should focus on targeting financial facilitators of evasion activity as well as entire evasion networks. For example, in the North Korea context, OFAC has sanctioned over 40 North Korean, Russian, Chinese, Singaporean, Burmese, and Thai financial facilitators who have helped the North Korean regime launder funds. The facilitator plays one of the most valuable roles for the North Korean regime: providing access to the global economy. The North Korean regime has a hard time finding third-country nationals they can trust to handle all its illicit needs. Exposing and sanctioning these individuals cuts the regime's access and obstructs the flow of funds.

In addition, targeting entire networks can be an effective approach for disrupting evasion activity.[49] For example, last year OFAC acted against an Iranian-Venezuelan network by designating the network's shipping companies, vessels, and vessel captains for delivering gasoline to Venezuela.[50] Although it may have appeared to be a routine designation, this was a landmark action, as OFAC had not previously targeted vessel captains. This action signaled to the maritime community that OFAC will hold all parties responsible and is willing to act against entire networks that facilitate sanctions evasion, not just the shipping companies themselves. This increased the incentives for compliance across the industry. The more that OFAC can designate entire networks, the less likely persons in those networks will be to engage in sanctions evasion in the future.

- *Providing the Private Sector With the Right Tools*. A critical element in the fight against sanctions evasion is ensuring that the private sector has the right tools to identify and disrupt such activity. As discussed, Treasury does not have the resources to monitor the full scope of global financial and trade transactions. In recent years, Treasury and the U.S. government more broadly have tried to arm the private sector with information on sanction-evasion tactics and red flags that can help companies spot sanctions evasion. Combined with clearly signaling to the private sector their compliance obligations and pursuing aggressive enforcement actions against those who fail to comply, this additional information can help the private sector more effectively counter evasion activity.

  In recent years, Treasury, State, and other agencies have provided the private sector with a substantial amount of information in the form of a range of advisories focused on Iranian,[51] North Korean,[52] Venezuelan,[53] and Syrian[54] sanctions-evasion tactics, as well as broader advisories focused on sanctions evasion in particular sectors.[55] This

[49] Under Secretary of the Treasury for Terrorism and Financial Intelligence, *Speech Delivered at the Center for Strategic and International Studies*, July 31, 2019. (https://home.treasury.gov/news/press-releases/sm748)
[50] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Five Iranian Captains Who Delivered Gasoline to the Maduro Regime in Venezuela," June 24, 2020. (https://home.treasury.gov/news/press-releases/sm1043)
[51] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018. (https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf)
[52] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)
[53] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Updated Advisory on Widespread Public Corruption in Venezuela," May 3, 2019. (https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf)
[54] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "OFAC Advisory to the Maritime Petroleum Shipping Community," November 20, 2018. (https://home.treasury.gov/system/files/126/syria_shipping_advisory_11202018.pdf)
[55] See, for example: U.S. Department of the Treasury, U.S. Department of State, and U.S. Coast Guard, Advisory, "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities," May 14, 2020. (https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf)

administration should continue and expand on this approach. To that end, the potential creation of an OFAC Exchange designed to help provide the private sector with information on illicit activity, red flags, and trends[56] could be an effective way to supplement the information provided to the private sector on sanctions evasion methods and typologies.

- *Identifying and Tackling Emerging Areas of Risk*. Critical to ensuring that our adversaries are not able to exploit new technologies and products is identifying and addressing the sanctions risks those technologies and products may pose. For some time, Treasury has been focused on the risks (and opportunities) presented by cryptocurrencies and digital assets more broadly. However, as certain products and services that present significant sanctions risks are more widely adopted, Treasury should clearly communicate its compliance expectations to the broader cryptocurrency community. Likewise, to the extent possible, it should identify relevant gatekeepers within the community to try to enlist as partners in combating sanctions-evasion activity.

- *Internationalizing the Fight*. Financial integrity – and the ability to effectively detect, disrupt, and deter sanctions evasion – is often only as strong as its weakest link. For example, if sanctions evaders and other illicit actors can set up front and shell companies in other jurisdictions and use those companies to access the U.S. financial system or other important financial systems, our efforts at countering sanctions evasion will be significantly hampered. While the United States has done a good job in recent years of pushing the financial integrity mission in conjunction with its allies and partners and in multilateral fora such as the Financial Action Task Force, our efforts to promote sanctions compliance abroad through the development and implementation of key standards and jurisdictional authorities to address these issues remain incomplete.

VII. Conclusion

To ensure that our sanctions programs remain effective and help us achieve national security objectives, Congress, the administration, and the private sector must all work together to help identify, disrupt, and deter sanctions evasion. While this is a challenging task, an approach that emphasizes aggressive designations, clear communication to the private sector regarding compliance obligations and red flags, and efforts to ensure regulations and guidance effectively address risks with new and innovative products and services will best position the United States to continue to have effective and powerful sanctions tools.

I look forward to your questions and thank you again for the opportunity to testify.

[56] Note that the OFAC Exchange could mirror the approach taken by the FinCEN exchange. U.S. Department of the Treasury, Financial Crimes Enforcement Network, Press Release, "FinCEN Launches 'FinCEN Exchange' to Enhance Public-Private Information Sharing," December 4, 2017. (https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing)