NATIONAL PROLIFERATION FINANCING RISK ASSESSMENT

2018

INTRODUCTION

The *National Proliferation Financing Risk Assessment* (NPFRA) identifies, discusses, and ultimately assesses the proliferation financing (PF) risks that the United States currently faces. This assessment seeks to identify and explore the PF threats and vulnerabilities faced by the United States, outline current efforts to address these threats and vulnerabilities, and understand the remaining, or residual, PF risk to the U.S. financial system and U.S. national security. The NPFRA, in conjunction with the 2018 National Money Laundering Risk Assessment (NMLRA) and 2018 National Terrorist Financing Risk Assessment (NTFRA), together provide an overview of the current illicit finance risks to the United States.

Weapons of mass destruction (WMD) and their associated delivery systems present a key national security threat to the United States, and the U.S. government (USG) has made it a top priority to combat the global proliferation of these dangerous weapons. The financing of WMD proliferation remains a central enabling activity of threat actors to achieve their nefarious ends, sometimes through attempts to exploit the U.S. financial system. Accordingly, the USG seeks to use the full capabilities at its disposal to counter this activity through a combination of robust laws, regulations, and other mechanisms meant to track and control WMD components and related materials; operational, investigative, and targeting authorities capable of disrupting the efforts of bad actors; and outreach and engagement to key stakeholders, both within and outside the United States to develop awareness, strengthen collective capacity, and build partnerships to address this unique threat.

Given the size of the U.S. financial system and the role that the U.S. plays in global trade and commerce, as well as the sophistication of U.S. technologies and industry in key areas related to WMD, the United States remains highly susceptible to exploitation by PF networks. In particular, the role that the U.S. dollar plays as a key global reserve currency and the subsequent role that U.S. financial institutions (FIs) play in processing U.S. dollar-denominated transactions globally, means that bad actors—including weapons proliferators—will often have to interact with the U.S. financial system at some point to achieve their ends, whether they want to or not.

In order to provide a depiction of PF risk in the United States, this assessment primarily draws from the work of USG counter-proliferation efforts, including information provided by U.S. law enforcement and intelligence agencies, but focuses on the financing aspects in these efforts to detect, disrupt, prevent, and deter proliferation activity. In order to provide context to these efforts, the NPFRA examines the financing methods used by known proliferation and procurement networks in a number of key cases principally derived from federal prosecutions, asset forfeiture actions, or publicly available targeting actions, including sanctions. Finally, after a discussion of threats, vulnerabilities, and current USG efforts, the NPFRA assesses residual PF risk currently facing the United States.

SCOPE AND DEFINITIONS

It is important to establish at the outset that this assessment discusses a global challenge but assesses how that challenge affects the United States. Further, in order to provide context of the current threat environment, this assessment will briefly discuss issues related to WMD proliferation, including the broader international framework in place to address this key

challenge; however, the focus of this assessment is *the financing* of WMD proliferation, and therefore the analysis of the threats and vulnerabilities will focus on the financial aspects unique to this challenge.

U.S. Nexus

It has long been the general consensus of the international community that the proliferation of WMD constitutes a grave threat to international peace and security.[1] The corollary threat posed by the procurement, including the financing, of these weapons by non-state actors such as terrorist groups and rogue regimes alike is also well-established in international law.[2] While proliferation and proliferation financing are both global phenomena that occur across international borders, utilize multiple entities and individuals from different countries, and seek to exploit gaps in international and national frameworks designed to prevent such activity, this assessment will focus on the PF risk borne by the United States and will not endeavor to analyze threat actors and vulnerabilities that do not have a U.S. nexus. In other words, this will not be an assessment of the PF risks facing other countries or feature a discussion about risks which are broadly applicable at a global level. Any discussion of foreign threat actors or external exploitation of vulnerabilities of the U.S. system will focus on how these elements contribute to the PF risk faced specifically by the United States.

WMD Proliferation vs. WMD Proliferation Financing

It is also essential to distinguish between the threat posed by WMD and their associated delivery systems from the *financing* of this activity, the latter being the focus of this assessment. While current USG strategy and efforts to combat the proliferation of WMD and their delivery systems help to inform the context and threat perspective for this assessment (and naturally include aspects of counter-proliferation financing strategy and tactics), this risk assessment will focus exclusively on the specific type of illicit finance that enables proliferation activity to occur.

It should be noted that a commonly accepted definition of "proliferation financing" has eluded relevant international regimes and fora for some time. The Financial Action Task Force (FATF)—the international standard-setting body for anti-money laundering (AML), countering the financing of terrorism (CFT), and countering the financing of proliferation (CPF)—has yet to officially define PF, although a 2010 FATF report by a project team comprised of international experts put forward the following working definition:

- **Proliferation financing** refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related

[1] The first United Nations (UN) General Assembly Resolution ever adopted on January 24, 1946 established a "Commission to Deal with the Problems Raised by the Discovery of Atomic Energy." This Commission was charged with making proposals to the UN "for the elimination from national armaments of atomic weapons and of all other major weapons adaptable to mass destruction." Since then, the United Nations Security Council (UNSC) has adopted a number of binding resolutions under Chapter VII of the UN Charter, including UNSCR 1540 (2004), which is aimed at preventing non-state actors from acquiring WMD and delivery systems, and a number of other resolutions targeted at the destabilizing, WMD-related activities of specific states, including Iran and North Korea.
[2] See UNSCR 1540 and multiple Iran and North Korea-focused UNSCRs.

> materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.[3]

Further, it is important to recognize the essential role that both international counter-proliferation frameworks and national export control systems play in the broader efforts to combat proliferation activity. The United States maintains its own robust national export control system, administered primarily by the Department of Commerce and the Department of State; fulfills its international obligations under various UN Security Council Resolutions (UNSCRs), including UNSCR 1540, which is the first UNSCR to universalize export controls as a mandatory requirement for Member States as well as to require that countries establish appropriate laws and regulations to address the financing of proliferation-sensitive materials; and is party to, or a member of, a number of other international treaties, agreements, and organizations, including the Nuclear Non-Proliferation Treaty (NPT), the Biological and Toxin Weapons Convention, the Chemical Weapons Convention, the International Atomic Energy Agency, the Nuclear Suppliers Group, the Missile Technology Control Regime, the Wassenaar Arrangement, and the Australia Group.

This robust and overlapping counter-proliferation framework has necessary and important links to efforts to detect and combat proliferation financing: the framework established by export control regimes and authorities helps to identify essential information that can be used to understand how a PF network operates. Similarly, export control and law enforcement authorities have noted the essential role of financial information in detecting export violations involving proliferation-sensitive goods and technology. However, for the purposes of this risk assessment, the functioning of the U.S. export control regime, including observations related to the movement of sensitive goods into and out of the United States, will serve primarily to provide context for a more specific discussion of PF threat actors, the illicit financial methods these persons and entities employ, as well as the vulnerabilities in the U.S. financial system these actors seek to exploit.

METHODOLOGY

As in the 2018 NMLRA and NTFRA, the terminology and methodology of the NPFRA is based on the guidance of the FATF, which presents a process for conducting a risk assessment at the national level.[4] Even though this guidance is primarily focused on conducting ML and TF risk assessments, it also provides a solid foundation and general principles on which to base a PF assessment.[5]

---

[3] FATF, *Combating Proliferation Financing: A Status Report on Policy Development and Consultation,* Feb. 2010, p. 5.

[4] See the following FATF guidance and published reports: *Proliferation Financing Report ("Typologies Report")* (2008); *Combating Proliferation Financing: A Status Report on Policy Development and Consultation* (2010); *Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction* (2018); and *Guidance on National Money Laundering and Terrorist Financing Risk Assessment* (2013).

[5] The FATF notes in its 2013 *Guidance on National Money Laundering and Terrorist Financing Risk Assessment* that "while FATF Recommendation 1 does not create specific risk assessment obligations regarding the financing of proliferation of weapons of mass destruction, the general principles laid out in this guidance could also be used in conducting a risk assessment for this area."

- **Threat:** A threat is a person or group of people, or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the PF context, this principally includes proliferation support networks, many of which depend upon key facilitators and individuals acting for, or on behalf of, state-sponsored weapons programs or sanctioned entities.[6] These individuals and entities seek to exploit the U.S. financial system to move funds that will either be used: (1) to directly acquire WMD or delivery systems or their components; or (2) ultimately in the furtherance or development of state-sponsored weapons programs. Proliferation support networks therefore use the international financial system to carry out transactions and business deals, often acting through illicit intermediaries, front companies and illegal trade brokers. These procurement networks have become significantly more complex over time, increasing the probability that the true end-users of proliferation-sensitive goods will avoid detection. FIs are generally unwitting actors in proliferation-related transactions.

- **Vulnerability:** A vulnerability is something that can be exploited to facilitate PF. A vulnerability may relate to a specific financial product or service used to move funds, or a weakness in regulation, supervision, or enforcement, or reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity. In the context of this risk assessment, it is important to distinguish a procurement vulnerability, which relates more to export controls of sensitive or dual-use materials, from how the procurement is actually financed. However, the degree to which threat actors exploit vulnerabilities related to the financing of such procurement will be a focus of this assessment, as will efforts by proliferation financing networks to raise funds in support of WMD programs.

- **Consequence:** It is generally recognized that the instability, potentially catastrophic loss of life, and damage to critical infrastructure posed by the use of WMD is one of the gravest threats to international peace and security facing the world. With regard to PF, however, it is difficult to evaluate the relative significance of one method over another and not all PF methods have equal consequences. It is not necessarily the method that allows for the greatest amount of money to be raised or moved that presents the highest potential consequence. However, it is generally impossible to distinguish the relative consequence of a given individual procurement from general activities meant to support a broader WMD or missile program in a country of proliferation concern. Therefore, for the purposes of this assessment, greater focus will be on analyzing threats and vulnerabilities as the most clearly distinguishable characteristics of WMD PF risk.[7]

---

[6] This assessment primarily focuses on the threat posed by state-sponsored proliferation support networks, considering these are the primary threat actors that have been found to attempt exploitation of the U.S. financial system. While the threat of non-state actors such as terrorist organizations acquiring WMD is a persistent concern for U.S. authorities, from a financing perspective within the United States, an interagency review of threat actors did not return results to support evidence of explicit exploitation of the U.S. financial system by non-state actors' to acquire WMD. While terrorist groups are often cited as the most likely and most concerning non-state actor group to seek a WMD capability, from an illicit finance perspective, the 2015 NTFRA and its 2018 update provides a more in depth analysis of the financing threat posed by terrorist groups to the United States.

[7] As noted in the FATF Guidance, given the challenges in determining or estimating the consequences, countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. Therefore, this NPFRA focuses on threats and vulnerabilities in determining residual PF risks.

- **Risk:** Risk is a function of threat, vulnerability, and consequence.

Throughout the NPFRA, potential PF threats, vulnerabilities and residual risks were identified, analyzed, and evaluated in the following manner:

- Using the 2017 National Security Strategy (NSS) and congressional testimony from senior USG officials, including 2017 testimony by the Director of National Intelligence (DNI), identifying the WMD proliferation threats that the U.S. government has determined pose the most significant threat to the United States and cross-referencing those threats with any instances where the United States and its financial system were involved;
- Cataloging the PF methods disclosed in criminal investigations, prosecutions, as well as relevant asset forfeiture cases and violations of U.S. sanctions for supporting individuals and entities designated for their support of WMD proliferation activities;
- Analyzing FI reporting and cross-referencing with law enforcement WMD proliferation-related investigations and/or U.S. sanctions designations;
- Comparing the above information with intelligence reporting to validate or refute the information;
- Assessing the extent to which domestic laws and regulations, law enforcement investigations and prosecutions, regulatory supervision and enforcement activity, and international outreach and coordination mitigate identified PF threats and vulnerabilities; and
- Using the aforementioned research and analysis to identify residual PF risks facing the United States.

PARTICIPANTS

The National PF Risk Assessment was drafted by Treasury's Office of Terrorist Financing and Financial Crimes (TFFC). In preparing the NPFRA, TFFC consulted with the following offices and agencies:

- Department of the Treasury
  - Office of Terrorism and Financial Intelligence (TFI)
    - Financial Crimes Enforcement Network (FinCEN)
    - Office of Foreign Assets Control (OFAC)
    - Office of Intelligence and Analysis (OIA)
- Department of Justice (DOJ)
  - Criminal Division (CRM)
    - Money Laundering and Asset Recovery Section (MLARS)
  - National Security Division (NSD)
    - Counterintelligence and Export Control Section (CES)

        - Office of Law and Policy
    - Federal Bureau of Investigation (FBI)
        - Counterproliferation Center (CPC)
            - Weapons of Mass Destruction Directorate (WMDD)
            - Counterintelligence Division
            - Directorate of Intelligence
- Department of Commerce (DOC)
    - Bureau of Industry and Security (BIS)
- Department of Homeland Security (DHS
    - Countering Weapons of Mass Destruction Office
    - Office of Policy
    - U.S. Immigration and Customs Enforcement (ICE)
        - Homeland Security Investigations (HIS)
    - Office of Intelligence and Analysis (I&A)
- Department of State (DOS)
    - Bureau of International Security and Nonproliferation (ISN)
    - Bureau of Economic and Business Affairs (EB)
- Federal Functional Regulators (FFRs)[8]
- National Defense University (NDU)
- Office of the Director of National Intelligence (ODNI)
    - National Counterproliferation Center (NCPC)

SOURCES

The NPFRA utilizes a wide variety of USG and non-USG analysis, guidance, advisories, reports, data sets, speeches, and testimony focusing on WMD proliferation and proliferation financing issues. Chief non-USG sources included analysis by academic institutions and think tanks, as well as reporting by international organizations, such as the United Nations (UN). The main USG source material, which focused chiefly on procurement and financing elements of WMD proliferation activity with a U.S. nexus, was derived from the following sources:

[8] For this assessment, staff from the following agencies were consulted: Board of Governors of the Federal Reserve System (FRB), Commodity Futures Trading Commission (CFTC), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC).

- A review of relevant Bank Secrecy Act (BSA) reporting from the private sector, including internal reports produced by FinCEN on potential PF-related Suspicious Activity Reports (SARs) filed by the private sector;
- U.S. sanctions designations related to WMD activity and relevant source material to support these cases;
- Export control violation cases where a financing element related to WMD was present;
- Publicly-available law enforcement documents relating to criminal cases, including smuggling, money laundering, and counterespionage cases with a WMD or WMD-related sanctions violations nexus; and
- Civil and criminal asset forfeiture complaints related to PF.

Further, the conclusions reached by a review and analysis of these sources was also validated by classified intelligence reporting, analysis, and subject matter expert review. Although this supporting review and underlying documentation cannot be made public, the risk assessment has endeavored to capture declassified aspects of activity broadly indicative of PF in order to provide a comprehensive assessment.

SECTION 1. PROLIFERATION FINANCING THREATS

A thorough analysis of the PF risks facing the United States today first requires identifying the threat actors posing the most significant WMD proliferation threats to the United States and the primary ways their activities are financed. In the PF context, proliferation support networks acting clandestinely to support state-sponsored weapons programs pose the most persistent threat to the U.S. financial system. These networks vary widely in size and sophistication, but are often working on behalf of entities sanctioned by the United States or for countries facing more stringent U.S. export controls for military or dual-use technologies. They all employ tradecraft meant to mask their illicit activity and their tactics share many commonalities with traditional money laundering methods, including the use of front and shell companies to obfuscate the source and/or purpose of funds.

These threat actors seek to exploit vulnerabilities in the global financial system and their activities most frequently intersect with the U.S. financial system in two principal ways: 1) attempts to acquire sensitive or controlled technologies from U.S. firms, which will almost always involve use of U.S. FIs and transactions denominated in U.S. dollars; and 2) attempts to move or transfer funds denominated in U.S. dollars, whether or not the final "destination" of those funds is within the United States and which generally results in U.S. FIs having to "clear" or facilitate these transactions.

This section will provide an overview of the principal state-sponsored WMD proliferation threats and discuss the extent to which these threat actors utilize the United States to facilitate the financing for these weapons programs, including a discussion of the methods and tactics used to carry out PF-related activity. This section will also examine USG efforts to detect and combat this activity through a series of illustrative case examples for each threat actor and will conclude with an overview of these efforts.

OVERVIEW OF THE WMD PROLIFERATION FINANCING THREAT FACING THE UNITED STATES

The threat posed by the proliferation and potential use of WMD is well-articulated at the highest levels of the U.S. government. The 2017 NSS, for instance, notes that "the danger from hostile state and non-state actors who are trying to acquire nuclear, chemical, radiological, and biological weapons is increasing" and that "we will deny revenue to terrorists, WMD proliferators, and other illicit actors in order to constrain their ability to use and move funds to support hostile acts and operations."[9] The unclassified "Worldwide Threat Assessment" released by the U.S. intelligence community annually, has consistently identified WMD and their proliferation as a key "global threat" to U.S national security. The Worldwide Threat Assessment notes that, "state efforts to modernize, develop, or acquire [WMD], their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies" and highlights six country-specific threats emanating from

[9] The White House, *National Security Strategy* – December 2017, p.11.

North Korea, Iran, Syria, China, Russia, and Pakistan, as well as the threat posed by the Islamic State of Iraq and Syria (ISIS).[10] [11]

The Worldwide Threat Assessment provides a useful benchmark for understanding the general national security threat posed to U.S. interests globally by WMD proliferation and potential use. Noting the priority threat actors identified—all state-level weapons programs, except for the example of ISIS using chemical weapons in Iraq and Syria—this risk assessment will overlay these threats with illicit finance information implicating the U.S. financial system, then analyze that information to better understand how procurement and financing networks have sought to aid these threat actors. This information will form the basis for the PF threat and vulnerability assessments, two key components of overall PF risk.

THREAT ACTORS, METHODS UTILIZED, AND RELEVANT CASES

Democratic People's Republic of Korea (DPRK)

Although U.S. and international sanctions have significantly hampered North Korean PF schemes, the North Korean government continues to adapt and use creative methods to access the international, and in many cases the U.S., financial system. The entities involved in these schemes range from state-owned entities and FIs in North Korea, to brokers, agents, banking representatives, and even diplomats based in third countries. These entities generally establish and utilize a complex and long-standing network of front and shell companies outside of North Korea or use other aliases to mask the origin and/or true purpose of the funds. They use these covers to establish multiple bank accounts in foreign jurisdictions and use the international banking system to generate funds and facilitate transactions for supplies benefitting the regime and its weapons programs While much of this activity takes place in foreign jurisdictions and involves non-U.S. persons, given the importance of the U.S. dollar and U.S. financial system to international trade and finance, these financial transactions are often processed through U.S. banks, which are generally unwitting and face complications in identifying the underlying illicit actors with the information available to them.

One of the principal challenges in mapping the PF threat emanating from the DPRK is not only that the North Korean regime uses a variety of deceptive practices to finance its WMD and ballistic missile programs, but also that a large amount of North Korean illicit financial activity transiting the U.S. financial system tends to look like traditional money laundering or smuggling schemes that, at first blush, may not have an obvious connection with the DPRK's WMD program. For example, in a number of cases where U.S. authorities have uncovered North Korean PF networks, the financial facilitators working on behalf of Pyongyang were not attempting to directly acquire sensitive or dual-use goods that can be utilized for weapons development purposes, but rather were engaging in elaborate schemes to evade U.S. and

[10] Worldwide Threat Assessment, pp. 7-8.

[11] As noted previously, this assessment primarily focuses on the threat posed by state-sponsored proliferation support networks, considering these are the primary threat actors that have been found to attempt exploitation of the U.S. financial system. For a more in depth analysis of the financing threat posed by terrorist groups to the United States, please see the 2018 NTFRA.

international sanctions to raise funds that can be used to fund the country's illicit weapons programs.

This fundraising element, rather than strict procurement of WMD-related components, is somewhat unique to North Korean, and to some extent Iranian, PF networks and differs from other threat actors' PF tactics identified in this assessment. This distinction can be attributed to two principal and interrelated factors.

First, the DPRK is a totalitarian state where the government controls all means of production and commerce and focuses its resources almost entirely on its military and weapons programs to the detriment of its own economic development and welfare of its people. The UNSC has made this point in several resolutions.[12] For example, UNSCR 2397, adopted in December 2017, notes that "the DPRK continues to develop nuclear weapons and ballistic missiles by diverting critically needed resources away from the people in the DPRK at tremendous cost when they have great unmet needs."[13] The U.S. government has consistently supported this position for a number of years through a variety of public actions, including through economic sanctions targeting this activity, in public remarks by senior officials, and in established case law where the United States has taken legal action against DPRK's illicit financial networks.[14] For example, in *United States of America v. Dandong Chengtai Trading Limited, et al*., a civil asset forfeiture complaint against a DPRK PF network that had sought to evade U.S. sanctions and launder funds through the U.S. financial system via the sale of North Korean coal, sworn testimony from a North Korean defector with "firsthand knowledge" of key DPRK state organs noted that, "Kim Jong-un puts over 95% of North Korea's foreign currency earnings generated from coal exports toward the advancement of North Korea's military, nuclear missiles, and other weapons programs."[15] [16]

Second, due to the regime's increasingly destabilizing behavior over the past few years and a gradual recognition that Pyongyang's weapons programs are expensive and would be difficult to support without significant financial resources, the international community has greatly expanded the global sanctions regime targeting North Korea. For instance, since North Korea's first nuclear test in October 2006, the UNSC has adopted ten resolutions—six of which came in 2016 and 2017—aimed at restricting the country's financial and operational capabilities that support its WMD, ballistic missile, and conventional weapons programs that continue to threaten international peace and security.[17] The UNSCRs include the imposition of both targeted and sectoral sanctions that focus on key facilitators and sources of revenue for the regime, but have

[12] See UNSCRs 2270 (March 2016), 2321 (November 2016), 2356 (June 2017), 2371 (August 2017), 2375 (September 2017), and 2397 (December 2017).
[13] UNSCR 2397, preambular paragraph 4.
[14] For example, in Sept. 2017, Under Secretary of the Treasury for Terrorism and Financial Intelligence Sigal Mandelker testified before the Senate Banking Committee that, "any revenue that North Korea generates can be used to support, directly or indirectly, its weapons development programs" and that, "a key part of [Treasury's] strategy to suffocate North Korea financially is to target the regime's most profitable industries, including coal, exportation of overseas labor, and the sale of weapons and other goods."
[15] *U.S. v. Funds Associated with Dandong Chengtai Trading Limited, et al.* (Civil Asset Forfeiture Complaint), p. 18, available at https://www.justice.gov/usao-dc/press-release/file/992451/download
[16] The March 2018 report from UN Panel of Experts (PoE) notes that the DPRK generated at least $177 million in revenue from the export of prohibited commodities between January and September 2017, and the PoE notes that figure could actually be much higher. See https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/reports
[17] UNSCRs 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017), and 2397 (2017).

also increasingly served to enshrine a broader recognition that DPRK governmental bodies beyond those most closely associated with the military and illicit weapons programs must be targeted to dissuade the regime from continuing its destabilizing behavior. For example, the UN sanctions now target sectors such as coal, iron ore, fisheries, and even "exports" of forced labor,[18] but also allow member states to freeze the assets of any entities of the Government of the DPRK or ruling Worker's Party of Korea if the state determines those entities have engaged in UNSCR-prohibited activities.[19]

Therefore, even in the sanctions evasion cases involving DPRK PF networks where facilitators are not procuring specific WMD and missile-related components and may be engaging in activities that appear to be more akin to money laundering, there is broad international consensus that these fundraising and/or fund moving activities are being leveraged for the benefit of Pyongyang's illicit weapons programs and are thus PF-related.

Methods Used and Patterns Identified

Given the significance of the U.S. dollar and U.S. FIs in global trade and finance, individuals acting for, or on behalf of, the DPRK have attempted to use the U.S. financial system to facilitate proliferation-related activity in a number of ways. There have been select cases in recent years where these illicit actors have sought to acquire sensitive or dual-use goods from the United States and have attempted to use the U.S. financial system to facilitate this activity. However, the majority of recent DPRK-related PF cases involving a U.S. nexus generally involve activities much broader than individual procurements of WMD technology and focus on sophisticated trade-based schemes designed to raise and move money and acquire a number of diverse commodities on behalf of the regime.

While recent cases demonstrate slight variances, these schemes generally follow a consistent pattern that starts with a key non-North Korean financial facilitator, who has established a non-North Korean trading company, acting as the central point of contact to fulfill commodity orders (both buy and sell side) on behalf of the DPRK.[20] Often these facilitators will import natural resources from the DPRK and sell them on the global market to generate funds, some of which will be used to fulfill import orders from DPRK entities. Other times, a complex, "dual-ledgering" system is used where DPRK entities have directly credited facilitators' accounts at branches/representative offices of North Korean banks in other jurisdictions, where the facilitator would simply keep track of payments and orders made on behalf of their North Korean clients and settle multiple accounts internally, including with unwitting suppliers, without having to involve additional wire transfers between North Korea and other jurisdictions. In this way, the facilitator essentially functions as a "cut out," allowing a DPRK entity to operate as an entity of another nationality in global commerce and in its ability to access the global financial system, and as a result generally takes a commission or charges a hefty mark-up for trades executed on behalf of the DPRK.

In order to evade authorities and unwitting trading counterparties, these facilitators establish complex networks of front and/or shell companies in jurisdictions spread out throughout the

[18] See UNSCRs 2321 (2016), 2371 (2017), and 2375 (2017).
[19] UNSCR 2270 (2016), OP 32.
[20] Most recent case examples have involved Chinese individuals and companies, often based near the North Korean border.

world, but often in places with active off-shore financial centers or areas with lax corporate registration laws. These fronts/shells, in turn, establish bank accounts which allow them access to the global banking system through normal correspondent banking ties. (This is the primary entry point into the U.S. financial system, as almost all transactions involving U.S. dollars must use a U.S. FI to settle the transaction).

Rather than directly paying an entity located in the DPRK, the facilitators will generally divide funds received by DPRK entities, or earned through the sale of DPRK-origin commodities, into smaller outflows directed to these front/shell companies in a complex layering scheme. The front or shell companies then use the received payments to purchase commodities from suppliers all over the world which would eventually reach the DPRK through a series of complex and masked shipping arrangements.[21]

In a November 2017 advisory to U.S. FIs, FinCEN elaborated on these schemes by describing how this activity transects the U.S. financial system and highlighted a number of "red flags" potentially indicative of DPRK deceptive practices and PF schemes, including:[22]

- **Geography:** Many North Korean front or shell companies, banking and financial representatives, and corporate service providers used by the North Korean government are based in China and/or use Chinese banks to facilitate the movement of illicit funds on behalf of the North Korean government. In particular, many of the corporate registration and business addresses for companies tied to North Korea have been shown to be registered in Liaoning province, China—specifically in the municipalities of Dalian, Dandong, Jinzhou, and Shenyang—which borders the DPRK, or in Hong Kong, a major financial center with a variety of corporate service providers. Liaoning province also appears to be a major banking hub for North Korean-related financing, and FinCEN has observed correspondent account transactions conducted by, or on behalf of, Liaoning-based banks. Finally, North Korea's network of overseas financial representatives have been observed to operate in Liaoning province and in Hong Kong, where they establish front and shell companies and set up and operate bank accounts on behalf of these companies. These representatives may appear as a corporate officer of multiple, seemingly unrelated, front or shell companies that also often transact with each other. They are typically North Korean-born and often use Chinese aliases or Chinese facilitators, and they may also appear as authorized signers for accounts maintained by the front or shell companies.

- **Surge Activity Cycles:** Facilitators working on behalf of the DPRK use and deposit funds through seemingly unrelated companies that share the same address. These companies are usually "cycled," or used for a short period of time before being retired. However, associated bank accounts may stay open during lengthy periods of inactivity. Financial activity transacted through these companies can often occur in cycles, whereby one company (Company A) will pay a common beneficiary for a period of time and then cease payments. Once Company A ceases making payments, a different

[21] Feb. 2017 and Sept. 2017 UN PoE reports and FinCEN DPRK Advisory of Nov. 2017. See https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/reports

[22] FinCEN Advisory FIN-2017-A008: "Advisory on North Korea's Use of the International Financial System," 2 Nov. 2017, available at https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf

company (Company B, which shares an address with Company A), pays the same beneficiary.

- **Common Front Companies and Supporting Indicators:** Shipping and import/export businesses are often employed to facilitate illicit North Korean activity and textile, garment, fishery, and seafood businesses are also frequently listed as the business lines for various front companies. In addition to sharing the same physical business address, front companies have also been found to share owners/managers, phone numbers, and employees and may also transact with one another or with similar counterparties, including suppliers. North Korean front companies also either often lack a stated business purpose, or the payments they receive for products and services are unrelated to an entity's specified line of business. Frequently, the fronts do not maintain a website or other online presence despite their significant transactions.

Many of these indicators will be apparent in the case studies that follow, particularly those focusing less on direct procurement of specific WMD components and more on broad financial and material support schemes.

Selected Cases

As noted above, North Korean PF cases with a U.S. nexus have largely been complex schemes to exploit vulnerabilities in the global banking system to raise and move funds on behalf of entities in support of the DPRK's weapons programs. While these cases are becoming more prevalent in recent years, there have also been some notable procurement cases involving financing elements that are worth highlighting. This assessment will discusses case examples in each category in order to give a representative snapshot of the current PF threat environment in the United States.

Alex and Gary Tsai

One of the more notable recent procurement cases involved the Taiwanese father-son duo of Hsien Tai Tsai (Alex Tsai), and his son Yueh-Hsun Tsai (Gary Tsai), which worked to acquire machine tools, among other things, on behalf of the DPRK.

Starting in the 1990s, Alex Tsai assisted the DRPK in procuring WMD-related goods through a network of companies connected to the Korea Mining Development Trading Corporation (KOMID)[23] and its subordinates and was involved in shipping items to the DRPK that could be used to support DPRK's ballistic missile program. Tsai was indicted by Taiwan's Taipei District Prosecutors Office for forging shipping invoices and illegally shipping restricted materials to North Korea in June 2008 and was found to have used at least two front companies based in Taiwan to accomplish this scheme: Global Interface Company, Inc., and Trans Merits Co., Ltd. As a result of these schemes, Alex Tsai, Global Interface, and Trans Merits were designated by OFAC under Executive Order (E.O.) 13382 in January 2009 for providing financial, technological, or other support to KOMID, which itself was designated by the U.S. in 2005 and by the UN in 2006.

[23] OFAC has described KOMID as North Korea's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons.

After the OFAC designations, Alex Tsai, his son Gary, and a Taiwanese associate of Alex Tsai (Individual A) continued to conduct business together but attempted to hide Alex Tsai's and Trans Merit's involvement in those transactions by conducting business under different company names, including Taiwan-based Trans Multi Mechanics. For example, by August 2009 – approximately eight months after the OFAC designations – Alex and Gary Tsai, Individual A and others allegedly began using Trans Multi Mechanics to purchase and export machinery on behalf of Trans Merits and Alex Tsai. Specifically, in September 2009 they purchased a Bryant center hole grinder—a machine tool that has potential WMD development applications—from a U.S. company based in suburban Chicago and exported it to Taiwan using Trans Multi Mechanics. The Tsais used their Taiwanese-based company bank accounts at Taiwanese banks to transfer funds to U.S. bank accounts of their U.S.-based facilitators, including Individual A, who would in turn use the funds to procure the goods and ship them to Taiwan. Due to the 2009 OFAC designations of the Tsai network, these transactions were already part of an illegal sanctions evasion scheme, which would become the focus of the criminal charges to be filed. However, given that the Tsai network was originally designated for providing similar support to entities associated with the DPRK WMD program, there is a strong possibility that the re-constituted network operating post-2009 also ultimately supported the same, or similar, DPRK entities.

On May 1, 2013, both Alex Tsai and Gary Tsai were arrested pursuant to two criminal complaints filed on April 19, 2013, which included charges of conspiracy to defraud the United States, conspiracy to evade prohibitions and restrictions imposed by OFAC (sanctions evasion), and money laundering conspiracy. Alex Tsai, who was believed to have resided in Taiwan, was arrested in Tallinn, Estonia, and later extradited to the United States. Gary Tsai, who is from Taiwan and is a U.S. legal permanent resident, was arrested at his home in Illinois. On June 6, 2013, Alex Tsai and Gary Tsai were indicted in the Northern District of Illinois for allegedly conspiring to violate U.S. laws designed to thwart WMD proliferation.

On October 10, 2014, Alex Tsai pleaded guilty to conspiracy to defraud the United States in its enforcement of regulations targeting WMD proliferators. In his plea agreement, Alex Tsai admitted that he engaged in illegal business transactions involving the export of U.S. origin goods and machinery. On March 16, 2015, Alex Tsai was sentenced to two years imprisonment. On December 16, 2014, Gary Tsai, pleaded guilty to making a false bill of lading. In his plea agreement, Gary Tsai admitted to arranging the export of a grinder to Taiwan by falsely identifying the consignee of the shipment. On April 24, 2015, Gary Tsai sentenced to 3 years of probation and a fine of $250.

Dandong Hongxiang Industrial Development Co. Ltd. (DHID)

The case of DHID—a Chinese trading company located near the North Korean border in the city of Dandong—perhaps best demonstrates some of the latest tactics used by DPRK PF networks to support the North Korean regime and its illicit weapons programs. According to public DOJ criminal and civil complaints, DHID and its senior management, including majority owner Ma Xiaohong (Ma), allegedly worked with North Korea-based Korea Kwangson Banking Corporation (KKBC) prior to 2009, when OFAC designated KKBC for providing U.S. dollar financial services for two other sanctioned North Korean entities tied to KOMID. After KKBC was designated by OFAC, DHID continued to function on behalf of its North Korean customers

both by establishing a complex scheme to evade U.S. sanctions and to launder money tied to sanctions-evading transactions, also in violation of U.S. law.

Ma and other DHID senior managers accomplished their scheme by creating or acquiring nearly two-dozen offshore front companies to hide transactions that were conducted for North Korean entities, including some on OFAC's Specially Designated Nationals and Blocked Persons List (SDN list). These front companies were established or incorporated in places such as the British Virgin Islands, the Seychelles, Hong Kong, Anguilla, England, and Wales.[24] Further, many of the businesses established in these jurisdictions shared the same physical address on their corporate registration documents and site visits revealed that there did not appear to be any actual business operations being conducted out of these office spaces.[25] Many of the front companies listed DHID and its directors, or individuals close to them, as the Chief Executive Officers, directors, and/or shareholders. The DHID conspirators ultimately used these companies to establish bank accounts at several Chinese banks in the name of the respective front companies. The Chinese companies maintained U.S. correspondent accounts at several U.S. banks. This setup allowed the DHID conspirators to conduct U.S. dollar transactions through U.S. correspondent banks for the benefit of their North Korean customers. For example, DOJ documents alleged that the bank accounts associated with several of these front companies located at three Chinese banks funded more than $75 million in transfers through the U.S. financial system. Other academic sources bring the network's total international count to 43 business entities across six separate jurisdictions on four continents.[26]

The alleged co-conspirators were also able to hide certain transactions by the use of a "ledger mechanism" maintained by KKBC and DHID. The ledger system allowed "KKBC to transact business in U.S. dollars through DHID and settle its outstanding dollar balance with DHID without transmitting any funds through the U.S. financial system, where such funds would be blocked because KKBC is a Specially Designated National (SDN)."[27] In 2015, for example, DHID employees possessed statements written primarily in Korean that showed U.S.-dollar denominated transactions between KKBC and DHID. The statements included some transaction descriptions detailing sales and/or purchases of fertilizer, anthracite coal, vehicles, and other goods. It appears that the alleged co-conspirators used this ledger system to keep track of U.S. dollar transactions effected through DHID. KKBC would deposit funds into a U.S.-dollar account in the name of DHID. This account would then be used by DHID to fund later commodity purchases made by DHID-controlled front companies using the U.S. dollars. Deposits from KKBC would often be matched shortly thereafter with withdrawals by DHID (both cash and wire) of almost identical amounts, which seems to suggest the direct funding of DHID operations by KKBC. This system allowed KKBC to settle outstanding balances with DHID without directly transmitting U.S. dollars through the U.S. financial system, which likely would have been blocked by the banks pursuant to existing sanctions.

The use of the ledger system of reimbursements and settling of accounts meant that instead of KKBC funding individual commodity payments and placing itself on the string of traceable,

---

[24] *U.S. v. Dandong Hongxiang Industrial Development Co. Ltd., Ma Xiaohong, Zhou Jianshu, Luo Chuanxu, and Hong Jinhua* (Criminal Complaint), pp. 12-15, available at https://www.justice.gov/opa/file/897041/download
[25] *U.S. v. DHID, et. al,* p. 11.
[26] C4ADS, "Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System," 2017, p. 13.
[27] *U.S. v. DHID, et. al,* p. 9.

cross-border payments processed through international banking channels to suppliers located throughout the world, DHID was able to take bulk deposits from KKBC and distribute funds throughout its global front company network in smaller amounts, essentially hiding all traces of North Korean involvement. This system also allowed trades and transactions between DHID, its North Korean customers (mainly facilitated by KKBC), and often unwitting suppliers to be netted and reconciled, thereby reducing the number of transactions that needed to involve cross-border, traceable banking transactions between KKBC and DHID. Similarly, when DHID would take consignment of North Korean-origin commodities (e.g., coal) to sell on the global market on behalf of North Korean clients, DHID could simply roll the funds from these commodity sales into future procurement orders without directly remitting payment for the original commodity delivery to North Korean customers.

However, while the initial funds remitted by KKBC to DHID did not need to transect the U.S. financial system, DHID's global network of front companies utilized the global banking system to facilitate transactions between suppliers and purchasers, and in the process U.S. correspondent banks unwittingly processed U.S. dollar payments on behalf of DHID entities and their North Korean clients. As a result of an investigation led by the FBI, in August 2016 a U.S. Magistrate Judge in the District of New Jersey signed a criminal complaint charging DHID, Ma, and other DHID top executives with conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and to defraud the United States; violating IEEPA; and money laundering conspiracy. In September 2016, after the charges were unsealed, OFAC imposed sanctions on DHID, Ma, and other co-conspirators for their ties to the government of North Korea's WMD proliferation efforts. In addition, the DOJ filed a civil forfeiture action for all funds contained in 25 Chinese bank accounts that allegedly belong to DHID and its front companies. The department has also requested that the federal court in the District of New Jersey issue a restraining order for all of the funds named in the civil forfeiture action, based upon the allegation that the funds represent property involved in money laundering, which makes them forfeitable under U.S. law. There are no allegations of wrongdoing by the U.S. correspondent banks or foreign banks that maintain these accounts.

Mingzheng International Trading Limited (Mingzheng) and Dandong Chengtai Trading Co. Ltd, also known as Dandong Zhicheng Metallic Material Co., Ltd (Zhicheng).

In mid-2017 the DOJ brought two separate civil asset forfeiture complaints against similar PF networks run by Chinese facilitators for their support of DPRK entities associated with Pyongyang's WMD programs. OFAC also designated individuals and entities linked to these networks.[28]

On June 14, 2017, DOJ initiated a civil forfeiture action against Mingzheng International Trading Limited (Mingzheng), for allegedly operating as a Hong Kong-based front company for a foreign-based branch of the North Korea-based Foreign Trade Bank (FTB). FTB is North Korea's primary foreign exchange bank and was designated by OFAC in 2013 for facilitating transactions on behalf of North Korea's proliferation network, including for UN- and U.S.-designated KOMID and KKBC.[29] According to the forfeiture complaint, "North Korea has used

[28] The designations were made pursuant to E.O. 13382, which targets WMD proliferators and their supporters, and E.O. 13722, which targets, in part, North Korea's revenue from coal, as well as its energy and financial services industries.

[29] The UN also later designated FTB in Aug. 2017 under UNSCR 2371.

the state-run Foreign Trade Bank ("FTB") to work with a host of front companies in order to access the U.S. financial system and evade the U.S. sanctions imposed on FTB and its sanctioned affiliates," and "Mingzheng acts as a front company to make U.S. dollar payments on behalf of a covert foreign branch of FTB, which is otherwise barred from making such U.S. dollar payments."[30] According to the complaint, Mingzheng has no website, stated no business purpose in corporate documents, made payments for products in unrelated industries, and served as a counterparty to multiple wire transfers over a short period of time. Perhaps most interestingly, in the 20 U.S. dollar wire transfers (totaling about $1.9 million) that Mingzheng allegedly sent or received between October and November 2015, seven of the fourteen counterparties to those transactions also transacted with DHID front companies.[31]

On August 22, 2017, the DOJ initiated a similar forfeiture action involving more than $4 million against Zhicheng, a company located in Dandong, China. The complaint alleges that Zhicheng and associated front companies controlled by Chinese national Chi Yupeng, comprise one of the largest financial facilitators for North Korea and, prior to being removed, Zhicheng's own website claimed the company was one of the largest importers of North Korean coal in China.[32] According to the complaint, Zhicheng conspired to evade U.S. economic sanctions by facilitating prohibited U.S. dollar transactions through the United States on behalf of the U.S.-designated North Korean Workers' Party. Zhicheng and other front companies in the Chi Yupeng network would accomplish this by first importing coal from North Korea and re-selling it on the global market. However, instead of pre-paying its North Korean suppliers for the coal in advance, Zhicheng would keep all the U.S. dollar proceeds from the coal sales, including the portion owed to the DPRK. The North Koreans would subsequently send instructions to Zhicheng for various items and commodities they required from the international market, and Zhicheng would then use the retained proceeds to purchase the items for export to North Korea. Some of these items included dual-use technology. These commodity acquisitions were well outside the scope of a mineral trading company and included bulk commodities such as sugar, rubber, petroleum products, and soybean oil, but also certain dual-use technologies.[33]

Bank of Dandong

In November 2017, FinCEN finalized a regulatory action under Section 311 of the USA PATRIOT Act to identify the China-based Bank of Dandong as an institution of "primary money laundering concern." FinCEN's finding documents the methods that North Korea uses to evade sanctions, and more specifically, the role of a willing foreign FI such as the Bank of Dandong to utilize its connectivity to the global banking system through correspondent relationships to aid Pyongyang's deceptive schemes. The finding notes that Bank of Dandong facilitated millions of dollars of transactions for companies involved in North Korea's WMD and ballistic missile programs, including KKBC and KOMID, and noted that a review of BSA data and other non-public information lead FinCEN to assess that "at least 17 percent of Bank of Dandong customer transactions conducted through the bank's U.S. correspondent accounts from May 2012 to May 2015 were conducted by companies that have transacted with, or on behalf of, U.S.- and UN-

[30] *U.S. v. Funds Associated with Mingzheng International Trading Limited, et. al.* (Civil Asset Forfeiture Complaint), p. 2.
[31] *U.S. v. Funds Associated with Dandong Chengtai Trading Limited, et al.*, pp. 16-19.
[32] Coal exports are thought to generate more than $1 billion in revenue per year for North Korea and represent the primary means of obtaining foreign currency for the regime.
[33] *U.S. v. Funds Associated with Dandong Chengtai Trading Limited, et al.*, p. 19.

sanctioned North Korean entities, including designated North Korean financial institutions and WMD proliferators."[34] The finding also notes that until December 2016, DHID owned a minority stake in Bank of Dandong, and that this relationship allowed DHID to access the U.S. financial system through Bank of Dandong to the tune of $56 million between October 2012 and December 2014.[35]

As a result of FinCEN's action, U.S. FIs are prohibited from maintaining correspondent accounts for, or on behalf of, Bank of Dandong, and are required to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their potential use to process transactions involving Bank of Dandong.

Iran

In contrast to the recent body of reporting on DPRK PF schemes, where threat actors and PF networks are working to provide broad financial support to help develop Pyongyang's illicit weapons programs, recent Iranian PF cases, including recent cases where the United States has imposed financial sanctions on Iranian PF facilitators and their networks, have mainly focused on procurement. There are, however, notable recent exceptions to this trend, including the Zarrab case highlighted below.

While Iranian state and military entities, including the Islamic Revolutionary Guard Corps (IRGC), control large swaths of the Iranian economy, private sector Iranian entities have been increasingly able to engage in international trade and finance, particularly after implementation of the Joint Comprehensive Plan of Action (JCPOA). Following JCPOA Implementation Day on January 16, 2016, some international sanctions targeting Iran still existed, as did a robust U.S. sanctions program focusing principally on Iran's support for terrorism, human rights abuses, and its ballistic missile program, and the United States also continued to maintain a broad primary embargo on all trade involving U.S.-origin items or U.S. persons. However, after Implementation Day, Iran perhaps had less of a need to employ the same covert fundraising and fund movement practices globally that it previously did to support its weapons programs, and the regime more broadly.

On May 8, 2018, the President issued National Security Presidential Memorandum-11 (NSPM-11), which ended the United States' participation in the JCPOA and declared that it is in the national interest of the United States to re-impose sanctions lifted or waived in connection with the JCPOA.[36] NSPM-11 also articulates a number of policy priorities with respect to Iran, including that Iran be denied a nuclear weapon and intercontinental ballistic missiles. With the re-imposition of certain sanctions following 90-day and 180-day wind-down periods, as well as a re-defined counter-proliferation financing posture with respect to Iran, it is likely that Iran will seek to focus additional resources on covertly moving funds through the international financial

[34] Imposition of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern – Final Rule; 31 C.F.R. Part 1010, p. 51759; available at https://www.fincen.gov/sites/default/files/federal_register_notices/2017-11-08/Dandong%20Final%202017-24238.pdf

[35] *Id*.

[36] See The White House, "Ceasing U.S. Participation in the JCPOA and Taking Additional Action to Counter Iran's Malign Influence and Deny Iran All Paths to a Nuclear Weapon," May 8, 2018, available at https://www.whitehouse.gov/presidential-actions/ceasing-u-s-participation-jcpoa-taking-additional-action-counter-irans-malign-influence-deny-iran-paths-nuclear-weapon/

system to support regime aims. In other words, illicit financial activity and proliferation support networks that Iran once relied upon prior to the JCPOA may be rejuvenated, as Iran seeks to evade U.S. sanctions.

In October 2018, FinCEN issued an advisory to help U.S. financial institutions better detect potentially illicit transactions related to Iran and to assist foreign financial institutions in better understanding the obligations of their U.S. correspondents, avoid exposure to U.S. sanctions, and address the risks that illicit Iranian activity poses to the international financial system.[37] Much like FinCEN's November 2017 DPRK advisory, the Iran advisory highlights the Iranian regime's exploitation of financial institutions worldwide, and describes a number of typologies used by the regime to illicitly access the international financial system and obscure and further its illicit activity.

Some of the methods used by the Iranian regime highlighted in the FinCEN advisory include: misusing exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, including those at the Central Bank of Iran (CBI). While not all of these methods are necessarily directly tied to WMD or ballistic missile procurement, versus other malign and destabilizing activity, Iran's ability to surreptitiously access the international financial system have the potential to aid Iranian entities involved in proliferation financing. For example, some of these efforts serve to provide funds to the IRGC, which has responsibility for Iran's ballistic missile program.

OFAC has also targeted entities responsible for providing support to Iran's ballistic missile program. For example, in February 2017, OFAC designated several networks and supporters of Iran's ballistic missile procurement, including a critical Iranian procurement agent and eight individuals and entities in his Iran- and China-based network, an Iranian procurement company and its Gulf-based network, and five individuals and entities that are part of another Iran-based procurement network.[38] These networks utilized a number of tactics to evade sanctions and export controls, including coordinating procurement through intermediary companies that obfuscated the final recipient of the goods and relying upon a network of trusted brokers in other countries, including, in one case, a China-based broker.

OFAC's proactive sanctions actions demonstrate how the USG utilizes preventative measures to target individuals and entities outside of the United States seeking to exploit the U.S. financial system on behalf of Iran. However, there have also been some notable examples in recent years of facilitators and networks operating on behalf of Iranian entities who have sought to circumvent U.S. sanctions and export controls by acquiring sensitive U.S.-origin technology and materials, or have otherwise exploited the U.S. financial system to benefit Iranian government entities tied to Iran's nuclear development activities and/or ballistic missile program. What follows is a selection of these cases.

---

[37] FinCEN, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," Oct. 11, 2018 available at https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf

[38] Treasury, Press Release, "Treasury Sanctions Supporters of Iran's Ballistic Missile Program and Iran's Islamic Revolutionary Guard Corps – Qods Force," Feb. 3, 2017, available at https://www.treasury.gov/press-center/press-releases/Pages/as0004.aspx

Selected Cases

Karl Lee

Chinese national Li Fangwei, also known as "Karl Lee," allegedly controls a large network of industrial companies based in eastern China, one of which is LIMMT Economic and Trade Company Ltd. (LIMMT). Over several years, Lee's companies have allegedly conducted millions of dollars' worth of business with Iran, including selling to Iranian entities various proliferation-sensitive goods controlled by the Nuclear Suppliers Group that were banned for transfer to Iran by the UN at the time. In addition, Lee had allegedly been a long-time supplier to entities affiliated with Iran's ballistic missile program, including the Defense Industries Organization and Iran's Aerospace Industries Organization.

OFAC publicly designated LIMMT (in 2006) and Lee (in 2009) under E.O. 13382 and added them to the SDN List. By virtue of these sanctions, Lee and LIMMT were effectively prohibited from conducting business with the United States and he was forced to operate much of his business covertly. Lee did this by establishing an extensive network of China-based front companies to conceal his and LIMMT's continuing participation in sanctionable activities. Many of these front companies have used the same address as LIMMT or a close variant thereof.

Between 2006 and 2014, Lee allegedly used front companies to engage in more than 165 separate U.S. dollar transactions, with a total value in excess of approximately $8.5 million. Included in those illicit transactions were allegedly sales of merchandise by Lee to Iran-based companies utilizing the U.S. financial system and attempts to acquire on behalf of Iran-based entities a number of dual-use items from the United States, China, and other countries.

To disrupt Lee's activities, the U.S. government employed multiple legal tools to target him and his network, including the initial sanctions first imposed in 2006 and 2009, criminal indictment, civil asset forfeiture, and additional financial sanctions and Commerce Department Entity List additions targeting his network of front companies. On April 29, 2014, the U.S. Attorney's Office for the Southern District of New York indicted Lee on multiple criminal charges, including violations of economic sanctions by using U.S.-based FIs to engage in millions of dollars of otherwise-prohibited U.S. dollar transactions, conspiring to commit wire fraud and bank fraud, a money laundering conspiracy, and two separate substantive counts of wire fraud in connection with such illicit transactions. Additionally, DOJ and the FBI announced the seizure of over $6,895,000 in funds attributable to the Lee front companies and the filing of a civil complaint seeking the forfeiture of those funds to the United States.[39] The indictment and asset forfeiture action were complemented by concurrent OFAC designations of eight additional front

[39] Despite challenges associated with seizure and forfeiture of property outside the United States, the use of a unique provision in U.S. asset forfeiture laws (18 U.S.C. § 981(k) and others) resulted in the forfeiture of $6,895,000, which represents the amount of funds used by the Lee front companies to engage in transactions that violated U.S. sanctions laws. The seized funds are substitutes for money held by Lee's front companies at banks in China and were seized from accounts at U.S. banks held in the name of foreign banks used by these front companies to conduct U.S. currency transactions (the correspondent accounts). Because the funds used in those transactions are held in banks overseas, the United States is unable to seize the funds directly. However, pursuant to section 981(k), the United States can seize funds located in a bank's correspondent accounts in the United States if there is probable cause to believe that funds subject to forfeiture are on deposit with that bank overseas. Based on this provision and others, the two separate seizure warrants were executed and on Feb. 20, 2015, the funds were ultimately forfeited to the United States.

companies used by Lee to the SDN List, along with the addition of nine China-based suppliers of Lee to the Commerce Entity List.

Bank Insider Complicity on Behalf of Entity Involved in Iranian Proliferation Activity

Often, FIs and their employees are unwitting participants in PF schemes, as PF facilitators and networks often operate a complex web of front companies and utilize other deceptive methods designed not only to evade government authorities, but also compliance programs of FIs. There have been occasions, however, where employees at FIs—generally large, global banks with worldwide operations—have sought to evade U.S. sanctions laws that would otherwise prohibit dealing with certain clients or countries.

One such case involved a foreign FI that processed electron funds transfers totaling approximately $39,567,720 on behalf of the Islamic Republic of Iran Shipping Lines (IRISL) or its affiliates to or through FIs located in the United States in apparent violation of the prohibitions against dealing in property or interests in property that come within the United States of any persons designated pursuant to OFAC's global WMD sanctions program.[40] OFAC designated IRISL on September 10, 2008, pursuant to E.O. 13382 for transporting cargo for entities involved in Iran's WMD program, as well as falsifying documents and using deceptive schemes to shroud its involvement in illicit commerce.

IRISL became a customer of a non-U.S. branch of the foreign bank in 2002, and by late 2004 was one of the branch's ten largest clients by revenue. However, by early 2005, U.S. FIs, including the New York branch of this foreign bank, were closely scrutinizing IRISL-related transactions. To facilitate funds transfers for IRISL, the non-U.S. branch employees created a "safe payment solution" that allowed IRISL to conduct transactions using the U.S. financial system that involved routing payments through special purpose entities controlled by IRISL, which were incorporated outside of Iran and bore no obvious connection to IRISL. The bank charged IRISL more money for this special service. When the New York branch's sanctions compliance filters were updated to detect the use of particular special purpose vehicles, the foreign bank switched use of those entities to other IRISL-approved entities. The non-U.S. bank branch employees also switched internal country codes to hide the fact that entities were actually owned by IRISL. The bank continued to process payments on behalf of non-designated IRISL affiliated entities even after IRISL was designated by OFAC.

In March 2015, the foreign bank and its New York branch were assessed a series of civil money penalties and/or entered into settlements with multiple USG law enforcement agencies and regulators for multiple apparent violations of U.S. economic sanctions laws and the BSA. In particular, DOJ entered into a deferred prosecution agreement (DPA) with the bank and its New York branch, whereby the banks admitted criminal conduct, agreed to forfeit $563 million and pay a $79 million fine, and comply with other conditions such as implementing rigorous internal controls and cooperating fully with DOJ, including by reporting any criminal conduct by an

[40] See U.S. v. Commerzbank AG, and Commerzbank AG New York Branch (Deferred Prosecution Agreement), March 10, 2015, available at https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf; *and also* Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Commerzbank AG, March, 12 2015, available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150312_commerzbank_settlement.pdf

employee. Assuming the banks' continued compliance with the DPA, DOJ agreed to defer prosecution for a period of three years, after which time, the government would seek to dismiss the charges. OFAC, the FRB, and New York's Department of Financial Services also entered into agreements and assessed monetary penalties for related violations, some of which the bank satisfied with its payments to DOJ. In total, the bank paid $1.45 billion in relation to this conduct.

The Zarrab Network

While many of the recent Iranian PF cases have largely been focused on the financing of weapons-related procurement, the case of the Zarrab Network is one that tracks more closely with recent North Korean schemes to utilize front companies and FIs to evade sanctions for the benefit of entities designated for their support of Iran's WMD or missile programs. Between at least 2010 and 2015, dual Turkish-Iranian citizens and brothers Reza and Mohammad Zarrab and their co-conspirators allegedly ran a network that conspired to conduct international financial transactions on behalf of and for the benefit of, among others, Iranian business, the Iranian government, and entities owned or controlled by the Iranian government.[41] The conspirators operated an international network of companies—including trading companies and money services businesses—located in Iran, Turkey, the United Arab Emirates (UAE), and elsewhere to conceal from U.S. banks, OFAC, and others that the transactions were on behalf of and for the benefit of Iranian entities.

Additional conspirators were added to superseding indictments, including the former Turkish Minister of Economy and three executives of Turkish Government-owned Halk Bank, including Hakan Atilla, the Deputy General Manager of International Banking at Halk Bank. Atilla and the other bankers in this scheme allegedly used Halk Bank to facilitate the Zarrab network's transfer of currency and gold to or from the sanctioned Iranian entities, while also concealing the bank's role in the evasion of U.S. sanctions from regulators. Specifically, the scheme allegedly involved the transfer of Iranian oil proceeds at Halk Bank to exchange houses and front companies controlled by Zarrab in order for those exchange houses and front companies to buy gold for export from Turkey. After being exported from Turkey, the gold could be converted into cash or currency and remitted to Iran or used to conduct international financial transfers on behalf of Iranian persons and entities. Mehmet Zafer Caglayan, who was serving as Minister of the Economy in Turkey during the scheme, allegedly received tens of millions of dollars' worth of bribes in cash and jewelry from the proceeds of the scheme to provide services to conceal the network's activities from USG officials. Using his official position, Caglayan allegedly directed the Turkish bankers to engage in certain types of deceptive transactions, approved the steps taken by other members to implement the scheme, and protected the scheme from competitors and from the scrutiny of authorities.

Reza Zarrab was arrested in March 2016 and Hakan Atilla was arrested in March 2017. Zarrab and Atilla were scheduled to stand trial in October 2017, while the rest of the defendants remain at large. Prior to the trial's commencement, Zarrab pled guilty and became a cooperating

[41] Among the beneficiaries of the conspirators' scheme were the CBI, the National Iranian Oil Company (NIOC), and the Iranian government-owned Bank Mellat. E.O. 13599 of Feb. 5, 2012 blocks all property and interests in property of the Government of Iran, including the CBI; OFAC identified NIOC as an agent or affiliate of the IRGC on Sep. 24, 2012, consistent with section 312 of the Iran Threat Reduction and Syria Human Rights Act of 2012; and Bank Mellat was designated by OFAC pursuant to E.O. 13382 on Oct. 25, 2007.

witness. Zarrab subsequently testified to details of the illicit operation, which included using false documentation, front companies, and other deceptive measures to access U.S. FIs on behalf of the Government of Iran and other Iranian entities. According to Zarrab, one tactic used by the co-conspirators was to create and use false and fraudulent documents to disguise prohibited transactions for Iran and make those transactions falsely appear as transactions involving food, thus falling within humanitarian exceptions to the sanctions regime. This induced U.S. banks to unknowingly process international financial transactions in violation of IEEPA. Atilla was subsequently convicted on January 3, 2018 of five of the six counts on the controlling indictment, including conspiracies to defraud the United States, to violate the IEEPA, to commit bank fraud, and to commit money laundering, as well as a substantive count of bank fraud.

Syria

The Syrian Civil War and rise of ISIS in the region have brought repeated violations by multiple actors of longstanding global norms prohibiting the use of chemical weapons. The Organization for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism (JIM) attributed multiple chemical weapons attacks to both the Syrian regime and to ISIS over the course of the conflict, and the U.S. has also independently assessed that the Assad regime was responsible for one of the largest chemical weapons attacks of the conflict in April 2017 at Khan Shaykhun.[42]

From an illicit finance perspective, the U.S. maintains a robust sanctions program targeting Syrian individuals and entities consistent with foreign policy and national security interests, including for WMD-related activities. Due to disturbing use of chemical weapons in the region, the U.S. increased its sanctions targeting individuals and entities associated with these WMD-related activities in Syria, which has also served as a signal to U.S. FIs of a possible threat emanating from PF-support networks acting on behalf of designated Syrian entities.

For example, in response to the JIM's findings in August and October 2016 that the Syrian government was responsible for chlorine gas attacks on its own people in 2014 and 2015, the USG designated eighteen senior regime officials and one entity connected to Syria's WMD program and identified five Syrian military branches as part of the Government of Syria, which brings these entities under separate, category-based sanctions. Also, following the April 2017 Khan Shaykhun sarin attack perpetrated by the Assad regime, OFAC designated 271 employees of Syria's Scientific Studies and Research Center (SSRC), which is the Syrian government agency responsible for developing and producing non-conventional weapons and the means to deliver them. On February 23, 2017, OFAC designated Metallic Manufacturing Factory for acting for on behalf of Mechanical Construction Factory, which was previously designated for acting for or on behalf of SSRC.[43]

[42] See "Letter dated 24 August 2016 from the Leadership Panel of the Organization for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism addressed to the Secretary-General"; Worldwide Threat Assessment, pp. 11-12.

[43] Treasury, Press Release, "Treasury Sanctions Senior Al-Nusrah Front Leaders Concurrently with UN Designations; Separate Action Targets Syrian entity related to the proliferation of weapons of mass destruction," Feb. 23, 2017, available at https://www.treasury.gov/press-center/press-releases/Pages/sm0011.aspx

These actions not only support U.S. foreign policy and national security objectives, by isolating key individuals and entities associated with Syrian WMD programs, but they also serve as a public signal regarding the potential PF risk emanating from Syria and thus help to protect the U.S. financial system as a preventive measure. They complement earlier efforts dating back to 2005, when the SSRC was first designated under an executive order targeting global WMD proliferation activity (E.O. 13382), to target the Syrian government's WMD programs and its key facilitators. Ongoing efforts, including multiple separate designations between 2015-2018, have focused on targeting the key facilitation networks of the SSRC, including but not limited to: SSRC cover companies used for a variety of purposes, including direct procurement or shipping/logistics; suppliers of science and technology materials based outside of Syria; brokers and individual businessmen involved in the trade of sensitive or dual-use technology; and independent shipping and logistics agents.[44] These threat actors are located in multiple jurisdictions across the globe, primarily in the Middle East and East Asia, and while they have sought to transact in U.S. dollars and thus present a PF risk to the U.S. financial system, there are also a few publicly available examples of procurement and financing cases with a direct U.S. nexus.

Selected Cases

Procurement of Restricted Laboratory Equipment

One example of a PF network attempting to use the U.S. financial system for the benefit of Syrian entities was recently made public and involved a procurement network of Syrian, British, and American individuals allegedly working to illegally export restricted chemical laboratory equipment to Syria.[45] The network, which operated from 2003 to at least late 2012, involved two brothers of Syrian descent and an American man who operated an export business based in Pennsylvania. The network facilitated the acquisition of chemical lab equipment[46] on behalf of Syrian customers and exported these items to Syria by transshipping them through third party countries such as Jordan, the UAE, and the UK. In order to accomplish this, the co-conspirators

[44] See, for example, Treasury, Press Release, Treasury Targets Syrian Regime Financial and Weapons Networks, March 31, 2015, available at https://www.treasury.gov/press-center/press-releases/Pages/JL10013.aspx; Treasury, Press Release, Treasury Sanctions Networks Providing Support to the Government of Syria, July 21, 2018, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0526.aspx; Treasury, Press Release, Treasury Sanctions Additional Individuals and Entities in Response to Continuing Violence in Syria, Dec. 23, 2016, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0690.aspx; Treasury, Press Release, The United States and France Take Coordinated Action on Global Procurement Network for Syria's Chemical Weapons Program, July 25, 2018, available at https://home.treasury.gov/index.php/news/press-releases/sm443

[45] *U.S. v. Harold Rinko, Ahmad Feras Diri, Moawea Deri, and d-Deri Contracting & Trading*, Case No. 3-12CR294 (Indictment) (M.D. Pa., Nov. 20, 2012).

[46] Note: the items involved in this case included a portable gas scanner used for detection of chemical warfare agents by civil defense, military, police and border control agencies; a handheld instrument for field detection and classification of chemical warfare agents and toxic industrial chemicals; a laboratory source for detection of chemical warfare agents and toxic industrial chemicals in research, public safety and industrial environments; a rubber mask for civil defense against chemicals and gases; a meter used to measure chemicals and their composition; flowmeters for measuring gas streams; a stirrer for mixing and testing liquid chemical compounds; industrial engines for use in oil and gas field operations; and a device used to accurately locate buried pipelines. While these items were Commerce-controlled for export to Syria and have potential WMD-applications, based upon publically available information, it is not possible to know how the end customers intended to use these items. However, as many of these items have potential connections to chemical warfare agents and could be used to benefit or contribute to WMD-related enterprises, there is a potential PF nexus in the case.

created false invoices that undervalued and mislabeled the goods being purchased in the United States and also listed false information regarding the buyers' identity and geographic location. The financing of this scheme was mainly accomplished through a series of international wire transfers ordered by the brothers from their Lebanese bank accounts to the American facilitator, often with vague and innocuous descriptions listed for the underlying purpose of the transfers, such as "goods value" or "value of industrial machine spare parts." These transfers were also of relatively small value, ranging from $500 to $18,000. Ultimately, an interagency law enforcement investigation led to two guilty verdicts for the U.S. individual and one of the brothers, as well as a forfeiture order of $45,698, while the second brother (a Syrian citizen) remains at large.

Lebanon- and U.S.-based Procurement Networks with ties to SSRC

On July 25, 2018, pursuant to E.O. 13382, OFAC designated Electronics Katrangi Trading (EKT) and its network, for providing or attempting to provide financial, material, technological, or other support for, or goods or services in support of, the SSRC. EKT is an electronics supplier based in Lebanon with operations in Syria, Egypt, China, and France, and is a leading supplier for the SSRC—including goods used in the production of weapons of mass destruction. EKT uses various aliases and numerous branches to conduct its activities.[47]

On the same day, OFAC designated Antoine Ajaka and Anni Beurklian, two individuals of Lebanese origin residing in Massachusetts, for providing similar support to EKT's Director, Amir Katranji. DOJ had previously indicted Ajaka, Beurklian, their company (Top Tech US Inc.), and Katranji on March 21, 2018 for conspiracy to violate U.S. export laws and regulations, conspiracy to defraud the United States, smuggling U.S. goods out of the United States, conspiracy to obstruct justice, and obstruction of justice.[48]

As alleged in the indictment, beginning no later than 2012 and continuing until January 9, 2018, Ajaka and Beurklian operated an export business, Top Tech US Inc., out of their Waltham, Massachusetts residence. The couple used their business to procure goods, including electronics, computer equipment, and electrical switches, from U.S. companies and export those goods out of the United States to customers in Lebanon and Syria, including Amir Katranji and EKT. In 2007, EKT and its founder, Mohammad Katranji, Amir Katranji's father, were added to the Department of Commerce's Entity List because the U.S. Government had determined that EKT and Mohammad Katranji were involved in activities related to the acquisition, attempted acquisition, and/or development of improvised explosive devices, which were being used against U.S. and Coalition troops in Iraq and Afghanistan.

The indictment further alleges that in or about 2013, Ajaka and Beurklian began doing business with Katranji and supplying U.S.-origin goods to EKT using Top Tech US. Ajaka and Beurklian knew that Katranji operated a business in Syria and that they were providing brokering services

[47] See Treasury, Press Release, "The United States and France Take Coordinated Action on Global Procurement Network for Syria's Chemical Weapons Program," Jul. 25, 2018, available at https://home.treasury.gov/index.php/news/press-releases/sm443.

[48] DOJ, Press Release, "Waltham Couple and Company Indicted for Conspiracy to Illegally Obtain U.S. Goods For Syria," Mar. 21, 2018, available at https://www.justice.gov/usao-ma/pr/waltham-couple-and-company-indicted-conspiracy-illegally-obtain-us-goods-syria

to Katranji and EKT by buying and shipping U.S.-origin goods to EKT and its customers. EKT paid Ajaka and Beurklian more than $200,000 through Top Tech US's bank accounts for their services. To conceal their illegal activity with EKT and evade the mandatory export filing requirement, Ajaka and Beurklian, with the knowledge and agreement of Katranji, falsified shipping paperwork and undervalued goods being shipped overseas directly to, or on behalf of, EKT.

China and Russia

There have been relatively few publicly reported cases in recent years of the U.S. financial system being used to facilitate the development of China's or Russia's indigenous WMD programs.[49] It should be noted at the outset that for China and Russia, the United States does not have economic sanctions programs directed specifically at these countries' WMD programs.[50] This is an important difference between these countries and North Korean, Iranian, and Syrian threat actors previously discussed in this section, as it likely means that the potential universe of PF-activity for Russian and Chinese threat actors seeking to benefit their own countries' programs is largely limited to procurement-based schemes designed to acquire sensitive goods and technologies, rather than sanctions-evasion schemes necessary to finance and move funds on behalf of weapons programs in states that are already recognized nuclear weapons powers. Even on the procurement front, there are relatively few publicly reported cases of these threat actors seeking to exploit the United States to finance WMD-related programs, versus other types of industrial espionage or trafficking in goods with broader military applications.

With respect to China, there are several important examples in recent years of Chinese entities and individuals engaging in PF activities with a U.S. nexus, but the activity in question has been for the benefit of other state-sponsored WMD programs, namely North Korea's and Iran's. While there are also some notable cases of Chinese economic espionage against the U.S. industrial base pertaining to military or other sensitive technologies, these cases fall outside the scope of this risk assessment, which is targeted at the illicit financing and procurement of WMD and their delivery systems. It is difficult to attribute specific intent for some of these industrial espionage cases, particularly in industries where there may be dual-use applications of some technology.[51] Further, in some sensitive industries, Chinese entities have also attempted to acquire technology and know-how through legitimate business transactions, including the acquisition of U.S. companies.

---

[49] However, as some of the cases in the North Korea and Iran sections demonstrate, there have been several instances of Chinese individuals or entities being involved in PF networks working on behalf of other countries' WMD programs. The UN PoE on North Korea has also pointed to North Korean overseas banking representatives operating in China, Russia, and other jurisdictions, where they control bank accounts and facilitate transactions supporting the DPRK's weapons programs (See previously cited March 2018 PoE Report, p. 60). These are North Korean individuals, however, so their operations within these jurisdictions aren't assessed as China- or Russia-specific PF threats, per se.

[50] However, the United States does have a separate sanctions authority targeting Russia for non-WMD reasons and Chinese and Russian entities have been sanctioned for WMD-related activities either under a separate, global WMD authority (E.O. 13382) or under another state-centric program (*e.g.*, Iran and DPRK sanctions programs).

[51] Furthermore, in some sensitive industries, Chinese entities have also attempted to acquire technology and know-how through legitimate business transactions, including the acquisition of U.S. companies. Such activity, done publicly and subject to regulatory and national security reviews by U.S. departments and agencies, is outside of an assessment that focuses on illicit use of the U.S. financial system to finance WMD proliferation.

In terms of PF networks benefitting Russia's WMD and delivery systems, there have been a few notable cases in recent years involving the procurement of U.S.-origin sensitive technology, some of which has WMD or missile technology applications. In the case of the Russian PF network cited below, the perpetrators sought to acquire specific sensitive U.S. components that were not available in Russia. According to expert analysis of the goods in question, there seemed to be both a lack of domestic capacity by the Russian industrial base and a lack of drive to acquire the know-how to produce this type of technology domestically (i.e., develop an indigenous production capability). This may be because some of the components, while high-tech and costly to produce, are somewhat older and less than state-of-the art, but still necessary to the proper functioning of legacy Russian weapons systems. So, while these components are required to maintain these important, WMD-capable delivery systems, it may be difficult to justify investment in developing a domestic production capability for a platform that is becoming obsolete.

ARC Electronics, Inc. (ARC)

According to an indictment and as reflected in court proceedings, individuals associated with Houston-based export company, ARC were at the center of a scheme to ship approximately $50 million worth of microelectronics and other sensitive technologies to Russia over several years.[52] ARC was run by a U.S.-Russian dual national and others living in the United States with ties to Russia. From at least October 2008 to October 2012, ARC essentially operated as a cover company for its principal conspirators to obtain advanced microelectronics from manufacturers and suppliers located within the United States and export these goods to Russia, in violation of U.S. export controls. These commodities have applications in a wide range of military systems, most notably in missile guidance systems, and Russia does not produce many of these sophisticated goods domestically.[53] The FBI-led investigation tied Russian military and intelligence agencies directly to the scheme, including through a letter sent by a specialized electronics laboratory of Russia's Federal Security Service (FSB), Russia's primary domestic intelligence agency, to a company affiliated with ARC claiming that certain microchips obtained for the FSB by ARC were faulty and needed to be replaced. The network functioned as follows:

- ARC would take orders for specific sensitive goods from Russian front companies acting on behalf of Russian military and intelligence agencies. The individuals who ran these fronts maintained direct contact between the Russian government end users, who provide direction regarding sourcing requirements.
- ARC would then seek to acquire these components from a host of different U.S. manufacturers, distributors, and brokers and would often request quotes from multiple parties for each component ordered in order to find a supplier willing to sell the parts

[52] See U.S. v. Alexander Fishenko, et al. September 28, 2012; relevant press releases also available here: https://www.justice.gov/opa/pr/russian-agent-pleads-guilty-leading-scheme-illegally-export-controlled-technology-russian and https://www.justice.gov/opa/pr/three-defendants-convicted-conspiring-illegally-export-controlled-technology-russian-military

[53] For example, a certain type of Field Programmable Gate Array (FPGA) chip exported by ARC to Russian customers has an application to the Russian Iskander SRBM-26, a type of short-range ballistic missile system that is capable of launching nuclear warheads. ARC was known to have exported at least 2,500 of these chips to Russian customers.

without asking questions. ARC sought to manipulate these suppliers by falsely claiming to be a manufacturer (rather than an exporter/reseller), falsifying end-user statements to indicate civilian applications, procuring items through sister companies, and disguising the true nature of ARC's business in the public domain, including its website.

- In order to further evade export controls, ARC falsely classified the goods they exported on export records submitted to the Department of Commerce and transshipped the goods through third-party countries such as Germany, Finland, and Singapore.
- The Russian front companies would pay ARC via wire transfers made indirectly through a series of shell companies established in jurisdictions that generally have a large off-shore or non-resident deposit banking presence, as banks in these jurisdictions were also used to facilitate payments to ARC through U.S. banks. The investigation uncovered that ARC was linked to $241 million worth of BSA reporting by U.S. FIs.

The investigation was initiated by FBI, but given the wide breadth of specialized knowledge required, an interagency task force consisting of Commerce, Naval Criminal Investigative Service, Office of Naval Intelligence, IRS, DOJ, and FBI was stood up. In the end, eleven individuals and two companies were indicted on federal charges including: acting as an agent of the Russian government within the United States without prior notification to the Attorney General; conspiring to export, and illegally exporting, controlled items to Russia; conspiring to launder money; and obstruction of justice. The eight individuals who were located in the U.S. were arrested, tried, and convicted/plead guilty to all or some of the charges, and approximately one million dollars was forfeited through criminal asset forfeiture complaints. One of the primary co-conspirators received a 135-month sentence, and another received 120 months. Additionally, in conjunction with the unsealing of the charges, Commerce added 165 foreign persons and companies who received, transshipped, or otherwise facilitated the export of controlled commodities by the defendants to its Entity List. Prior to this listing, there were only two entities from Russia on the Entity List.

A somewhat unique aspect of this case was the full extent to which U.S. authorities were able to piece together the entire procurement and financing network, including by directly connecting the chain of involvement from the U.S. facilitator to Russian front companies and facilitators to specific Russian government agencies.

Pakistan

The 2018 Worldwide Threat Assessment notes that, "Pakistan continues to produce nuclear weapons and develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer-range ballistic missiles."[54] Like China and Russia, Pakistan is a nuclear weapons state but there is no U.S. targeted financial sanctions program dedicated to Pakistan for the development and maintenance of its nuclear weapons program.[55] Unlike China and Russia, however, Pakistan is not a party to the NPT and

[54] Worldwide Threat Assessment, p. 8.

[55] For example, unlike Iran, North Korea, and Syria, OFAC does not administer a sanctions program targeted specifically at Pakistan. However, the United States has historically imposed other types of sanctions on Pakistan for its nuclear weapons and ballistic missile programs. The bulk of these nuclear-related sanctions were waived by President Bush on September 22, 2001, due to Pakistan's cooperation in the Global War on Terror. See

therefore is not recognized under international law as having the right to the peaceful use of nuclear energy, to include the transfer or acquisition of nuclear technology. As a result, the Pakistani nuclear program has been marked with controversy since its inception, not just in its own right as a state-led program going against the grain of international norms, but also due to the outward proliferation tied to former members of the program in future years.[56] Having to operate outside of regulated international channels has meant that Pakistan has largely had to acquire technology and know-how through covert means, and in select cases, those acting for on behalf of Pakistani government entities have sought to procure U.S.-origin goods and facilitate these illicit transactions by exploiting the U.S. financial system.

Diversion of U.S.-origin Products with WMD Applications to Entities Linked to the Pakistani Military

According to court documents and statements made in court, from at least 2012 to December 2016, Muhammad Ismail, and his two sons, Kamran and Imran Khan, were engaged in a scheme to purchase goods that were controlled under the Export Administration Regulations (EAR) and to export those goods without a license to Pakistan, in violation of the EAR. Through a series of front companies located in both Pakistan and the United States, the three men received orders from a Pakistani company that procured materials and equipment for Pakistani entities tied to Pakistan's nuclear weapons and ballistic missile programs requesting the conspirators to procure specific products that were subject to the EAR, and which have WMD and ballistic missile applications. When U.S. manufacturers asked about the end-user for a product, the defendants either informed the manufacturer that the product would remain in the U.S. or completed an end-user certification indicating that the product would not be exported.

After the products were purchased, they were shipped by the manufacturer to the conspirators in Connecticut. The products were then shipped to Pakistan, to a front company acting on behalf of Pakistani entities, which was responsible for ensuring that the items were then turned over to either the Pakistan Atomic Energy Commission (PAEC), the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics, none of which were on the original shipping declarations and all of which were placed on the Commerce Entity List for "nuclear non-proliferation reasons."[57] Some of the materials procured were received by the National Development Complex (NDC), a division within SUPARCO that is "the focal point for Pakistan's missile development program and is credited for the redesign of several models, including the Ghaznavi and Shaheen I and II medium range ballistic missile."[58] NDC is also on Commerce's Entity List.

The conspirators never obtained a license to export any item to the listed entities even though they knew that a license was required prior to export. They received the proceeds for the sale of export controlled items through wire transactions from entities based in Pakistan and the United

---

See Presidential Determination No. 2001–28 of September 22, 2001, Waiver of Nuclear-Related Sanctions on India and Pakistan, 66 Fed. Reg. 191 (Oct. 2, 2001).

[56] In 2004, Pakistani nuclear scientist Abdul Qadeer Khan admitted to running a nuclear proliferation ring responsible for transferring sensitive technology to Iran, North Korea, and Libya in the 1980s and 1990s.

[57] *U.S. v. Kamran Khan, et. al.* criminal indictment, p. 3.

[58] *Id.,* p. 11.

Arab Emirates to a U.S. bank account that the conspirators controlled. On June 1, 2017, Imran Khan pleaded guilty to one count of violating IEEPA. In pleading guilty, Khan specifically admitted that, between August 2012 and January 2013, he procured, received and exported to PAEC an Alpha Duo Spectrometer, a device that has military applications, without a license to do so. On March 5, 2018, Ismail and Kamran Khan each pleaded guilty to one count of international money laundering, for causing funds to be transferred from Pakistan to the U.S. in connection with the export control violations. In pleading guilty, Ismail and Kamran Khan specifically admitted that, between January and July 2013, they procured, received and exported to SUPARCO, without a license to do so, certain bagging film that is used for advanced composite fabrication and other high temperature applications, which has military applications.

SECTION 2. U.S. GOVERNMENT EFFORTS TO DETECT AND COMBAT PROLIFERATION FINANCING

As these case studies have demonstrated, the USG wields a variety of tools and authorities to detect and combat PF. Interagency coordination is essential, and involves a variety of measures ranging from global sanctions and other financial authorities utilized to target PF and support networks to domestic actions taken by law enforcement to investigate, prosecute, and pursue the forfeiture of PF-derived proceeds. Financial regulators are also involved in monitoring private sector compliance with U.S. regulations designed to combat various types of illicit finance, a process that involves regular supervisory reviews and occasionally taking enforcement action against institutions that run afoul of these regulations, when appropriate. Coordinated outreach from all of these departments and agencies to the private sector and communication with international partners is also a key component that helps to inform and refine actions taken and provide these stakeholders with necessary information to help better combat PF threats.

FINANCIAL AND REGULATORY EFFORTS

As part of the broader post-September 11, 2001 national security reform efforts, the U.S. government focused increasingly on the importance of disrupting the finances and funding networks that fueled various national security threats and on the importance of financial intelligence collected and disseminated by U.S. FIs. Treasury's TFI was established in 2004 to lead the U.S. government's counter-illicit financing efforts, including efforts to combat PF.[59] TFI seeks to mitigate PF risk through both systemic and targeted actions, bringing various capabilities to bear to exploit financial intelligence, impose economic sanctions on PF networks, engage private sector entities and foreign partners, and take regulatory actions to protect the U.S. financial system from abuse.

Targeted actions, usually in the form of targeted financial sanctions administered and enforced by OFAC, are used to identify, disrupt, and prevent WMD proliferators from accessing the U.S. financial system. Faced the State Department use authorities granted to them through legislation and under various executive orders to designate and identify WMD proliferators and their support networks. Once designated or identified, OFAC regulations require U.S. persons—including FIs—to block (freeze) the property, including financial assets, of the targets. E.O. 13382[60] is the principal authority used to target WMD proliferators and their support networks worldwide, but OFAC can also utilize various authorities granted under certain country sanctions

[59] TFI is composed of: TFFC, TFI's policy development and outreach office; OFAC which is charged with administering and enforcing U.S. economic sanctions programs, including those targeting PF activities; OIA, TFI's in-house intelligence agency; and FinCEN, the U.S. financial intelligence unit, which is also charged with administering and enforcing the BSA. See Department of the Treasury, Organizational Structure, available at https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx

[60] E.O. 13382 (2005), among other things, blocks the property of persons engaged in proliferation activities and their support networks. The establishment of such an authority was a key recommendation of the 2005 report from the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the "Silberman-Robb Commission"), which concluded that Treasury should possess equally robust authorities to target WMD proliferation activity as the Department had for targeting terrorism (E.O. 13224).

programs, such as those targeting North Korea.[61] As of July 2018, 387 individuals and entities were designated pursuant to E.O. 13382.[62]

FinCEN also has its own targeted authorities it can utilize to protect the U.S. financial system from abuse. As discussed previously, under Section 311 of the USA PATRIOT Act, FinCEN can determine that a foreign jurisdiction, FI, class of transaction, or type of account is of "primary money laundering concern" and can impose a variety of regulatory measures that trigger a number of obligations for U.S. FIs when dealing with the subject of these actions. These "special measures" range from increased recordkeeping and reporting requirements for transactions associated with the target to a complete prohibition on opening a correspondent account for the target. Since November 2016, FinCEN has taken action under Section 311 three times. In all three cases, the target has been connected to PF activity (all related to North Korea) and in each case, FinCEN proposed a prohibition under the "fifth special measure" on U.S. FIs opening or maintaining correspondent banking accounts for the targets, as well as the application of special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their indirect use to process transactions involving these targets.[63]

These actions are complemented by the efforts of FinCEN and the federal functional regulators that evaluate and enforce FIs' compliance with the appropriate regulatory requirements. For example, as administrator of the BSA, FinCEN promulgates implementing regulations for the BSA to reduce the potential for abuse by various illicit finance threats, including PF. To develop these regulations FinCEN and other offices within TFI regularly engage all the appropriate stakeholders to understand these threats. FinCEN works with the federal functional regulators and law enforcement to develop guidance, administrative rulings and advisories for the financial industry to aid FIs in identifying priority threats, such as PF.

For their part, the federal functional regulators regularly examine the FIs they supervise for compliance with BSA/AML program requirements and OFAC obligations, as well as the reporting and recordkeeping requirements of the BSA. The functional regulators also have a range of formal and informal enforcement authority to address significant violations that may be identified through their supervisory activities. The combination of a strong AML/CFT framework and effective supervision makes it more difficult for proliferators and their facilitators to access the U.S. financial system.

FinCEN also serves as the U.S. government's central repository for suspicious activity reporting on potential proliferation financing activity, which it makes available to state, local, tribal, and federal law enforcement agencies across the country. When necessary, FinCEN also makes use of its regulatory authorities under the BSA to obtain targeted information from FIs on proliferation finance-related cases. This information may be used in a variety of efforts to target

[61] For example, at the time of writing, there were six separate Executive Orders targeting North Korea: 13466, 13551, 13570, 13687, 13722, and 13810.
[62] See SDN List, available at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx
[63] See (1) Nov. 2016 Section 311 final rule for the entire jurisdiction of North Korea; (2) Nov. 2017 Section 311 final rule targeting the China-based Bank of Dandong for facilitating millions of dollars of transactions for companies tied to the DPRK weapons programs; and (3) Feb. 2018 Section 311 finding and notice of proposed rulemaking targeting Latvia-based ABLV Bank for institutionalized money laundering practices, including processing transactions for parties connected to UN-designated entities involved in North Korea's procurement or export of ballistic missiles. All available at https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures

threats, inform regulatory policy, or engage and educate stakeholders such as FIs and foreign partners.

Additionally, USG counter-PF initiatives have benefited from and contributed to long-standing efforts to protect the U.S. financial system against all forms of illicit finance. These laws, rules, regulations and guidance have aided FIs in identifying and mitigating risk, provided valuable information to law enforcement, and created the foundation of financial transparency required to deter, detect, and punish those who would abuse the U.S. financial system to launder the proceeds of crime and move funds for illicit purposes. For example, controls instituted to combat money laundering and terrorist financing have also strengthened the U.S. government's ability to identify, deter, and disrupt PF.

LAW ENFORCEMENT EFFORTS

Law enforcement agencies play a critical role in U.S. counter-PF efforts. The DOJ is the principal government entity responsible for overseeing the investigation and prosecution of PF offenses at the federal level. Within DOJ NSD, CES supervises and coordinates these efforts across the country, ensuring that these cases are given the appropriate amount of attention and resources. CES, in partnership with the U.S. Attorneys' offices and other law enforcement agencies, investigates and dismantles PF networks, which have sought to exploit the U.S. financial system. As we have seen in the case studies above, DOJ's ability to bring federal charges and asset forfeiture claims against PF facilitators and front companies is a critical aspect of the USG's effort to counter PF activity in the U.S. A public charging document not only serves a criminal deterrent purpose, but can also be shared with private sector stakeholders, which are then able to act based on that information.

These actions would not be possible without the investigative efforts of key federal law enforcement agencies, such as the FBI and BIS, which specializes in export control violation cases. In fact, in recognition of the threat facing the U.S. from nation-states efforts to acquire WMD, the proliferation of advanced weapons technology worldwide, and attempts by terrorist groups to obtain WMD or advanced weapons technology, the FBI combined three counterproliferation-related components into a single jointly-managed entity at FBI Headquarters—the CPC—to disrupt global proliferation networks.[64] The creation of the CPC has resulted in an expanded counterproliferation mandate and enhanced coordination among various related components, including agents, analysts, and professional staff. The CPC mission is to lead the FBI's efforts to identify, deny, disrupt, and exploit attempts to obtain or divert embargoed, export-controlled, or otherwise sensitive technologies or activities related to WMD, missile delivery systems, space or conventional weapons systems, or dual-use components. In order to accomplish its mission, the CPC works to identify, penetrate, mitigate, and disrupt proliferation networks that are engaged in efforts to acquire and utilize WMD and critical controlled U.S. technologies and in doing so, often work to identify and understand the financing tactics these networks employ.

[64] The three components comprising the CPC are: 1) the WMD Directorate, which provides scientific expertise; 2) the Counterintelligence Division, which provides operational expertise; and 3) the Directorate of Intelligence, which provides analytical expertise. See https://www.fbi.gov/about/leadership-and-structure/national-security-branch/fbi-counterproliferation-cente .

Similarly, BIS works to advance U.S. national security objectives by ensuring an effective export control system. In addition to managing the export control regulatory framework, BIS's Export Enforcement (EE) division works to mitigate the risk of sensitive exports reaching hostile entities or those that engage in onward proliferation through the use of both preventative and investigative methods. These methods include applying law enforcement and export control expertise to prevent and deter exports of the most sensitive items to illicit end-users and to embargoed destinations. EE works closely with other federal law enforcement agencies, including the FBI and DHS when conducting investigations or preventative actions and also works with DOJ to bring criminal cases for violations.[65] As we have seen in some of the procurement-related case studies in this section, BIS lends key expertise regarding controlled goods and technology and works with other agencies to track efforts by PF networks to finance illicit procurement.

[65] See Department of Commerce, BIS, Enforcement, available at https://www.bis.doc.gov/index.php/enforcement

SECTION 3. VULNERABILITIES AND RISKS

The growth and increasing sophistication of the international financial system has enabled illicit actors to place and move money, hide assets, and conduct transactions anywhere in the world, exposing financial centers to exploitation and abuse in an unprecedented way. As demonstrated in the Threats section, weapons proliferators and procurement agents gain access to the international financial system through aliases, agents, and individuals in a number of jurisdictions, as well as well-established networks of front companies and financial representatives abroad, including embassy personnel from countries of proliferation concern.[66] The sheer size and complexity of the international financial system affords these threat actors opportunities to disguise their illicit activity, a state of affairs only exacerbated by uneven implementation of global counter-PF standards across jurisdictions. As the UN PoE notes in its March 2018 report, "the [sanctions] regime is yet to be matched by the requisite political will, international coordination, prioritization and resource allocation necessary to drive effective implementation."[67] The PoE explores a number of vulnerabilities in the international financial system and in the restrictive measures imposed by the international community to change North Korea's behavior, but as we have seen in the case studies, the instances of North Korean and other PF threat actors accessing the U.S. financial system came in select instances where the U.S. plays a central role in the international financial system.

The global dominance of the U.S. dollar generates trillions of dollars of daily transaction volume through U.S. banks, creating significant exposure to potential illicit financial activity. In the United States, there are two real-time gross settlement systems for high-value transactions: the Federal Reserve System's Fedwire Funds Service (Fedwire) and the Clearing House Interbank Payment System (CHIPS), operated by The Clearing House, a private-sector bank association.[68] Fedwire, is used to clear and settle payments with immediate finality for FIs that hold an account with a Federal Reserve Bank[69] and processed about 152 million transfers in 2017, averaging $2.9 trillion per day.[70] CHIPS is the largest private-sector U.S.-dollar clearing system in the world and it is primarily used to clear and settle the U.S. dollar leg of international wire payments.[71] CHIPS clears and settles an average of almost 450,000 transactions worth $1.5 trillion in domestic payments and the U.S. dollar segment of international wire payments each day.[72] It has

---

[66] See UNSC, "S/2016/157: Final report of the Panel of Experts submitted pursuant to resolution 2207 (2015)" (24 Feb. 2016), available at http://www.un.org/ga/search/view_doc.asp?symbol=S/2016/157

[67] See UNSC, "S/2018/171: Final report of the Panel of Experts submitted pursuant to resolution 2345 (2017)" (5 Mar. 2018), p. 5, available at http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171

[68] The proprietary message formats used by both Fedwire and CHIPS are compatible with each other as well as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging format to facilitate cross-border funds transfers. SWIFT's messaging platform and services connects more than 11,000 banking and financial institutions in more than 200 countries and territories. See https://www.swift.com/about-us/discover-swift#topic-tabs-menu.

[69] See https://www.federalreserve.gov/paymentsystems/fedfunds_about.htm.

[70] See https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm

[71] Based on data from the third quarter of 2017, approximately 75 percent of payments that clear and settle through CHIPS originate outside the U.S. See CHIPS Public Disclosure of Legal, Governance, Risk Management, and Operating Framework (Jun. 2018), p.6, available at https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips-public-disclosure-2018.pdf.

[72] See CHIPS Annual Statistics: https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips-volume_v2.pdf.

been estimated that CHIPS processes the majority of all international interbank funds transfers that are denominated in U.S. dollars and today CHIPS accounts for roughly half the value of all Fedwire transactions.[73] This exposure to a daily flow of trillions of dollars in transaction volume across these payment systems requires U.S. FIs to maintain robust safeguards to minimize the potential for illicit activity.

THE U.S. REGULATORY FRAMEWORK AND PF

The U.S. regulatory framework for countering illicit financial activity was originally conceived with the intent of detecting and deterring long-established, traditional forms of illicit finance, such as money laundering and terrorist financing. Beginning with the passage of the BSA in 1970, which was amended substantially by the USA PATRIOT Act in 2001, the USG has largely designed and implemented its counter-illicit finance framework to ensure that FIs and other key sectors have robust AML/CFT controls in place, and that U.S. regulatory agencies are supervising these sectors for compliance with relevant regulations. While "proliferation financing" is not a term of art used in the foundational counter-illicit finance legislation, or even in its implementing regulations, the U.S. AML/CFT framework that has come about as a result of these laws and regulations, as well as the supervisory expectations and enforcement posture of key USG agencies charged with enforcing these rules, has also functioned to counter PF activity. Further, as demonstrated throughout this assessment, the robust U.S. sanctions regime targeting PF activity globally has also worked to help protect the U.S. financial system by deterring and disrupting foreign threat actors, but also by establishing and enforcing penalties for those who violate U.S. sanctions.

As demonstrated by the case studies, the bulk of PF activity transecting the U.S. financial system has occurred as a result of threat actors exploiting the connectivity in the international banking system. While this may be an inherent vulnerability and preferred method for PF threat actors to move funds across borders to support their aims, the U.S. AML/CFT and sanctions framework has become well-developed over time and a number of requirements have been put in place for U.S. FIs help to detect and prevent PF activity.

BSA/AML programs and reporting and record keeping requirements for FIs form the core of these required measures. These measures are designed not only to protect U.S. FIs from abuse by illicit actors, but also to provide useful information to law enforcement and national security authorities for the purpose of combating the full range of illicit finance threats. A BSA/AML compliance program must include, at a minimum, a system of internal controls to ensure ongoing compliance, independent testing, designation of an individual responsible for managing BSA compliance, ongoing training for appropriate personnel, and (as a result of Customer Due Diligence Rule described below) risk-based procedures for conducting ongoing customer due

[73] CHIPS is both a customer and competitor of Fedwire, as CHIPS relies upon Fedwire for settlement but accepts large value payments that could be processed directly by Fedwire. See https://www.newyorkfed.org/aboutthefed/fedpoint/fed36.html.

diligence.[74] Under the BSA, FIs must also have a written customer identification program[75] and enhanced due diligence procedures for those customers that present a high risk for money laundering or terrorist financing, as well as for the provision of foreign correspondent accounts and private banking services.[76]

Until recently, a major gap in these regulations pertained to the potential misuse of legal entities by illicit actors. However, on May 11, 2016, FinCEN issued a final rule entitled "Customer Due Diligence Requirements for Financial Institutions" (also known as the "CDD Rule"), which amended aspects of BSA regulations to improve financial transparency and prevent threat actors from misusing companies to disguise their illicit activities. The CDD Rule, which became mandatory on May 11, 2018, clarifies and strengthens customer due diligence requirements for U.S. banks, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities and adds a new requirement for these covered FIs to identify and verify the identity the natural persons (known as beneficial owners) who own, control, and profit from companies when those companies open accounts.

The CDD Rule requires covered FIs to establish and maintain written policies and procedures that are reasonably designed to (1) identify and verify the identity of the beneficial owners of companies opening accounts; (2) understand the nature and purpose of customer relationships to develop customer risk profiles; and (3) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. With respect to the new requirement to obtain beneficial ownership information, FIs will have to identify and verify the identity of any individual who owns 25 percent or more of the equity interests in a legal entity, and an individual who controls the legal entity through management.[77]

Previously, except in limited circumstances, when an account at a FI was opened in the name of a legal entity, there was no obligation on the FI to identify the person or persons who owned or controlled the legal entity or to verify their identity. This meant that criminals and other bad actors were potentially able to hide behind shell companies, using the company's account to send and receive funds anonymously, or misuse front companies that have legitimate operations, allowing illicit proceeds to be comingled with earnings from legitimate operations.[78] Despite this gap, U.S. law enforcement was generally able to investigate shell companies that conduct some activity in the United States through financial investigatory techniques, such as the examination of bank records, tax filings, and other government records. While law enforcement

[74] See 31 C.F.R. § 1010.210, 1020.210; 12 C.F.R. § 21.21 (national banks and federal savings associations); 12 C.F.R. § 208.61 (state member banks); 12 C.F.R. § 326.8 (nonmember banks); 12 C.F.R. § 748.2 (credit unions); FINRA Rule 3310 (securities broker-dealers); 31 C.F.R. 1026.210(b) National Futures Association Rule 2-9(c) (futures commission merchants and introducing brokers in commodities); Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual (2014), pp. 28-29.

[75] See 31 C.F.R. 1020.220 (banks), 1023.220 (securities broker-dealers), 1024.220 (mutual funds) and 1026.220 (futures commission merchants and introducing brokers in commodities).

[76] See 31 C.F.R. § 1010.610 and 620; FFIEC BSA/AML Examination Manual at pp. 112-118, 125-129; Joint Guidance on Obtaining and Retaining Beneficial Ownership Information, FIN– 2010–G001, Mar. 5, 2010.

[77] See 31 C.F.R. §§ 1010.230, 1020.210, 1023.210, 1024.210, and 1026.210.

[78] A shell company, to be a legal entity, must be registered with a state and can serve legitimate purposes; for example, holding property rights or financial assets. However, because shell companies do not have physical operations or assets, their purpose can be easily misrepresented in the account-opening process.

had success in determining beneficial ownership through this process, it was often time consuming.

As we have seen from the case studies, foreign actors have mainly used foreign shell or front companies to establish foreign bank accounts, which they can then use to execute dollar-denominated transactions through U.S. banks, thus accessing the U.S. financial system. The CDD Rule makes it more difficult for PF facilitators and networks to successfully utilize legal entities within the United States to obtain access to U.S. FIs, by increasing law enforcement's access to beneficial ownership information, thereby enhancing financial investigative efforts. While this does not specifically address the issue of shell and front companies in foreign jurisdictions, as discussed below in the discussion on correspondent banking, there are additional BSA/AML requirements with respect to this type of cross-border financial activity that help prevent the types of PF activity demonstrated by the cases.

In summary, while the principal focus of the U.S. counter-illicit finance regulatory framework has been directed towards combatting money laundering and terrorist financing, it also works to help U.S. authorities and regulated entities detect and combat PF activity. As the case studies have demonstrated, much of the PF activity detected is generally initially identified as another type of illicit activity, such as money laundering or a violation of export controls, yet U.S. authorities were able to utilize a number of criminal, civil, and administrative tools to take action.

Further, the fact that all U.S. persons must comply with U.S. sanctions laws and regulations, most notably OFAC's sanctions regulations, such as those related to WMD proliferation, means that while there is no explicit provision labeled "counter-proliferation financing" within the U.S. counter-illicit finance regulatory framework, key elements of PF risk must be considered by U.S. industries exposed to sanctions risk. OFAC has issued Economic Sanctions Enforcement Guidelines to provide guidance and articulate various factors the agency takes into account when making enforcement determinations, including the adequacy of risk-based compliance programs institutions may put in place to ensure compliance with OFAC regulations.[79] OFAC encourages this same risk-based approach for banks in designing and implementing their sanctions compliance programs and the federal functional regulators evaluate these programs to ensure that the FIs they regulate are complying with U.S. sanctions.[80] Further, FinCEN also issues advisories to the private sector identifying specific "red flags" that could be indicative of PF activity. These advisories are intended both to assist FIs in identifying suspected illicit activity and to remind them of their regulatory obligations with respect to this activity.[81]

---

[79] OFAC Economic Sanctions Enforcement Guidelines, available at https://www.treasury.gov/resource-center/sanctions/Documents/fr74_57593.pdf; 31 C.F.R. Pt. 501, App. A, 83 Fed. Reg. 11876 (Mar. 19, 2018).
[80] See, e.g., FFIEC BSA/AML Examination Manual, pp. 142-151.
[81] For example, as noted in the Threats section, in Nov. 2017 FinCEN issued an "Advisory on North Korea's Use of the International Financial System," wherein FinCEN identified a number of DPRK-related schemes to access the international financial system and reiterated a number of regulatory obligations required for U.S. covered financial institutions, including the general prohibition on correspondent accounts for North Korean financial institutions (due to the Nov. 2016 DPRK 311 Action), requirements to apply special due diligence for North Korean financial institutions and the Bank of Dandong (due to 311 Actions on both), and general suspicious activity reporting requirements.

Therefore, the U.S. regulatory framework does aid FIs in identifying PF risk, and in the process also provides valuable information to law enforcement and informs U.S. national security policy. The combination of a strong regulatory framework and effective supervision makes it more difficult for proliferators and their facilitators to access the U.S. financial system; however, the sheer size and scale of the global banking system, which is underpinned by cross-border banking relationships linking together virtually every jurisdiction in the world, means that proliferation networks can make use of complex corporate and banking arrangements to mask their illicit activity and achieve their ends. While there are occasional instances where these networks have sought to rely on non-banking channels to raise revenue and facilitate funds transfers, including select cases where PF networks have utilized money services businesses (MSBs) and relied upon bulk cash transfers, these vulnerabilities were largely exploited outside of the United States.

MISUSE OF FOREIGN CORRESPONDENT RELATIONSHIPS

As demonstrated by the case studies, PF threat actors have accessed the U.S. financial system through the global banking system, as opposed to other types of FIs such as MSBs or by other methods such as bulk cash smuggling. U.S. FIs, particularly large dollar-clearing banks operating on a global scale, play an integral role in facilitating global finance and trade, specifically by providing U.S. dollar clearing services through cross-border banking relationships. It is therefore not surprising that these institutions would have exposure to PF activity by virtue of processing transactions on behalf of foreign FIs with which they have business relationships.

This type of financial service or relationship is broadly referred to as a "correspondent account." Correspondent accounts are relationships between FIs that facilitate the provision of services from one FI (the correspondent) to another (the respondent). These services can relate to transactions for the respondent FI itself or on behalf of the respondent's customers, including processing wire transfers, international trade settlements, remittances, and cross-border payments. Correspondent account relationships are essential to the proper functioning of the global economy and international correspondent account relationships allow FIs worldwide to facilitate cross-border transactions in their currency of choice. They also enable FIs to conduct business and provide services to clients in foreign countries without the expense and burden of establishing a foreign presence. However, because of the complexity of correspondent account relationships, multiple intermediary FIs may be involved in a single funds transfer transaction. Since a significant percentage of international transactions are denominated in U.S. dollars,[82] U.S. banks and other FIs are particularly important providers of correspondent services.

With respect to proliferation financing, the case studies demonstrate that correspondent accounts held by banks, versus other FIs such as broker-dealers or introducing brokers in commodities, appear to be a consistent target that threat actors have sought to exploit. When U.S. banks receive funds or instructions for a funds transfer from a foreign respondent, they likely do not

[82] According to some estimates, dollar-denominated transactions account for the majority of the value of transfers operated through SWIFT. For instance, the Financial Stability Board's 2017 Correspondent Banking Data Report, which incorporates some data provided directly by SWIFT, noted that USD transactions accounted for 53.49 percent of the total value of all transfers using the SWIFT system (December 2016 figure). For comparison, the Euro had the second highest value at 28.67 percent. *Report available here:* http://www.fsb.org/wp-content/uploads/P040717-4.pdf.

have an account relationship with the originator of the payment, who is either a direct or indirect client of the respondent, and therefore often have limited information on the transaction details. The challenges of "intermediation," where multiple intermediary FIs may be involved in a single funds transfer transaction means that some correspondent relationships carry an even higher potential risk. For these reasons, conducting appropriate due diligence on the foreign respondent is critical to managing the vulnerability associated with this product. The complexity and volume of transactions that flow through U.S. correspondent accounts, coupled with the varying (often limited) recordkeeping requirements of funds transfer systems in different countries, increase the likelihood that some correspondent accounts can be exploited to facilitate the flow of illicit proceeds into or through the U.S. financial system.

As PF generally deals with the trade in commodities or goods, both licit and illicit, trade financing services in the area of correspondent banking are of particular concern with respect to this type of illicit finance. Trade finance arrangements often involve the use of documentary collections and guarantees, whereby banks act as the intermediary guaranteeing a transaction if certain documentary requirements are met by the counterparties to a transaction (exporter and importer). This type of financing can generally be vulnerable to documentary fraud or forgery, as the bank does not actually inspect the goods in the shipment, but rather relies upon the supporting documents to determine whether payment should be made.[83]

U.S. FIs that maintain correspondent accounts for foreign FIs are required to establish appropriate, specific, and risk-based due diligence policies, procedures, and processes that are reasonably designed to assess and mitigate the risks inherent with these relationships. To comply with their regulatory obligations, U.S. FIs must monitor transactions related to these accounts to detect and report suspicious activities. These policies, procedures, and processes will depend on the level of risk posed by the foreign respondent. Such risks can vary depending on the respondent's strategic profile, including its size and geographic locations, the products and services it offers, and the markets and customer bases it serves.[84]

U.S. FIs are also required to conduct enhanced due diligence on certain higher risk foreign correspondent banks that requires: (1) enhanced scrutiny, (2) determining whether the foreign correspondent bank maintains nested accounts for other foreign banks, and (3) the collection of beneficial owner information regarding foreign correspondent banks that are not publicly traded.[85] In addition to these requirements for foreign correspondents, U.S. FIs are also prohibited from maintaining correspondent accounts for foreign "shell banks" (i.e., foreign banks with no physical presence in any country).[86] While there is no general requirement for U.S. FIs to conduct due diligence on a foreign respondent's customers, in determining the appropriate level of due diligence to perform on foreign respondents, U.S. FIs should consider the extent to

[83] However, while these opportunities for fraud and forgery are perhaps more pronounced with trade finance transactions involving documentary procedures, it should also be noted that FIs may also be able to see more information related to a given transaction with these types of financing arrangements, thus providing potentially greater opportunities to perform appropriate due diligence. It should also be noted that, based on the information publicly available within this assessment, none of the cases identified appeared to utilize trade financing arrangements and were primarily open account transactions.
[84] See FFIEC BSA/AML Examination Manual, pp. 267-271.
[85] See 31 C.F.R. § 1010.610(b).
[86] See 31 C.F.R. § 1010.630.

which information related to the respondent's markets and types of customers is necessary to assess the risks posed by the relationship, satisfy the institution's obligations to detect and report suspicious activity, and comply with U.S. economic sanctions. In practice, this means that U.S. FIs may request additional information concerning the activity underlying the foreign respondent's transactions in accordance with U.S. suspicious activity reporting rules and sanctions compliance obligations.[87]

In the case of trade finance transactions, beyond the normal CDD procedures required of banks in all transactions, the federal functional regulators expect a bank's policies, procedures, and processes to include a thorough review of all applicable trade documentation (e.g., customs declarations, trade documents, invoices, etc.) to enable the bank to monitor and report unusual and suspicious activity, based on the role played by the bank in the letter of credit process. The sophistication of the documentation review process should be commensurate with the size and complexity of the bank's trade finance portfolio and its role in the letter of credit process.[88]

The federal functional regulators expect U.S. FIs to have robust BSA programs and OFAC compliance programs that include appropriate customer due diligence so that the institutions have a clear understanding of a foreign respondent's risk profile and expected account activity. This information helps U.S. FIs make informed decisions regarding the risks associated with their foreign correspondent account relationships and the level and nature of suspicious activity monitoring needed to mitigate those risks effectively.

In order for U.S. FIs to develop a clear understanding of foreign respondent risk profiles and determine how best to manage the risks associated with these relationships, they are expected to obtain and review sufficient information about their foreign correspondent relationships, including the types of customers their foreign respondents serve and the markets in which the respondent is active. This approach allows the U.S. FI to conduct an adequate assessment of the risks present in: (1) the foreign respondent's business and markets, (2) the type, purpose and anticipated activity, (3) the nature and duration of the relationship with the foreign respondent, and (4) the supervisory regime of the jurisdiction in which the foreign respondent is licensed, and to design and implement controls to manage these risks effectively.[89]

[87] U.S. Department of the Treasury and Federal Banking Agencies Joint Fact Sheet on Foreign Correspondent Banking, p. 2, available at https://www.treasury.gov/press-center/press-releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf
[88] See FFIEC BSA/AML Examination Manual, pp. 267-270.
[89] *Id.*

SECTION 4. RISK SUMMARY

Even with these requirements, most of the PF activity involving the U.S. financial system has been the result of PF networks exploiting global correspondent banking relationships. In some examples, such as the case of the foreign bank described in the Threats section, this is due to insider complicity or systemic deficiencies within a bank's own AML/CFT compliance program. Most instances, however, are the result of difficulties in detecting sophisticated schemes and deceptive practices of PF networks, as demonstrated by many of the North Korea cases, including DHID, Mingzheng, and Zhicheng. These cases almost always involve U.S. banks clearing transactions on behalf of the customers of foreign FIs, and in certain types of transactions such as dollar clearing for trade finance, there may be a lack of underlying transaction information, which adds an additional challenge for FIs, even after these transactions are subjected to scrutiny required by U.S. regulations.

Another challenge for FIs in detecting and mitigating PF activity is understanding how PF differs from other illicit financial activity such as money laundering or terrorist financing. For some, the segmenting of PF from other types of illicit financial activity may seem like a difference without distinction. However, it becomes very difficult to proactively detect PF activity if one does not know what to look for and is relying on methods primarily designed to catch other types of illicit activity, despite how similar that activity may be to PF. While a FI's obligations under the BSA are the same regardless of the financial crime, a less nuanced understanding of PF also presents a corollary challenge for U.S. law enforcement and other authorities, which may not receive as timely information regarding potential PF networks if FIs are reporting the activity as some other type of financial crime, even if that reporting is fully consistent with their regulatory obligations. While some larger U.S. FIs have recently made great strides in responding to targeted requests from U.S. authorities—that is, using targeted information to identify PF activity, map PF networks, and report this information to U.S. authorities—this is largely reactive to USG requests and is not fully engrained as a systemic practice within these institutions, let alone among all approximately 40,000 U.S. FIs.[90]

FinCEN has sought to remedy this potential gap in targeted PF reporting through its advisory process. In recent FinCEN advisories on PF subjects, such as North Korea, FinCEN has not only provided the latest red flags and indicators that could be indicative of PF activity, but has also reminded FIs of their regulatory obligations, including SAR reporting requirements, and has requested that FIs include targeted phrases in any BSA filings to indicate that the scheme is tied to a PF entity of concern. This way, FinCEN and law enforcement entities receiving BSA reporting are more quickly able to collate potential lead information, map networks, and pursue investigative leads.

---

[90] There are more than 11,000 depository institutions (5,593 FDIC insured banks, and 5,573 federally insured credit unions), more than 24,000 MSBs registered with FinCEN, almost 4,000 active broker-dealers registered with the SEC, and approximately 1,000 casinos. See: https://research.fdic.gov/bankfind/; https://www.ncua.gov/analysis/Pages/industry/industry-at-a-glance-december-2017.pdf; https://www.fincen.gov/msb-registrant-search; https://www.americangaming.org/sites/default/files/research_files/2017%20State%20of%20the%20States.pdf

Treasury and U.S. law enforcement agencies have also sought to increase outreach to private sector entities, particularly U.S. FIs, regarding proliferation financing. These efforts have come in the form of more formal outreach in the course of executing regulatory or investigative duties and have included sharing of targeted information to help target FI reporting on potential PF networks. They have also taken the form of bilateral or multilateral meetings with FIs, sometimes in coordination with relevant foreign government partners and foreign FIs, to discuss PF typologies and trends more broadly. Given the cross border nature of PF, Treasury has made it a priority to proactively engage all stakeholders, foreign and domestic, in properly identifying and collectively mitigating PF risk.

CONCLUSION

While the U.S. counter-illicit finance regulatory framework is well-developed, U.S. FIs generally understand and comply with their regulatory requirements, and USG efforts to counter PF activity are aggressive and proactive, global PF threat actors still seek to exploit the vastness of the global financial system to achieve their ends. Given the central role that U.S. FIs and the U.S. dollar play in global commerce, it is inevitable that these activities will at times touch the United States. While global correspondent banking is highlighted in this assessment as a principal vulnerability and driver of PF risk within the United States, this has more to do with its central role as perhaps the most important facilitator of cross-border trade and less with a lack of controls or focus within the sector. To the contrary, the potential vulnerability is well-recognized and there are robust regulatory and monitoring controls in place by USG authorities and FIs to mitigate the risks associated with this activity. While other forms of illicit financial activity have relied upon other types of financial products or institutions,[91] and while some of these products or entities have played a role internationally in facilitating PF activity,[92] the cases demonstrate that PF activity with a U.S. nexus has relied heavily on international banking.

The financing of proliferation presents a key national security threat to the United States and indeed to international peace and security. This assessment has demonstrated that the United States does currently contend with noteworthy PF risks from a variety of threat actors due to its position as a global financial center. However, the maturity of the U.S. counter-illicit finance regulatory framework, the robust national security policy and operational architecture put in place by the USG, and the proactive actions of U.S. authorities to aggressively seek out and combat PF activity have meant that residual risk emanating from this type of illicit finance remains manageable.

[91] See 2018 NMLRA and 2018 NTFRA, published concurrently with this assessment as part of the 2018 *Illicit Finance Strategy*.

[92] For example, the March 2018 PoE report specifically identifies bulk cash smuggling by DPRK overseas financial representatives, corporate service providers/company formation issues in foreign jurisdictions, and the use of joint ventures to obfuscate links to designated entities. See previously cited UNSC Report S/2018/171, pp. 4-5.