FIN-2017-A007 **September 25, 2017**

Advisory on North Korea's Use of the International Financial System

North Korea uses front and trade companies to disguise, move, and launder funds to finance its nuclear and ballistic missile programs.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to further alert financial institutions to North Korean schemes being used to evade U.S. and United Nations (UN) sanctions, launder funds, and finance the North Korean regime's weapons of mass destruction (WMD) and ballistic missile programs. This advisory is being issued in conjunction with today's designations by Treasury's Office of Foreign Assets Control (OFAC), which targeted several representatives of designated North Korean financial institutions.[1] This advisory provides financial red flags of illicit North Korean schemes, including the use of China-based financial representatives, front companies, trading companies, and financial institutions operating in areas bordering the Democratic People's Republic of Korea (DPRK). These red flags will assist financial institutions in identifying and reporting suspected illicit activity by the North Korean government and its financial institutions.

This advisory should be shared with:

- *Chief Risk Officers*
- *Chief Compliance Officers*
- *Legal Departments*
- *AML/BSA Departments*
- *AML/BSA Analysts*
- *Sanctions Analysts*

Recent Treasury Actions

The U.S. Department of the Treasury is implementing a strategy designed to impose pressure on the DPRK's finances and economy and protect the U.S. and international financial systems from misuse by the DPRK. The Treasury Department continues to take actions targeting DPRK's ongoing development of WMD and ballistic missile programs, as well as its continued violations of UN Security Council resolutions (UNSCRs).[2] Recent Treasury Department actions include the following:

- OFAC has issued a number of substantial DPRK-related designations and identifications, including Executive Order 13810, which was issued on September 21, 2017. This Executive Order significantly expands Treasury's authorities to target persons who continue to finance and facilitate North Korea's economic activity. The designations, 257

[1] For more information on today's OFAC sanctions, see https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/OFAC-Recent-Actions.aspx.

[2] Relevant UNSCRs include 2375 (September 2017), 2371 (August 2017), 2356 (June 2017), 2321 (November 2016), 2270 (March 2016), 2094 (March 2013), 2087 (January 2013), 1874 (June 2009), and 1718 (October 2006). *See* http://www.un.org/en/sc/documents/resolutions/ for more information.

persons to date, expose the North Korean regime's international reach and continued access to the international financial system;[3]

- FinCEN has designated the DPRK as a primary money laundering concern subject to special countermeasures under Section 311 of the USA PATRIOT Act to safeguard the U.S. financial system;[4] and,

- FinCEN has issued advisories and guidance about the increased risk that the DPRK and North Korean entities pose to U.S. and foreign financial institutions.[5]

On August 22, 2017, and on September 25, 2017, OFAC designated Mingzheng International Trading Limited (Mingzheng), a Hong Kong-based front company, and several dozen North Korean individuals as well as a number of banks, respectively, for their involvement in evading sanctions and laundering funds on behalf of the North Korean regime. Treasury believes that the bank accounts used by these sanctioned persons are maintained predominantly at major Chinese financial institutions. These sanctioned North Korean persons have used their accounts to access the U.S. and international financial systems in support of the DPRK's WMD and ballistic missile and weapons programs.

In addition, in June 2017, FinCEN issued a Notice of Proposed Rulemaking (NPRM) finding the China-based Bank of Dandong to be a "foreign financial institution of primary money laundering concern" under Section 311 of the USA PATRIOT Act.[6] If finalized, the proposed rule would prohibit covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, Bank of Dandong. Covered financial institutions

---

[3] OFAC's sanctions prohibit U.S. persons, including U.S. financial institutions, from engaging in most transactions involving the DPRK, the Government of North Korea, and the Korean Workers' Party. In addition to today's actions, OFAC recently imposed DPRK-related sanctions actions pursuant to Executive Orders 13382 and 13722 on August 22, 2017. OFAC imposed DPRK-related sanctions pursuant to those same authorities on June 29, 2017. *See* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170629.aspx for more information. OFAC also imposed DPRK-related sanctions actions pursuant to those same Executive Orders and/or Executive Order 13687 on June 1, 2017, March 31, 2017, December 2, 2016, and September 26, 2016. For the complete listing of all OFAC actions related to the DPRK, *see* https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx.

[4] FinCEN's Section 311 rule imposing the fifth special measure against the DPRK: a) prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, North Korean banking institutions; b) requires covered financial institutions to take reasonable steps not to process a transaction for the correspondent account of a foreign bank in the United States if such a transaction involves a North Korean financial institution; and c) requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving North Korean financial institutions. *See* https://www.treasury.gov/press-center/press-releases/Pages/jl0603.aspx and https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf [81 FR 78715 (November 9, 2016)] as codified in 31 CFR § 1010.659. FinCEN issued the finding and initial notice of proposed rulemaking (NPRM) on June 1, 2016 [81 FR 35441 (June 2, 2016) and 81 FR 35665 (June 3, 2016)], respectively; *see* https://www.fincen.gov/sites/default/files/shared/2016-13038(DPRK_Finding).pdf and https://www.fincen.gov/sites/default/files/shared/2016-13037(DPRK_NPRM).pdf.

[5] *See* FinCEN Advisories pertaining to the DPRK: FIN-2013-A005 (July 2013), FIN-2009-A002 (June 2009), and FinCEN Advisory – Issue 40 (December 2005). *See also* FIN-2017-A005 (September 2017) regarding the June 23, 2017, Financial Action Task Force (FATF) "Public Statement" on the DPRK.

[6] *See* 82 FR 31537 (July 2017) and "Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern" (July 2017).

would also be required to apply special due diligence measures to their foreign correspondent accounts reasonably designed to guard against such accounts being used to process transactions involving the Bank of Dandong.

How North Korea Accesses the International Financial System

Although international sanctions have significantly isolated North Korean banks, the North Korean government continues to use state-owned entities and banks, as well as bulk-cash smuggling and trade, to access the international financial system through aliases, agents, and individuals in strategic jurisdictions, as well as long-standing networks of front companies and embassy personnel.[7]

As explained in the United Nations Security Council "Report of the Panel of Experts established pursuant to resolution 1874" (February 2016) (hereafter referred to as "UN Report"), the North Korean government uses state-owned entities and banks to conduct transactions in support of its WMD and ballistic missile programs. These North Korean state-owned enterprises in turn use foreign-based front companies and covert representatives based abroad to obfuscate the true originator, beneficiary, and purpose of transactions, enabling millions of dollars of North Korean illicit activity to flow through U.S. correspondent accounts.

To conduct these transactions, the UN Report notes that North Korean state-owned enterprises typically orchestrate elaborate trade-based payment schemes. For instance:

(1) **Sale/Export of Natural Resources**: The DPRK sells/exports natural resources (*e.g.*, coal, iron ore, minerals) to China-based companies, often located near the North Korean border, such as in the Liaoning province.[8] The Chinese companies, in turn, sell such natural resources to the Asian market.

(2) **Indirect Payment for Natural Resources**: Rather than directly paying the DPRK, the China-based companies divide their payments into smaller outflows in a complex layering scheme directed to front companies, shell companies, shipping or trade businesses based in Asia (often registered in Hong Kong), and other companies based in various offshore jurisdictions (*e.g.*, British Virgin Islands, Marshall Islands, Seychelles). Various financial representatives and corporate service providers may establish the front or shell companies or be representatives of the various involved entities.

(3) **Import/Smuggling of Goods**: The front or shell companies then use the received payments to purchase and ship commodities to the DPRK. These commodity shipments in turn may be used to smuggle goods that the North Korean government uses to build its WMD and ballistic missile programs.

These types of trade-based schemes allow the North Korean government to evade U.S. and UN sanctions by directing payments for natural resource sales to its front and shell companies. The North Korean government can then use these laundered proceeds, through its front and shell

[7] *See* United Nations Security Council "Report of the Panel of Experts established pursuant to resolution 1874" (February 2016).

[8] UNSCR 2371 prohibits imports of North Korean coal, iron and iron ore, lead and lead ore, and seafood. UNSCR 2375 prohibits imports of textiles, among other new measures.

companies, to access the international financial system and acquire technology for use in its WMD and missile programs. North Korean representatives often use these companies to establish bank accounts at local banks and take orders from sanctioned North Korean entities.

Treasury believes that the DPRK uses and maintains a network of financial representatives, primarily in China, who operate as agents for North Korean financial institutions. In this capacity, these representatives orchestrate schemes, set up front companies, and manage surreptitious bank accounts to move and disguise illicit funds, evade sanctions, and finance the proliferation of the DPRK's WMD and ballistic missile programs.

U.S. Forfeiture Actions Reveal Complex North Korean Schemes to Evade Sanctions

Two recent actions by the Department of Justice also highlight the DPRK's methods to evade sanctions:

Mingzheng International Trading Limited (Mingzheng). On June 14, 2017, the U.S. Department of Justice (DOJ) initiated a 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).[9] The forfeiture complaint illustrates how the DPRK allegedly used a network of front companies and corporate representatives to evade U.S. sanctions by acting on behalf of a designated North Korean bank. According to the forfeiture complaint, "North Korea has used 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,"[10] 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." 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. In this case, Mingzheng allegedly conducted 20 wire transfers in U.S. dollars, totaling about $1.9 million, between October and November 2015.

Velmur Management Pte Ltd (Velmur) and Transatlantic Partners Pte. Ltd (Transatlantic); Dandong Chengtai Trading Co. Ltd (Dandong) also known as Dandong Zhicheng Metallic Material Co., Ltd. On August 22, 2017, in conjunction with OFAC's DPRK-related sanctions, the DOJ initiated similar forfeiture actions involving more than $11 million against 1) Velmur, a Singapore-based company, and Transatlantic and 2) Dandong, a company in Dandong, China.[11] The forfeiture complaints allege, "(T)he companies have participated in schemes to launder U.S. dollars on behalf of sanctioned North Korean entities….(and) the companies participated in financial transactions in violation of the International Emergency Economic Powers Act

[9] *See* "United States Files Complaint to Forfeit More Than $1.9 Million From China-Based Company Accused of Acting as a Front for Sanctioned North Korean Bank" (June 2017).
[10] At the time of this forfeiture action, Foreign Trade Bank was a U.S. designated entity; *see* https://www.treasury.gov/press-center/press-releases/Pages/jl1876.aspx.
[11] *See* "United States Files Complaints to Forfeit More Than $11 Million From Companies That Allegedly Laundered Funds To Benefit Sanctioned North Korean Entities" (August 2017) (noting that "the complaints are the first filed actions based on the 2016 North Korea Sanction and Policy Enhancement Act.") For information on the OFAC designation of IPC, see https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170601.aspx.

(IEEPA), the North Korean Sanctions and Policy Enhancement Act of 2016, and federal conspiracy and money laundering statutes." In the case of Velmur and Transatlantic, the companies acted as fronts for designated North Korean banks to facilitate U.S. dollar payments to an OFAC-sanctioned Russian oil products supplier involved in the shipping oil and other petroleum products to the DPRK. The Dandong complaint also involved the facilitation of U.S. dollar payments to benefit an OFAC-designated entity, the North Korean Workers Party, through the purchase of Chinese coal.

Red Flags of Potential North Korean Illicit Financial Activity

Many North Korean-related front companies, financial representatives, and corporate service providers working on behalf of the North Korean government often share similar characteristics. While none of these characteristics are *per se* indicative of North Korean involvement, financial institutions may wish to consider treating these characteristics as red flags to ensure that a financial institution's correspondent accounts are not being utilized by entities or other financial facilitators on behalf of North Korean financial institutions and the DPRK. These red flags also will assist financial institutions in identifying potentially suspicious transactions that are required to be reported promptly to FinCEN.

Geography: As illustrated above, many North Korean front companies, banking and financial representatives, and corporate service providers used by the North Korean government are based in China or use Chinese banks to facilitate the movement of illicit funds on behalf of the North Korean government.

- **Financial Representatives Areas of Activity:** These representatives are typically North Korean-born and often use Chinese aliases or Chinese facilitators to establish and operate bank accounts and front companies, particularly in the Liaoning province and the Hong Kong Special Administration Region. Each representatives may appear as a corporate officer of multiple, seemingly unrelated, front companies that also often transact with each other. North Korean representatives may also appear as authorized signers for accounts maintained by the front companies.

- ***Corporate Registration and Shared Business Addresses*:** Based on information from the UN Report and other information available to Treasury, a number of front and shell companies operating on behalf of the North Korean government are registered in either 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. Additionally, front company addresses are frequently recycled and used for multiple business registrations. A key example of this is the Jiadi Square area in the city of Dandong, Liaoning province. The OFAC-sanctioned corporation Dandong Hongxiang Industrial Development Co Ltd, and several suspected shell companies, maintained Jiadi Square addresses, which is also home to North Korea's Dandong-based consulate.

- ***Liaoning-Based Banking***: The proximity of the Chinese province of Liaoning to the North Korean border makes it an attractive location for North Korean illicit actors to access the international financial system. FinCEN has observed North Korean-related financing involving correspondent account-transactions conducted by, or on behalf of, Liaoning-based banks, including, but not limited to, institutions located in the cities of Dalian, Dandong, Jinzhou, and Shenyang. For example, FinCEN recently issued a proposed Section 311 rulemaking against Bank of Dandong, which is located in the Liaoning province. FinCEN found that Bank of Dandong has participated in obfuscating transactions made on behalf of U.S.- and UN-designated North Korean entities, enabling them to access U.S. correspondent accounts in circumvention of sanctions.[12]

Surge Activity Cycles: North Korean representatives 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 company (Company B, which shares an address with Company A), pays the same beneficiary. Reviewing the timing of transactions and associated payees may allow financial institutions to determine whether seemingly unrelated companies are being utilized for this type of financial cycling.

Common Front Companies and Supporting Indicators: FinCEN has identified that shipping and import/export businesses are often employed as fronts for illicit North Korean activity. Law enforcement information available to FinCEN has identified that textile, garment, fishery, and seafood businesses are also frequently listed as the business lines for various front companies. The UN Report also highlighted the North Korean

[12] *See* Footnote 6.

government's reliance on coal exports to access foreign currency. Other potential related indicators include:

- ***Companies Sharing Owners or Managers, Phones, or Employees***: DPRK-linked financial facilitators often establish and use multiple companies with the same owners or managers. These companies also frequently share addresses, telephone numbers, and employees, and they may transact with similar business partners. The use of multiple companies provides financial facilitators with alternatives in the event that one company is compromised. Multiple companies also allow financial facilitators to divert attention from any particular company, avoiding scrutiny, and increasing their ability to launder money. The Department of Justice's complaint against OFAC-designated Mingzheng highlighted an example of companies sharing managers and employees. In addition, Luo Chuanxu, a U.S.-designated Chinese national, allegedly established multiple front companies to facilitate payments on behalf of UN- and U.S.-designated Korea Kwangsong Banking Corp (KKBC). Luo allegedly facilitated numerous payments for both Dandong Hongxiang Industrial Development (DHID), which was designated by OFAC in September 2016, and Mingzheng, which OFAC designated in August 2017.[13]

- ***Substantial Financial Activity Unrelated to Stated Areas of Business***: The North Korean front companies often lack a stated business purpose, and the payments they receive for products and services are unrelated to an entity's specified lines of business. For example, as noted in the UN Report and highlighted in the DOJ complaint against Zhicheng, one company (Company A) imports coal from the DPRK—without prepaying for it—and resells it to coal customers around the world. Company A then retains the proceeds of these U.S. dollar sales, including the money owed to the DPRK. The DPRK subsequently sends payment instructions to Company A for items the regime would like to purchase. Company A then uses the retained proceeds to purchase the items for export to the DPRK. The items are typically in unrelated industries, such as bulk commodities (sugar, rubber, petroleum products, soybean oil), cell phones, luxury items, or dual-use technology.

- ***Lack of Online Presence***: Businesses serving as front companies for illicit North Korean activity frequently do not maintain a website or other online presence despite their significant transactions.

Chinese-North Korean Joint Ventures: Joint ventures of foreign companies may try to provide financial services or operate as subsidiaries of North Korean entities and banks.[14] UNSCR 2375 prohibits the opening, maintenance, or operation of joint ventures with the DPRK.

[13] *See* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20160926.aspx and https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170822.aspx, respectively.
[14] *See* Footnote 7.

Regulatory Obligations for U.S. Financial Institutions

Prohibition on Use of Correspondent Accounts involving North Korean Financial Institutions

FinCEN's November 2016 Section 311 action against the DPRK prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, North Korean banking institutions.[15] Under this Section 311 action, covered financial institutions must take reasonable steps to not process a transaction for the correspondent account of a foreign bank in the United States if such a transaction involves a North Korean financial institution.

Special Due Diligence of Correspondent Accounts

31 CFR § 1010.659 also requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving North Korean financial institutions. At a minimum, that special due diligence must include:

- Notifying those foreign correspondent account holders, which the covered financial institution knows or has reason to believe provide services to a North Korean financial institution, that they may not provide a North Korean financial institution with access to the correspondent account maintained at the covered financial institution;[16] and,
- Taking reasonable steps to identify any use of its foreign correspondent accounts by a North Korean financial institution, to the extent that such use can be determined from transactional records maintained in the covered financial institution's normal course of business.[17]

Covered financial institutions shall take a risk-based approach when deciding what, if any, other due diligence measures it reasonably must adopt to guard against the use of its foreign correspondent accounts to process transactions involving North Korean financial institutions.[18]

Covered financial institutions that know or have reason to believe that a foreign bank's correspondent account has been or is being used to process transactions involving a North Korean financial institution must take all appropriate steps to further investigate and prevent such access, including the notification of its correspondent account holder (as mentioned above) and, where necessary, termination of the correspondent account.[19]

Suspicious Activity Reporting

Consistent with suspicious activity reporting requirements in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be

[15] *See* 81 FR 35441 (June 2016) and 31 CFR § 1010.659.
[16] 31 CFR § 1010.659(b)(3)(i)(A).
[17] 31 CFR § 1010.659(b)(3)(i)(B).
[18] 31 CFR § 1010.659(b)(3)(ii).
[19] 31 CFR § 1010.659(b)(3)(iii).

expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report (SAR).[20]

The presence or absence of a red flag in any given transaction is not by itself determinative of whether a transaction is suspicious. Due to some similarities with legitimate financial activities, financial institutions may want to consider evaluating indicators of potential DPRK-related illicit activity in combination with other red flags and factors before making determinations of suspiciousness. Financial institutions are encouraged to use previous FinCEN advisories and guidance related to the DPRK as a reference when evaluating potential suspicious activity.[21] Financial institutions may also want to consider the specifics of their own risk profiles and business models as those relate to the guidance and red flags outlined in this advisory.

In evaluating whether certain transactions are suspicious and related to North Korean illicit finance, financial institutions are encouraged to share information with one another, as appropriate, either for the purposes of filing a joint SAR or under Section 314(b) of the USA PATRIOT Act.[22] Section 314(b) establishes a voluntary information sharing mechanism allowing financial institutions to share information with one another regarding possible terrorist activity or money laundering and provides financial institutions with the benefit of a safe harbor from liability that might not otherwise exist with respect to the sharing of such information.[23]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov. ***Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

###

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

---

[20] 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
[21] FinCEN Advisories pertaining to the DPRK: FIN-2013-A005 (July 2013), FIN-2009-A002 (June 2009), and FinCEN Advisory – Issue 40 (December 2005).
[22] *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2)(i), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2) regarding joint SAR sharing. See Pub. L. No. 107-56, § 314(b) promulgated under 31 CFR § 1010.540 regarding Section 314(b) voluntary information sharing.
[23] For further guidance related to the 314(b) Program, please see FinCEN's Section 314(b) Fact Sheet and FIN-2009-G002 "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act" (June 2009).