

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

<hr/>)
UNITED STATES OF AMERICA,)
U.S. Attorney’s Office)
555 Fourth Street, NW)
Washington, DC 20530,)
)
Plaintiff,)
)
v.)
)
\$6,999,925.00 OF FUNDS ASSOCIATED)
WITH VELMUR MANAGEMENT PTE)
LTD,)
)
Defendant In Rem, and)
	Civil Action No. _____)
)
VELMUR MANAGEMENT PTE. LTD.,)
2 Marina Boulevard, #66-08)
The Sail @ Marina Bay)
Singapore (018987),)
)
TRANSATLANTIC PARTNERS PTE. LTD.,)
10 Anson Road, #29-05A)
International Plaza)
Singapore (079903),)
)
Defendants.)
<hr/>)

VERIFIED COMPLAINT FOR FORFEITURE *IN REM* AND CIVIL COMPLAINT

COMES NOW, Plaintiff, the United States of America, by and through the United States Attorney for the District of Columbia, and brings this verified complaint for forfeiture in a civil action *in rem* against \$6,999,925.00 associated with Velmur Management Pte. Ltd (“Velmur”) (the “Defendant Funds”), which is in the control of the U.S. government, and civil complaint *in personam* against Velmur and Transatlantic Partners Pte. Ltd. (“TransAtlantic”) (collectively, the “Defendant Entities”) and alleges as follows:

NATURE OF ACTION AND THE DEFENDANTS *IN REM* AND *IN PERSONAM*

1. This action arises out of an investigation by the Federal Bureau of Investigation (“FBI”) of a scheme by Velmur and TransAtlantic -- companies sanctioned by the U.S. Department of the Treasury -- to launder U.S. dollars through the United States on behalf of sanctioned entities in the Democratic People’s Republic of Korea (“DPRK” or “North Korea”).

2. As described in detail below, North Korea has used sanctioned state-run banks 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 these banks and their sanctioned affiliates.

3. Additionally, companies that contract with North Korean entities, or make arrangements to receive funds from sanctioned state-run banks, frequently set up their own front companies to receive funds related to North Korean contracts.

4. This action relates to funds that were transferred through different companies and remitted to Velmur to remit funds to JSC Independent Petroleum Company (“IPC”), a Russian petroleum products supplier. The U.S. Department of the Treasury recently sanctioned IPC for contracting to provide petroleum products to North Korea.

5. Specifically, Velmur was a counterparty to seven illicit wire transfers in U.S. dollars, totaling \$6,999,925.00, which were routed through U.S. correspondent banking accounts, and which comprise the Defendant Funds.

6. These transfers were in violation of the International Emergency Economic Powers Act (“IEEPA”), codified at 50 U.S.C. § 1701, *et seq.*, the prohibitions of the North Korea Sanctions and Policy Enhancement Act of 2016 (“NKSPEA”), codified at 22 U.S.C. § 9201, *et seq.*, the conspiracy statute, codified at 18 U.S.C. § 371, and the federal money laundering statute, codified at 18 U.S.C. § 1956(a)(2)(A), (h).

7. The Defendant Funds are subject to forfeiture pursuant to: 18 U.S.C. §§ 981(a)(1)(C), 18 U.S.C. § 981(a)(1)(I), and 18 U.S.C. § 981(a)(1)(A).

8. The Defendant Funds are subject to a money laundering monetary penalty pursuant to 18 U.S.C. § 1956(b).

JURISDICTION AND VENUE

9. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1345 and 1355.

10. Venue is proper pursuant to 28 U.S.C. §§ 1355(b)(1)(A) and 1391(b)(2) because the acts and omissions giving rise to the forfeiture took place in the District of Columbia. The Defendant Funds are currently held in a bank account in the United States. The Defendant Entities and co-conspirators failed to seek or obtain licenses from the Department of the Treasury's Office of Foreign Asset Control ("OFAC"), which is located in Washington, D.C., for conducting transactions with these funds, for which licenses were required under United States law.

11. Velmur is a corporation purportedly headquartered in Singapore. As detailed herein, Velmur purposefully directed its illicit actions towards the United States by routing funds through bank accounts located in this country.

12. TransAtlantic is a corporation purportedly headquartered in Singapore. As detailed herein, TransAtlantic purposefully directed its illicit actions towards the United States by routing funds through bank accounts located in this country.

STATUTORY FRAMEWORK

I. THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT.

13. This investigation relates to violations of regulations issued pursuant to IEEPA. By virtue of IEEPA, the President of the United States was granted authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. *See* 50 U.S.C.

§§ 1701, 1702. Pursuant to that authority, the President and the executive branch have issued orders and regulations governing and prohibiting certain transactions, including financial transactions, with North Korea by U.S. persons or involving U.S.-origin goods.

14. Pursuant to 50 U.S.C. § 1705(a), “[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter,” and pursuant to Section 1705(c), “[a] person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act described in subsection (a) of this section shall” be guilty of a crime. 18 U.S.C. § 371 criminalizes a conspiracy to commit offenses against the United States.

15. On November 14, 1994, pursuant to IEEPA, the National Emergencies Act, and the Arms Export Control Act, the President issued Executive Order (“E.O.”) 12938 finding that “the proliferation of nuclear, biological and chemical weapons (‘weapons of mass destruction’) and of the means of delivering such weapons, constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and [declaring] a national emergency to deal with that threat.”

16. By the authority vested in the President by IEEPA and the National Emergencies Act, on or about June 28, 2005, the President signed Executive Order (“E.O.”) 13382, which takes additional steps with respect to the national emergency described and declared in E.O. 12938, to target proliferators of weapons of mass destruction (“WMD”) and their support networks and deny designated WMD proliferators access to the U.S. financial and commercial system. As part of E.O. 13382, a number of North Korean entities were identified by the President as WMD proliferators and listed in the Annex to E.O. 13382 as being subject to U.S. sanctions. This blocking program initially applied to eight organizations in North Korea, Iran, and Syria

17. On April 13, 2009, the U.S. Department of the Treasury (“Treasury”) promulgated the Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. §544.101, et seq., (the “WMDPSR”), which blocked, as a function of law, any property and interests of property, belonging to individuals and entities listed in or designated pursuant to E.O. 13382, who were concurrently placed on Treasury’s Office of Foreign Assets Control’s (“OFAC”) Specially Designated Nationals and Blocked Persons List (the “SDN list”), see 31 C.F.R. §544.201(a). The terms “property” and “property interests” include but are not limited to money, bank deposits, guarantees, and other financial instruments. *See* 31 C.F.R. §544.308.

18. Pursuant to 31 C.F.R. § 544.405, no U.S. person may provide financial or other services for the benefit of a person or entity added to the SDN list pursuant to the authorities provided by E.O. 13382, except as authorized or licensed by OFAC. Additionally, a non-U.S. person may not cause the provision of financial or other services by a U.S. person for the benefit of a person or entity so designated under these sanctions, except as authorized or licensed by OFAC. *See* 31 C.F.R. § 544.405; 50 U.S.C. § 1705.

19. OFAC has designated numerous North Korean banks. In March 2013, OFAC designated North Korea’s Foreign Trade Bank pursuant to E.O. 13382. In December 2016, OFAC designated North Korea’s Koryo Credit Development Bank a/k/a Daesong Credit Development Bank pursuant to E.O. 13722.

II. THE NORTH KOREA SANCTIONS AND POLICY ENHANCEMENT ACT OF 2016

20. On February 18, 2016, President Obama signed into law the NKSPEA.

21. Within the NKSPEA, Congress found that “[t]he Government of North Korea has been implicated repeatedly in money laundering[.]” 22 U.S.C. § 9201(a)(3).

22. NKSPEA states that the President “shall designate” any person that “knowingly, directly or indirectly, engages in money laundering . . . that supports the Government of North Korea or any senior official or person acting for or on behalf of that Government.” 22 U.S.C. § 9214(a)(6).

III. BANK SECRECY ACT CRIMINALIZES CORRESPONDENT BANKING WITH NORTH KOREAN FINANCIAL INSTITUTIONS

23. According to the U.S. Department of the Treasury (“Treasury Department”), the global financial system, trade flows, and economic development rely on correspondent banking relationships. To protect this system from abuse, U.S. financial institutions must comply with national anti-money laundering requirements set forth in the Bank Secrecy Act as well as sanctions programs administered by OFAC. The Financial Crimes Enforcement Network (“FinCEN”) is responsible for administering the Bank Secrecy Act in furtherance of its mission to safeguard the U.S. financial system from illicit use.

24. Nearly all U.S. dollar transactions conducted by foreign financial institutions are processed via correspondent bank accounts in the United States. Correspondent bank accounts are broadly defined to include any account established for a foreign financial institution to receive deposits from, or to make payments or disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution. *See* 31 C.F.R. § 1010.605. The Bank Secrecy Act requires U.S. financial institutions to take anti-money laundering measures for foreign financial institutions engaged in correspondent banking of U.S. dollar transactions.

25. The Bank Secrecy Act broadly defines foreign financial institutions to include dealers of foreign exchange and money transmitters in a manner not merely incidental to their business. *See* 31 C.F.R. 1010.605(f).

26. Section 311 of the USA PATRIOT Act, codified at 31 U.S.C. § 5318A as part of the Bank Secrecy Act, gives FinCEN a range of options, called special measures, that can be adapted to target specific money laundering and terrorist financing concerns. A Section 311 finding and the related special measure are implemented through various orders and regulations incorporated into 31 C.F.R. Chapter X. In order to protect the integrity of the U.S. financial system, a special measure imposed under Section 311 prevents financial institutions from causing U.S. financial institutions from engaging in any type of financial transaction with an entity within the jurisdiction deemed an area of money laundering concern.

27. In May 2016, FinCEN made a Section 311 finding against North Korea. Specifically, FinCEN's finding deemed *the entire North Korean financial sector* as a jurisdiction of primary money laundering concern. *See* Federal Register, Vol. 81, No. 107 (June 3, 2016).

28. In November 2016, FinCEN implemented the most severe special measure against the entire North Korean financial sector. *See* Federal Register, Vol. 81, No. 217 (November 9, 2016); 31 CFR 1010.659. The special measure bars U.S. financial institutions from maintaining a correspondent account for any North Korean financial institution or any party acting on its behalf. The special measure also requires covered financial institutions to 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. Because of the finding that the entire North Korea financial sector was a primary money laundering concern, FinCEN cut all North Korean financial institutions – and entities acting on their behalf – off from any trade in U.S. dollar transactions via correspondent banking. One expert described the effect of such action is to cut the target off from trade in dollars, isolating it from worldwide business.

29. A violation of the Section 311 finding, codified at 31 U.S.C. § 5318A, or of the regulations published at 31 C.F.R. § 1010.659, is punishable criminally pursuant to 31 U.S.C. § 5322.

IV. MONEY LAUNDERING VIOLATIONS

30. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

31. 18 U.S.C. § 1956(a)(2)(A) (the international promotional money laundering statute) criminalizes transporting, transmitting, and transferring, and attempting to transport, transmit, and transfer a monetary instrument or funds to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity.

32. Pursuant to 18 U.S.C. § 1956(c)(7)(A), the term “specified unlawful activity,” includes violations of 18 U.S.C. § 1343 (relating to wire fraud) and 18 U.S.C. § 1344 (relating to bank fraud).

a. As noted above, U.S. financial institutions are barred, pursuant to the section 311(a) special measure, from engaging in financial transactions with North Korean financial institutions. As the FinCEN finding noted, North Korea makes “extensive use of deceptive financial practices, including the use of shell and front companies to obfuscate the true originator, beneficiary, and purpose behind its transactions,” in part “to evade international sanctions.” *See* Federal Register, Vol. 81, No. 217 at 78716, 78718. North Korean entities have attempted to circumvent the section 311(a) ban by using foreign front companies to engage in financial transactions on their behalf. These financial transactions would be in violation of 22 U.S.C. § 9214, if the parties openly acknowledged the involvement of the North Korean entities. Instead, the true North Korean counterparties to these transactions remain concealed in order to allow the U.S. dollars to be processed.

b. This constitutes wire fraud, as the false transactions occur via wire, and are done in part to defraud the U.S. Treasury department, which has forbidden such transactions.

c. This also constitutes wire fraud and bank fraud, as the false transactions occur via wire, and are done in part to defraud U.S. financial institutions, which are barred from conducting such transactions, and could face civil and criminal penalties for not detecting these transactions.

d. But for this scheme to defraud U.S. correspondent banks, North Korean foreign financial institutions would not be able to engage in U.S. dollar transactions.

33. Pursuant to 18 U.S.C. § 1956(c)(7)(D), the term “specified unlawful activity,” includes violations of IEEPA (including violations of any license, order, regulation, or prohibition issued under IEEPA), and offenses under section 104(a) of NKSPEA (relating to prohibited activities with respect to North Korea).

a. One of the primary means U.S. financial institutions use to comply with national anti-money laundering procedures is through regular consultation of OFAC’s SDN list. The SDN list contains a number of persons (individuals and entities) designated under OFAC’s Non-Proliferation Sanctions and North Korea Sanctions programs, including North Korean weapons trading firms, North Korean Government officials, North Korean financial institutions, and nationals of other foreign countries supporting North Korea’s weapons of mass destruction programs.

b. Criminals are aware of the SDN list and that U.S. financial institutions are obligated to conduct due diligence of their clients, in an attempt to prevent sanctioned parties from transacting in U.S. dollars. As a result, criminals employ front companies to

engage in laundered transactions on their behalf, in order to prevent banks from learning that the sanctioned entity is a party to the transaction.

c. North Korean financial facilitators in particular are aware of these designation lists and of U.S. financial institutions' due diligence obligations. In turn, these North Korean entities have a documented practice of using front companies to avoid the imposition of designations and blockings, which may occur pursuant to IEEPA and NKSPEA. These opaque U.S. dollar transactions by front companies promote IEEPA and NKSPEA violations, by preventing the imposition of sanctions. That is, if the transactions were not conducted in a fashion to conceal the involvement of the North Korean entities, the transactions would meet the criteria for designation of the involved parties. But, because the parties conceal their laundering of funds, designations are impeded. Financial transactions by North Korean financial facilitators facilitate a conspiracy to circumvent designations under IEEPA and NKSPEA.

V. FORFEITURE

34. Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of IEEPA is subject to civil forfeiture.

35. Pursuant to 18 U.S.C. § 981(a)(1)(I), any property, real or personal, that is involved in a violation or attempted violation, or which constitutes or is derived from proceeds traceable to a prohibition imposed pursuant to section 104(a) of NKSPEA, is subject to civil forfeiture. NKSPEA allows for forfeiture of conduct other than a violation of NKSPEA. Specifically, the first part of the statute focuses on violations of the statute; however, the second prong mandates forfeiture for the broad prohibitions imposed by section 104(a).

36. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction, in violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to civil forfeiture.

37. Forfeiture pursuant to violations of the above money laundering statute and NKSPEA apply to a larger class of property than forfeiture under 18 U.S.C § 981(a)(1)(C), because such forfeitures are not limited to proceeds of the crime. Rather, these forfeitures include property “involved in” the crime or the attempted crime, which can include “clean” or “legitimate” money that is commingled with “tainted” money derived from illicit sources.

VI. MONETARY PENALTY

38. Pursuant to 18 U.S.C. § 1956(b), whoever conducts or attempts to conduct a transaction described in §§ 1956 (a)(1) or (a)(3), or a transportation, transmission, or transfer described in § 1956(a)(2), is liable to the United States for a civil penalty of not more than the greater of the value of the property, funds, or monetary instruments involved in the transaction or \$10,000.

FACTUAL ALLEGATIONS

I. THE NORTH KOREAN FINANCIAL SECTOR LAUNDERS FUNDS FOR SANCTIONED ENTITIES AND TO PROMOTE THEIR PROLIFERATION PROGRAMS

A. BACKGROUND

39. The focus of this action is the money laundering activities of sanctioned state-run North Korean banks and co-conspirator unsanctioned companies located outside of North Korea that act as financial institutions by transacting in U.S. dollars on behalf of the North Korean banks (“North Korean financial facilitators”). The money laundering conspiracy benefits entities in North Korea for the purpose of advancing procurement and financial activity for the government of North Korea in contravention of U.S. and United Nations prohibitions on such activity.

40. The United States House of Representatives' Foreign Affairs Committee released a report which concluded that North Korea remains dependent on its access to the international financial system, which in turn reflects a dependency on the U.S. dollar. *See* House Rept. 114–392, at 18 (January 11, 2016). This is because “[t]he vast majority of international transactions are denominated in dollars, the world’s reserve currency.” *Id.* North Korea continues to transact in U.S. dollars for many of its international and domestic business transactions, by hiding “its dollar transactions within the dollar-based financial system using false names, shell companies, and other deceptive practices.” *Id.*

B. NORTH KOREAN FINANCIAL INSTITUTIONS CONTINUE TO LAUNDER U.S. DOLLARS

41. The North Korean financial sector is comprised of state-controlled financial institutions that use “front companies to conduct international financial transactions that support the proliferation of weapons of mass destruction (WMD) and the development of ballistic missiles in violation of international and U.S. sanctions,” and because these institutions are subject to “little or no bank supervision or anti-money laundering or combating the financing of terrorism (“AML/CFT”) controls.” Federal Register, Vol. 81, No. 217 at 78715.

42. FinCEN’s Section 311 action included a finding that North Korean financial institutions continued to access the U.S. financial system, in violation of the U.S. sanctions. The finding further stated that millions of U.S. dollars’ worth of illicit transactions were flowing through U.S. correspondent accounts in spite of the sanctions because of the coordinated use of money laundering techniques to conceal North Korea’s involvement and the processing of the payments by North Korean financial institutions. Specifically, FinCEN found that:

North Korea continues to advance its nuclear and ballistic missile programs in violation of international treaties, international censure and sanctions measures, and U.S. law. North Korea does this using an extensive overseas network of front companies, shell companies,

joint ventures, and opaque business relationships. North Korea conducts almost no banking in true name in the formal financial system given that many of its outward facing agencies and financial institutions have been sanctioned by the United States, the United Nations, or both.

While none of North Korea's financial institutions maintain correspondent accounts with U.S. financial institutions, *North Korea does have access to the U.S. financial system through a system of front companies, business arrangements, and representatives* that obfuscate the true originator, beneficiary, and purpose of transactions. We assess that *these deceptive practices have allowed millions of U.S. dollars of [North Korean] illicit activity to flow through U.S. correspondent accounts.*

Moreover, although U.S. and international sanctions have served to significantly isolate North Korean banks from the international financial system, the North Korean government continues to access the international financial system to support its [weapons of mass destruction] and conventional weapons programs. This is made possible through its use of aliases, agents, foreign individuals in multiple jurisdictions, and a long-standing network of front companies and North Korean embassy personnel which support illicit activities through banking, bulk cash, and trade. Front company transactions originating in foreign-based banks have been processed through correspondent bank accounts in the United States and Europe.

Federal Register, Vol. 81, No. 107 at 35442 (emphasis added).

43. In its 2017 annual report, the Panel of Experts established by the U.N. Security Council to investigate compliance with sanctions against North Korea ("Panel of Experts") noted the central role of North Korean banks in allowing North Korean entities to continue to illegally access the U.S. financial system. Specifically, the report states that:

[T]he Democratic People's Republic of Korea has continued to access the international financial system to support its activities. Financial networks of the Democratic People's Republic of Korea have adapted to these sanctions, using evasive methods to maintain access to formal banking channels and bulk cash transfers to facilitate prohibited activities.

...

The Panel has identified multiple ways in which *the financial institutions and networks of the Democratic People's Republic of Korea access the international banking system to engage in activities in violation and/or evasion of the provisions of the resolutions:*

- *Banks of the Democratic People's Republic of Korea, including designated banks, hold correspondent or payable-through accounts with foreign banks*
- Banks of the Democratic People's Republic of Korea form joint ventures with foreign companies
- Foreign companies establish banks inside the Democratic People's Republic of Korea
- *Banks of the Democratic People's Republic of Korea, including designated banks, maintain representative offices abroad.*

2017 Report of the Panel of Experts, at 79-80 (emphasis added).

44. The front companies that launder funds on behalf of sanctioned North Korean banks are supporting sanctioned North Korean end users, including North Korean military and North Korean weapons programs. In the 2013 designation of North Korea's Foreign Trade Bank ("FTB"), the Treasury Department noted that the North Korean bank was "a key financial node in North Korea's WMD [weapons of mass destruction] apparatus." <https://www.treasury.gov/press-center/press-releases/Pages/j11876.aspx>. On June 1, 2016, the Treasury Department again noted that "North Korea uses *state-controlled financial institutions* and front companies to conduct international financial transactions that support the proliferation and development of [weapons of mass destruction] and ballistic missiles." <https://www.treasury.gov/press-center/press-releases/Pages/j10471.aspx> (emphasis added).

C. FTB IS A PRIMARY VEHICLE IN NORTH KOREA'S ILLICIT MONEY LAUNDERING NETWORK

45. U.N. and OFAC sanction designation publications reveal that FTB is responsible for handling foreign currency transactions for North Korea's government ministries and their subordinate trading companies. Reforms undertaken in the early and mid-2000s codified FTB's role and relevance in North Korea's banking industry. In approximately 2000, FTB developed and instituted an inter-bank clearing system in North Korea. After the institution of this system, North Korean banks were generally required to maintain currency clearing accounts at FTB. These accounts are used to clear transactions among North Korea's commercial banks. This reform, in effect, channeled transactions from North Korea's arms exports and luxury goods imports through FTB.

46. In the March 2013 designation of FTB, OFAC noted that FTB is a state-owned bank and "acts as North Korea's primary foreign exchange bank." The designation further noted that North Korea uses FTB to facilitate millions of dollars in transactions on behalf of actors linked to its proliferation network.

47. FTB continues to act as the umbrella bank for foreign currency transactions in North Korea. In fact, FTB sets the official exchange rate for North Korean currency to foreign currency.

48. The FinCEN Section 311 action made specific findings as to FTB, that is:

The following examples are representative of the activities of FTB and its front companies. Between 2008 and 2012, FTB used front companies in multiple countries to make and receive payments equivalent to tens of millions of U.S. dollars. In 2011, an FTB front company was involved with U.S.-designated [Korea Kwangson Banking Corp.] and Korea 5 Trading Corporation, a subordinate of U.S. and UN-designated Korea Ryonbong General Corporation, in financial dealings totaling several millions of U.S. dollars. *The same*

FTB front company processed transactions through U.S. correspondent accounts as recently as April 2014.

Federal Register, Vol. 81, No. 107 at 35445 (emphasis added). The investigation revealed transactions by FTB front companies as recently as May 2017.

49. This FinCEN report alone demonstrates that FTB has illegally laundered “millions of U.S. dollars,” in violation of the U.S. sanctions. Moreover, this report shows that even prior to designation, FTB was laundering U.S. dollar transactions on behalf of sanctioned North Korean entities.

D. NORTH KOREAN ENTITIES CONTINUE TO LAUNDER U.S. DOLLARS VIA FRONT COMPANIES

50. Designated North Korean companies continue to transact in U.S. dollars via front companies. The Panel of Experts noted that transactions originating in foreign banks have been processed through correspondent accounts in the United States via front companies, which are “often registered by non-nationals, who also use indirect payment methods and circuitous transactions dissociated from the movement of goods or services to conceal their activity.” 2016 Report of the Panel of Experts, at 62. North Korean front companies are instructed to strip all information tying their U.S. dollar transactions to North Korea, in order to prevent the Treasury Department from blocking the transactions. *Id.* at 66.

51. This use of front companies was recently highlighted by the Panel of Experts. The report stated that:

The financial sanctions notwithstanding, the Democratic People’s Republic of Korea continues to gain access to and exploit the global international financial system (including banking and insurance) through reliance on aliases, agents, foreign individuals in multiple jurisdictions, and a long-standing network of front companies and embassy personnel, all of which support illicit activities through banking, bulk cash and trade.

United Nations Security Council’s February 24, 2016 Report of the Panel of Experts, at 62.

52. FinCEN noted that “one way that North Korean financial institutions and networks access the international banking system is through trading companies, including designated entities, that are linked to North Korea. These trading companies open bank accounts that perform the same financial services as banks, such as maintaining funds on deposit and providing indirect correspondent bank account services.” *Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern*, 82 Fed. Reg. 31,537 (July 7, 2017).

53. North Korean financial facilitators frequently establish and maintain offshore U.S. dollar accounts for the purposes of remitting wire transfers denominated in U.S. dollars on behalf of sanctioned North Korean entities and their related front companies. *See, e.g.*, Federal Register, Vol. 81, No. 107 at 35442 (“While none of North Korea’s financial institutions maintain correspondent accounts with U.S. financial institutions, North Korea does have access to the U.S. financial system through a system of front companies, business arrangements, and representatives that obfuscate the true originator, beneficiary, and purpose of transactions. We assess that these deceptive practices have allowed millions of U.S. dollars of North Korean illicit activity to flow through U.S. correspondent accounts.”). These U.S. dollar wire transfers originate from financial institutions located outside the United States, which clear them through the United States using established correspondent banking relationships with financial institutions in the United States.

54. Once the wire transfers are cleared through the U.S. financial system, payments are transmitted to offshore U.S. dollar accounts maintained by front companies on behalf of the foreign financial institutions and the North Korean entities and/or parties from whom the North Korean sanctioned entities are seeking goods.

II. TARGET FOREIGN FINANCIAL FACILITATORS: VELMUR AND TRANSATLANTIC

55. The scheme to launder funds is as follows: (1) designated North Korean banks direct front companies, such as Transatlantic, to send U.S. dollars to Velmur; (2) the front companies, such as Transatlantic, wire U.S. dollars to Velmur; (3) Velmur then wires the U.S. dollars to IPC; and (4) IPC then ships the gasoil to North Korea.

A. INTRODUCTION OF DEFENDANT PROPERTIES

56. Defendant properties are identified as follows:

#	Date	Wire Amount	Party Sending Wire	Party Receiving Wire	Wire Detail
1	05/05/17	\$1,199,975.00	Company 1	Velmur	Prepayment for Gasoil Against Invoice 1EW DD 27.04.2017
2	05/09/17	\$1,099,975.00	Company 1	Velmur	Prepayment for Gasoil Against Invoice 1EW DD 27.04.2017
3	05/10/17	\$999,975.00	Company 1	Velmur	Prepayment for Gasoil Against Invoice 1EW DD 27.04.2017
4	05/12/17	\$1,200,000.00	Company 2	Velmur	Prepayment for Gasoil Against Invoice 1EW DD 27.04.2017
5	05/12/17	\$1,510,000.00	TransAtlantic	Velmur	Prepayment for Gasoil Against Contract 05/06.16 DD 06.12.2016
6	05/24/17	\$500,000.00	Company 3	Velmur	Prepayment for Gasoil Against Contract 1 GP/13 DD 25.4.2017
7	06/01/17	\$490,000.00	TransAtlantic	Velmur	Prepayment for Gasoil Against Contract 5TP DD 11.5.2017
		\$6,999,925	Total		
	05/19/17	IPC shipments of gasoil to Velmur for the benefit of North Korea			

i. Velmur

57. On August 22, 2017, OFAC designated Velmur for operating in the energy industry in the North Korean economy, by importing gasoil to North Korea. OFAC designated Velmur for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, TransAtlantic (described below). The designation noted that Velmur has sold gasoil to North Korea and that it has attempted to use the U.S. financial system to send millions of dollars in payments on behalf of North Korea-related transactions. “Gasoil” is often used to refer to a distilled petroleum product such as gasoline and/or diesel fuel.

58. Velmur was registered in Singapore in November 2014. A confidential reliable source (CS-1) revealed that the Velmur is operated in part by Irina Huish, a Russian national who OFAC designated on August 22, 2017, for acting for or on behalf of Velmur, and working with TransAtlantic to evade sanctions on North Korea.

59. Velmur’s self-described principal business activity is “Commercial and Industrial Real Estate Management.” Velmur bears the hallmarks of a front company. That is, it lacks an official website and appears to have little to no web presence. Additionally, law enforcement is unaware of Velmur having a true physical office space, as numerous companies are registered at their official location.

60. A reliable confidential source (CS-2) independently revealed that Velmur has been a recipient of U.S. dollar payments on behalf of North Korean entities -- in particular, FTB, as detailed below.

61. Velmur’s business focuses on facilitating the laundering of funds for North Korean financial facilitators and sanctioned entities. For example:

a. In September 2016, Dandong Zhicheng Metallic Material Co. (“Dandong Zhicheng”) wired \$230,000 to Velmur. Dandong Zhicheng and its related front companies are known to have made payments for FTB. In May 2017, this Court found probable cause existed to believe that Dandong Zhicheng had laundered funds to promote sanctions violations. *See United States v. All Wire Transactions Involving Dandong Zhicheng Metallic Material Company, Ltd.*, No. 17-mj-217-DAR-BAH, 2017 WL 3233062, at *1 (D.D.C. May 22, 2017). On August 22, 2017, OFAC designated Dandong Zhicheng.

b. In July 2016, Ruizhi Resources Limited (“Ruizhi Resources”) wired \$189,980 to Velmur. Ruizhi Resources is a front company for Dandong Zhicheng. Ruizhi Resources and related front companies are known to have made payments for FTB. In May 2017, this Court found probable cause existed to believe that Ruizhi Resources had laundered funds to promote sanctions violations. *See id.*

c. In 2016, a FTB front company made two payments to Velmur totaling more than \$250,000. CS-2 revealed that this company made payments at the direction of FTB. CS-2 revealed that a covert FTB branch representative had previously ordered two payments by this front company to a third party, which payments directly benefited FTB.

d. In 2017, another FTB front company made two payments to Velmur totaling more than \$500,000. CS-2 independently confirmed that this front company made payments at the direction of FTB. CS-2 revealed that a covert FTB branch representative had directed that these two payments be made to Velmur.

62. Velmur’s activities are consistent with FinCEN’s finding that North Korean banks rely on trading companies to open bank accounts that perform the same financial services as banks.

See Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern, 82 Fed. Reg. 31,537 (July 7, 2017).

63. CS-2 further provided information tying FTB to Velmur and the wiring of the Defendant Funds, as further described below.

ii. TransAtlantic

64. TransAtlantic is a front company that a designated North Korean bank has used to send illicit U.S. dollar payments to Velmur.

65. On August 22, 2017, OFAC designated TransAtlantic for operating in the energy industry in the North Korean economy, by importing gasoil to North Korea. OFAC noted that TransAtlantic concluded a contract to purchase fuel oil with Daesong Credit Development Bank, a North Korean bank designated in 2016. The designation also noted that TransAtlantic has attempted to use the U.S. financial system to send millions of dollars in payments on behalf of North Korea-related transactions.

66. TransAtlantic was registered in Singapore in May 2016. CS-1 revealed that TransAtlantic is operated in part by Andrei Serbin, a Russian National who OFAC designated on August 22, 2017. The designation noted that Andrei Serbin worked with Irina Huish of Velmur to purchase gasoil for delivery to North Korea. OFAC also designated, Mikhail Pisklin, a Russian national, who concluded the above referenced contract for Transatlantic with Daesong Credit Development Bank.

67. Transatlantic's self-described principal business activity is "General Wholesale Trade." TransAtlantic bears the hallmarks of a front company. That is, it lacks an official website and appears to have little to no web presence. Additionally, law enforcement is unaware of TransAtlantic having a true physical office space, as numerous companies are registered at their

official location. In fact, the address for TransAtlantic is within the same building used by Company 2.

68. CS-1 revealed that TransAtlantic entered into a contract with Velmur on December 6, 2016, for the purchase by TransAtlantic of 5,000 metric tons of gasoil. CS-1 further revealed that on May 11, 2017, there was an addendum to the original contract. This contract corroborates the relationship between TransAtlantic and Velmur.

69. TransAtlantic's activities are consistent with FinCEN's finding that North Korean banks rely on trading companies to open bank accounts that perform the same financial services as banks. *See Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern*, 82 Fed. Reg. 31,537 (July 7, 2017).

iii. Company 1

70. Company 1 is a front company that a designated North Korean bank has used to send illicit U.S. dollar payments to Velmur.

71. Company 1 appears to have been registered in Hong Kong in December 2008, and is operated by a Chinese national. Bank records show an address for Company 1 in Qingdao City, Shandong Province, China. Company 1 bears the hallmarks of a front company. That is, it lacks an official website and appears to have little to no web presence. Records reveal that Company 1 is listed as being in the machine-tools, parts, and accessories industry, which is unrelated to bulk gasoil importation.

iv. Company 2

72. Company 2 is a front company that a designated North Korean bank has used to send illicit U.S. dollar payments to Velmur.

73. Company 2 appears to have been registered in Singapore in October 2016. Company 2 bears the hallmarks of a front company. That is, it lacks an official website and appears to have little to no web presence. Additionally, law enforcement is unaware of Company 2 having a true physical office space, as numerous companies are registered at their official location. In fact, the address for Company 2 is within the same building used by TransAtlantic.

v. Company 3

74. Company 3 appears to have been registered in Singapore in May 2014. Corporate registry records identify it as a “value added logistics provider” involved with “general wholesale trade.” However, Company 3’s website identifies it as a petrochemical company. Law enforcement is unaware of Company 3 having a true physical office space, as its listed address is a virtual office address shared by many companies. The publically available domain registration information for Company 3’s website indicates it was registered in May 2016 using an anonymization service; however, the domain record indicates the website is hosted by a Russian webhost. A search of Company 3 in public databases that collect data on international import and exports yielded no results.

vi. JSC Independent Petroleum Company (IPC)

75. On June 1, 2017, OFAC designated IPC, a Russian company. The designation noted that IPC had a contract to provide oil to North Korea and reportedly shipped over \$1 million worth of petroleum products to North Korea.

76. During the same time period that TransAtlantic and others entities were wiring payments to Velmur, Velmur remitted money to only one company, IPC, as follows:

Date	Wire Amount	Party Sending Wire	Party Receiving Wire	Wire Detail
02/27/17	\$1,907,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
03/01/17	\$337,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
03/24/17	\$530,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
03/28/17	\$1,370,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
03/31/17	\$200,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
04/07/17	\$790,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
04/19/17	\$369,000.00	Velmur	IPC	Inv 2-1P-044 DD 06.02.2017 For Gasoil
	\$6,853,000	Total		

77. Each payment to IPC included a notation that the payment was related to an invoice for gasoil.

78. A confidential reliable source (CS-3) provided bill of lading information for May 19, 2017, shipments by IPC to Velmur. The cargo was identified as diesel fuel. IPC sent the diesel fuel shipment on tankers departing from Port Vladivostok, Russia. This port is a known waypoint for Russian transshipments to North Korea. Publically available shipping data from May 2017 shows a steady flow of oil tanker traffic from Vladivostok into North Korean east coast ports. In fact, on or about May 17, 2017, North Korea launched a ferry service to the Russian port city of Vladivostok to develop links and boost economic cooperation, according to North Korea's state media. Additional open source reporting reveals that North Korea began relying heavily on Russia for gasoil importation in 2017.

79. The investigation has concluded that North Korea was the destination of the May 19, 2017 transshipments by IPC.

80. As such, it appears that Velmur, while registered as a real estate management company, is in fact a North Korean financial facilitator involved with making illicit payments sourced from front companies, such as Transatlantic, to IPC for the illegal importation of gasoil into North Korea.

B. CONFIDENTIAL SOURCE CONFIRMS VELMUR'S INVOLVEMENT IN LAUNDERING FUNDS FROM NORTH KOREA

81. CS-2 revealed that a clandestine FTB branch located outside of North Korea ordered a \$1.09 million payment to be made via a FTB front company to Velmur. This payment instruction is what led to the wiring of a portion of the Defendant Funds.

82. CS-1 revealed that FTB had records which identified numerous bank accounts belonging to Velmur. A covert FTB branch representative selected Velmur's U.S. dollar account to receive the illicit \$1.09 million payment from FTB's front company.

83. This type of covert payment activity is consistent with how sanctioned North Korean banks work with foreign front companies to procure items in U.S. dollars, which sustains North Korea's proliferation program and economy. This practice was further detailed by the Panel of Experts:

Behind these illicit activities is the continued access of the Democratic People's Republic of Korea to the international banking system. Despite strengthened financial sanctions in 2016, the country's networks are adapting by using greater ingenuity in accessing formal banking channels, as well as bulk cash and gold transfers. *Banks of the Democratic People's Republic of Korea maintain correspondent bank accounts and representative offices abroad and partner with foreign companies in joint ventures. Banks and designated entities of the Democratic People's Republic of Korea make use of broad interwoven networks to undertake procurement and banking activity. Their ability to conceal financial*

activity by using foreign nationals and entities allows them to continue to transact through top global financial centres.

2017 Report of the Panel of Experts, at 1 (emphasis added).

C. INTERNATIONAL WIRES CONFIRM ILLICIT PAYMENTS TO VELMUR

84. Financial records reveal that numerous front companies sent wires to Velmur. In turn, Velmur would wire funds to IPC. Thus, the investigation concluded that the payments, described further below, were illicit U.S. dollar transactions to fund the importation of gasoil that supported the government of North Korea.

i. Company 1

85. On May 5, 2017, Company 1 wired Velmur \$1,199,975.00, with a notation that the money was a “prepayment for gasoil against invoice 1EW DD 27.04.2017.” This payment was consistent with the instructions relayed by CS-2 to wire U.S. dollars to Velmur. The funds comprising this wire make up a portion of the Defendant Funds.

86. Following this May 5, 2017 payment, three additional payments were wired over the next seven days, which all included the same wire notation – “prepayment for gasoil against invoice 1EW DD 27.04.2017.” Company 1 wired two of the additional prepayments to Velmur as follows: \$1,099,975 on May 9, and \$999,975 on May 10. These payments were consistent with the instructions relayed by CS-2 to wire U.S. dollars to Velmur. The funds comprising these two wires make up a portion of the Defendant Funds. Company 2 wired the third additional payment, as described below.

87. The payment for gasoil to Velmur, a “commercial and industrial real estate management” company is outside of Velmur’s purported scope of industry; however, this is consistent with how North Korean entities launder money.

ii. Company 2

88. Company 2 has wired funds to Company 1 in the past. Of particular note, on or about May 2, 2017, Company 2 wired \$350,000 to Company 1. Three days later, Company 1 wired Velmur \$1,199,975.00 (as described above).

89. On May 12, 2017, after the three failed prior payments to Velmur by Company 1, Company 2 attempted a similar payment to Velmur with the same notation: “prepayment for gasoil against invoice 1EW DD 27.04.2017” in the amount of \$1,200,000. This payment was consistent with the instructions relayed by CS-2 to wire U.S. dollars to Velmur. The funds comprising this wire make up a portion of the Defendant Funds.

iii. Additional Illicit Payments to Velmur

90. In addition to the payments from Company 1 and Company 2, two additional companies attempted to make payments to Velmur that also comprise a portion of the Defendant Funds.

91. On May 12, 2017 TransAtlantic wired \$1,510,000 to Velmur with a notation that it was for prepayment for gasoil. This payment was consistent with the instructions relayed by CS-2 to wire U.S. dollars to Velmur. The funds comprising this wire make up a portion of the Defendant Funds.

92. On May 24, 2017, Company 3 wired \$500,000 with a notation that it was for prepayment for gasoil. This payment was consistent with the instructions relayed by CS-2 to wire U.S. dollars to Velmur. The funds comprising this wire make up a portion of the Defendant Funds.

93. On June 1, 2017, TransAtlantic wired \$490,000 to Velmur with a notation that it was for prepayment for gasoil. This payment was consistent with the instructions relayed by CS-

2 to wire U.S. dollars to Velmur. The funds comprising this wire make up a portion of the Defendant Funds.

III. SUMMARY OF FACTS GIVING RISE TO FORFEITURE

94. In sum, the Government's investigation revealed that TransAtlantic, Company 1, Company 2, and Company 3 have acted on behalf of FTB to launder U.S. dollar payments to Velmur, which in turn was seeking to illegally procure gasoil from IPC in U.S. dollars, in violation of United States laws.

95. Financial records reveal that Velmur and TransAtlantic directly or indirectly engaged in money laundering that supported the Government of North Korea or any senior official or person acting for or on behalf of that Government, specifically, by wiring out at least \$15,000,000 in U.S. dollars subsequent to the enactment of the NKSPEA.

96. Based on the above facts, Velmur and TransAtlantic fall within the definition of foreign financial institutions under the Bank Secrecy Act, because they act as dealers of foreign exchange and money transmitters in a manner not merely incidental to their business. *See* 31 C.F.R. § 1010.605(f).

97. Financial records reveal that Velmur and TransAtlantic engaged in at least \$20,000,000 in wires via U.S. correspondent banking transactions in spite of the section 311 action barring such transactions.

COUNT ONE -- FORFEITURE
(Against Defendant Funds; 18 U.S.C. § 981(a)(1)(C))

98. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 97 above as if fully set forth herein.

99. FTB, Velmur, TransAtlantic, and others, known and unknown, acted individually and conspired together to conduct the above identified illegal procurements and payments in violation of IEEPA, 50 U.S.C. § 1705, and the conspiracy statute, 18 U.S.C. § 371.

100. As such, the Defendant Funds are subject to forfeiture, pursuant to 18 U.S.C. § 981(a)(1)(C), as property which constitutes or is derived from proceeds traceable to substantive violations of IEEPA and a conspiracy to violate IEEPA.

COUNT TWO -- FORFEITURE
(Against Defendant Funds; 18 U.S.C. § 981(a)(1)(A))

101. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 97 above as if fully set forth herein.

102. FTB, Velmur, and TransAtlantic acted individually and together to transmit and transfer the Defendant Funds to a place inside the United States from or through a place outside the United States, with the intent to promote the carrying on of violations of IEEPA, 18 U.S.C. § 1343 (relating to wire fraud), and 18 U.S.C. § 1344 (relating to bank fraud), and the prohibited conduct under Section 104(a) of NKSPEA, in violation of 18 U.S.C. § 1956(a)(2)(A)).

103. FTB, Velmur, TransAtlantic, and others, known and unknown, conspired together to commit a violation of 18 U.S.C. §§ 1956(a)(2)(A), in violation of 18 U.S.C. § 1956(h).

104. As such, the Defendant Funds are subject to forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(A), as property involved in transactions in violation of 18 U.S.C. § 1956(a)(2)(A) and (h), or as any property traceable to such property.

COUNT THREE -- FORFEITURE
(Against Defendant Funds; 18 U.S.C. § 981(a)(1)(I))

105. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 97 above as if fully set forth herein.

106. The Defendant Funds are subject to forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(I), as property, real or personal, that is involved in a violation or attempted violation, or which constitutes or is derived from proceeds traceable to a prohibition imposed pursuant to section 104(a) of NKSPEA.

COUNT FOUR – MONEY LAUNDERING MONETARY PENALTIES
(Against Defendant Entities; 18 U.S.C. § 1956(b))

107. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 97 above as if fully set forth herein.

108. Defendant Entities transmitted and transferred at least \$15,000,000, which promoted IEEPA violative transactions.

109. Defendant Entities transmitted and transferred at least \$15,000,000, which promoted prohibited activities under Section 104(a) of NKSPEA.

110. Defendant Entities transmitted and transferred at least \$20,000,000 involving prohibited correspondent banking transactions, which promoted violations of 18 U.S.C. § 1343 (relating to wire fraud), and 18 U.S.C. § 1344 (relating to bank fraud).

111. Velmur and TransAtlantic acted individually and together to transmit and transfer funds to a place inside the United States from or through a place outside the United States, and to a place outside the United States from or through a place inside the United States, with the intent to promote the carrying on of violations of IEEPA, 18 U.S.C. § 1343 (relating to wire fraud), and 18 U.S.C. § 1344 (relating to bank fraud), and the prohibited conduct under Section 104(a) of NKSPEA, in violation of 18 U.S.C. § 1956(a)(2)(A)).

112. Velmur, TransAtlantic, and others, known and unknown, conspired together to commit violations of 18 U.S.C. §§ 1956(a)(2)(A), in violation of 18 U.S.C. § 1956(h).

113. Accordingly, the Court should impose monetary penalties against the Defendant Entities for the value of the funds and monetary instruments involved in the transactions, in an amount to be determined at trial.

* * *

VERIFICATION

I, Benjamin Whitley, a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 22nd day of August, 2017.

 /s/ Benjamin Whitley
Benjamin Whitley
Special Agent
Federal Bureau of Investigation