UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, U.S. Attorney's Office 555 Fourth Street, NW Washington, DC 20530, Plaintiff, v. $1,827,242.65 OF FUNDS ASSOCIATED WITH COMPANY 1, $88,731.00 OF FUNDS ASSOCIATED WITH COMPANY 2, -- and -- $456,820.00 ASSOCIATED WITH "COMPANY 3" Defendants In Rem.	Civil Action No. 20-cv-2019

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 $1,827,242.65 associated with "Company 1" ("Defendant Funds 1"), $88,731.00 associated with "Company 2" ("Defendant Funds 2"), and $456,820.00 associated with "Company 3" ("Defendant Funds 3") (collectively the "Defendant Funds"), and alleges as follows:

NATURE OF ACTION AND THE PARTIES

1. This action arises out of an investigation by the Federal Bureau of Investigation ("FBI") of a scheme by North Korean banks 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, sanctioned North Korean state-run banks have used 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 U.S. dollar transfers involved in Company 1's, Company 2's, and Company 3's scheme with North Korean financial facilitators. These wires were frozen by U.S. correspondent banks while transiting through the U.S. financial system:

Transaction	Date	Originator	Beneficiary	Amount
1	5/26/2017	Company 1	Counterparty 1	$99,936.25
2	5/30/2017	Company 1	Counterparty 1	$149,936.63
3	6/1/2017	Company 1	Counterparty 1	$99,936.74
4	6/1/2017	Company 1	Counterparty 1	$78,278.74
5	6/2/2017	Counterparty 2	Company 1	$84,862.63
6	6/2/2017	Company 1	Counterparty 3	$499,692.00
7	6/2/2017	Company 1	Counterparty 4	$99,286.00
8	6/2/2017	Company 1	Counterparty 5	$89,352.17
9	6/2/2017	Counterparty 3	Company 1	$99,932.00

10	6/5/2017	Company 1	Counterparty 6	$79,416.06
11	6/5/2017	Company 1	Counterparty 7	$89,936.06
12	6/5/2017	Company 1	Counterparty 8	$89,351.06
13	6/6/2017	Company 1	Counterparty 9	$36,007.82
14	6/6/2017	Company 1	Counterparty 10	$134,935.82
15	6/6/2017	Company 1	Counterparty 11	$49,935.82
16	6/6/2017	Company 1	Counterparty 12	$46,446.82
			Total	**$1,827,242.65**
17	2/7/2018	Counterparty 13	Company 2	$51,201.00
18	2/20/2018	Company 2	Counterparty 14	$36,530.00
19	4/16/2018	Counterparty 15	Company 2	$1,000.00
			Total	**88,731.00**
20	6/5/2017	Company 3	Company 4	$456,820.00

5. These transfers were in violation of the International Emergency Economic Powers Act ("IEEPA"), codified at 50 U.S.C. § 1701, *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).

6. 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).

JURISDICTION AND VENUE

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

8. 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 government-controlled bank account in the United States,

pursuant to a previously executed seizure warrant. These funds were seized from correspondent banks in New York, which banks froze the transactions as they transited through the United States. The Defendant Entities and co-conspirators failed to seek or obtain licenses from the Department of the Treasury's ("Treasury's") Office of Foreign Asset Control ("OFAC"), which is located in Washington, D.C., to conduct transactions through the United States for which licenses were required under United States law.

STATUTORY FRAMEWORK

I. IEEPA

9. IEEPA, enacted in 1977, authorizes the President to impose economic sanctions in response to an unusual or extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat.

10. The Department of the Treasury enforces and administers economic sanctions to accomplish U.S. foreign policy and national security goals. In particular, the Department of the Treasury publishes a publicly available list of individuals and entities ("Specially Designated Nationals and Blocked Persons" or "SDNs") targeted by U.S. economic sanctions. SDNs' property and interests in property, subject to U.S. jurisdiction or in the possession and control of U.S. persons, are blocked when they are placed on the SDN list. U.S. persons, including U.S. financial institutions, are generally prohibited from dealing with SDNs and their property and interests in property.

11. Using the powers conferred by IEEPA, the President and the Executive Branch have issued orders and regulations governing and prohibiting certain transactions with countries, individuals, and entities suspected of proliferating Weapons of Mass Destruction ("WMD"). On November 14, 1994, the President issued Executive Order 12,938, 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."

12. On June 27, 2008, the President declared in Executive Order 13,466 ("Continuing Certain Restrictions With Respect to North Korea and North Korean Nationals") that "the existence and risk of the proliferation of weapons-usable fissile material on the Korean Peninsula constituted an unusual and extraordinary threat to the national security and foreign policy of the United States," and thereby declared a "national emergency." The Executive Order further authorized the United States Secretary of the Treasury, in consultation with the Secretary of State, "to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order."

13. On March 15, 2016, the President, to take additional steps with respect to the previously described national emergency, issued Executive Order 13,722 to address the Government of North Korea's continuing pursuit of its nuclear and missile programs. Pursuant to that authority, on March 16, 2016, the Secretary of the Treasury promulgated the "North Korea Sanctions Regulations." See 31 C.F.R. § 510.101 *et seq*. Executive Order 13,722 and the North Korea Sanctions Regulations prohibit the export of financial services from the United States or by any U.S. person to North Korea, unless exempt or authorized by OFAC.

14. Foreign financial institutions maintain U.S. dollar bank accounts at banks in the United States ("Correspondent Banks"). Correspondent bank accounts are broadly defined to include any account established at a Correspondent Bank for a foreign financial institution wherein the Correspondent Bank receives deposits from, or make payments or disbursements on behalf of,

the foreign financial institution, or handles other financial transactions, such as currency conversions, related to such foreign financial institution. See 31 C.F.R. § 1010.605. Correspondent Banks serve to support international wire transfers for foreign customers in a currency that the foreign customer's overseas financial institution normally does not hold on reserve, such as U.S. dollars and to conduct currency conversions to/from U.S. dollars. It is through these accounts that the funds used in U.S. dollar transactions clear and/or are converted into other currencies.

15. SDNs are, among other things, prohibited from accessing Correspondent Banks in the United States through foreign financial institutions, either directly or indirectly.

16. The North Korea Sanctions Regulations further prohibited the export of financial services to North Korea, to include Correspondent Banking activities, by any U.S. person or any person within the United States. The North Korea Sanctions Regulations also prohibited activities that evaded or avoided, or had the purpose of evading or avoiding, any prohibition set forth in these regulations.

17. OFAC has designated numerous North Korean banks. In particular, in March 2013, OFAC designated North Korea's Foreign Trade Bank ("FTB").

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

18. According to the 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.

19. The Bank Secrecy Act requires U.S. financial institutions to take anti-money laundering measures when dealing with foreign financial institutions engaged in correspondent banking of U.S. dollar transactions.

20. 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).

21. 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. One such special measure imposed under Section 311 protects the integrity of the U.S. financial system by prohibiting financial institutions from causing U.S. financial institutions to engage in any type of financial transaction with any entity within the jurisdiction deemed an area of money laundering concern.

22. On June 1, 2016, FinCEN issued a Notice of Finding for a Section 311 designation of 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).

23. In November 2016, FinCEN published a final rule implementing the most severe special measure against the entire North Korean financial sector. *See* Federal Register, Vol. 81, No. 217 (Nov. 9, 2016); 31 C.F.R. § 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. A second special measure requires covered financial institutions to exercise

"enhanced due diligence" and 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. 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. The Chairman of the House Foreign Affairs Committee stated that the Section 311 designation "impacts all financial institutions, anywhere, who now have a choice to make between doing business with North Korea and being cut off from financial transactions with the United States and the international financial system."

24. A violation of the Section 311(b) special measure, codified at 31 U.S.C. § 5318A(b), or of the regulations published at 31 C.F.R. § 1010.659, is punishable criminally pursuant to 31 U.S.C. § 5322.

III. MONEY LAUNDERING VIOLATIONS

25. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

26. 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, *inter alia*, 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.

27. Pursuant to 18 U.S.C. § 1956(c)(7)(A), the term "specified unlawful activity," includes violations of 18 U.S.C. § 1344 (relating to bank fraud).

a. As noted above, U.S. financial institutions are barred, pursuant to the section 311(b)(5) 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* 81 Fed. Reg. 78,716, 78,718. North Korean entities have attempted to circumvent the section 311(b)(5) ban by using foreign front companies to engage in financial transactions on their behalf. These financial transactions would violate U.S. law 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. dollar transactions to be processed.

b. This scheme, and these types of transactions, constitute bank fraud because the false transactions occur via wire, and are done in part to deceive and defraud U.S. financial institutions, which are barred from conducting such transactions, and could face civil and criminal penalties for processing such transactions.

c. 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.

28. 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).

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 often 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 accessing the U.S. financial system. As a result, criminals often 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 U.S. sanctions and of U.S. financial institutions' corresponding due diligence obligations. In turn, these North Korean entities have a documented practice of using front companies to avoid the imposition of designations and the blocking of property, which may occur pursuant to IEEPA. These opaque U.S. dollar transactions by front companies promote IEEPA violations, by preventing the imposition of sanctions and the blocking of property. 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 an enforcement action. But, because the parties conceal their laundering of funds, such enforcement actions are impeded. Financial transactions by North Korean financial facilitators facilitate a conspiracy to circumvent the sanctions.

d. In its 2018 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:

> Once the Democratic People's Republic of Korea can register a front company without overt links to the country through the assistance of foreign nationals, it becomes significantly easier for its firms to pass rudimentary due diligence checks by financial institutions and

> open and maintain accounts. An investigation into a Singaporean company with ownership ties to financial institutions of the Democratic People's Republic of Korea revealed the use of overseas representatives and front companies, especially those established in Hong Kong, to ensure that transactions were conducted in a manner that would not reveal any overt connection to a designated entity or interest of the Democratic People's Republic of Korea.

2018 Report of the Panel of Experts, at 171.

IV. FACTUAL ALLEGATIONS

A. THE NORTH KOREAN FINANCIAL SECTOR LAUNDERS FUNDS FOR SANCTIONED ENTITIES

i. Background

29. 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.

30. For example, on March 2, 2016, the United Nations Security Council unanimously approved resolution 2270. Paragraph 33 of that resolution requires U.N. member states to prohibit financial institutions from establishing or maintaining correspondent relationships with North Korean banks.

31. The United States House of Representatives' Foreign Affairs Committee released a report that 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.*

ii. North Korean Financial Institutions Continue to Launder U.S. Dollars

32. 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 WMD and the development of ballistic missiles in violation of international and U.S. sanctions," and are subject to "little or no bank supervision or anti-money laundering or combating the financing of terrorism [] controls." 81 Fed. Reg. at 78,715.

33. 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.

81 Fed. Reg. at 35,442 (emphasis added).

34. The Panel of Experts noted the central role of North Korean banks in allowing North Korean entities to continue to access the U.S. financial system illegally. 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).

35. 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 apparatus." https://www.treasury.gov/press-center/press-releases/Pages/jl1876 .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/jl0471.aspx (emphasis added).

iii. FTB is a Primary Vehicle in North Korea's Illicit Money Laundering Network

36. U.N. and OFAC sanctions 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.

37. 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.

38. In a May 2020 indictment, the government alleged that FTB has laundered over $2.5 billion through the United States as part of an ongoing money laundering and sanction evasion scheme. The indictment further alleges that FTB established covert branches overseas to execute this illegal scheme.

iv. North Korean Entities Continue to Launder U.S. Dollars Via Front Companies

39. 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.

40. This use of front companies was 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.

2016 Report of the Panel of Experts, at 62.

41. 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).

42. 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.*, 81 Fed. Reg. at 35,442 ("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.

43. 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.

B. TARGET FOREIGN FINANCIAL FACILITATORS

44. The scheme to launder funds is as follows: (1) foreign customers receiving North Korean services and North Korean customers receiving services from foreign companies make or receive payments in U.S. dollars; (2) designated North Korean banks work with covert overseas foreign branch representatives to establish front companies which can process U.S. dollar payments; and (3) individuals including commodity brokers, front company owners, and/or unauthorized money remitters make arrangements for the North Korean front companies to be paid in U.S. dollars.

45. These 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).

46. The following transactions were emblematic of transactions conducted by or for front companies using correspondent bank accounts at U.S. financial institutions to conduct dollar-denominated transactions on behalf of sanctioned entities associated with North Korea. They involve Company 1 and Company 2, which succeeded Company 1 in making prohibited transactions after Company 1's funds were seized.

i. Company 1 Laundered Funds for North Korea with Known North Korean Financial Facilitators

1. FTB Vladivostok

47. On August 22, 2017, OFAC designated Velmur Management Pte. Ltd. ("Velmur") under E.O. 13,722 for operating in the energy industry in the North Korean economy, by importing gasoil to North Korea.

48. As pled in the related FTB indictment, 1:20-cr-32 (RC), Velmur was a front company established by the covert branch representatives of FTB Vladivostok.

49. Company 1 sent a wire of approximately $410,000.00 to Velmur on April 25, 2017 as part of this scheme.

2. Apex Choice

50. The government previously filed a forfeiture complaint, 18-cv-2746 (RC), alleging Apex Choice ("Apex") of laundering funds for FTB.

51. On May 23, 2017, Apex sent one wire for approximately $214,983.00 to Company 1.

52. On May 31, 2017, a company related to Apex sent a wire for approximately $99,983.00 to Company 1.

3. FTB Thailand

53. On or about December 2, 2016, OFAC sanctioned Korea Rungrado General Trading Corporation ("Korea Rungrado") for having engaged in, facilitated, or been responsible for the exportation of workers from North Korea, including exportation to generate revenue for the sanctioned Government of North Korea.

54. Cooperating Company A entered into multiple contracts for products with Korea Rungrado, for which payments were laundered via FTB Thailand front companies.

55. According to information provided by Cooperating Company A, the commodities associated with these contracts were shipped to Dalian, China; however, the ultimate counterparties to the transactions were North Korean trade companies.

56. In 2017, Company 1 sent a wire for approximately $150,000.00 to Cooperating Company A as part of this scheme.

4. FTB Shenyang

57. On May 31, 2017 and June 1, 2017, a FTB Shenyang front company sent two wires totaling $599,619.00 to Company 1.

5. FTB Kuwait

58. On June 7, 2017, Company 1 sent a wire of approximately $134,935.82 to a Kuwaiti state fund for economic development. This payment was directed by the North Korean nationals operating the covert FTB Kuwait branch.

6. Sunico

59. On August 17, 2017, the government of Australia designated Sunico for assisting in the evasion and/or violation of sanctions. The designation noted that Sunico acted as a, "North Korean associated company that has facilitated proliferation-related activity."

60. Company 1 sent five payments to Sunico totaling $319,720.74 between April 3, 2017 and June 5, 2017.

7. First Credit Bank

61. The investigation revealed that Company 1 received three wires totaling $334,599.54 from a front company for North Korea's First Credit Bank. On September 6, 2017, OFAC designated North Korea's First Credit Bank. In May 2020, Jin Yonghuan was charged with sanctions and money laundering violations as part of his related activities to launder funds between North Korea's First Credit Bank and FTB.

8. Summary

62. The above-identified illicit payments involving Company 1 total at least $2,263,840.47.

63. Defendant Funds 1 are comprised of 12 subsequent transactions that Correspondent Banks in New York froze as they transited through the U.S. financial system. These 16 transactions

with 12 counterparties, totaling $1,827,242.65, represent illicit funds that the government seized as part of this scheme. The 12 counterparties to these transactions included many of the above-identified entities, such as Sunico and FTB Kuwait, as well as other FTB front companies.

ii. Company 2, a Front Company for Company 1, Laundered Funds for North Korea with Known North Korean Financial Facilitators

1. Receipt of Funds from Company 1

64. Company 2 was incorporated in Singapore approximately two months after Company 1's last U.S. dollar payment was seized by the government.

65. In August 2017, a Czech bank transferred approximately $246,244.12 via two transactions to Company 2's bank account in Singapore. The wire reference for both transfers indicated that the transfer was for the closed balance of the Company 1 bank account.

66. Company 2 acted as a front company for Company 1, because Company 1 could no longer make U.S.-dollar denominated wire payment.

2. FTB Thailand

67. On August 29, 2017, Company 2 received a wire for $33,000 from Kisgum Co. Ltd. ("Kisgum"). On September 11, 2017, Company 2 then sent a wire for $33,000.00 to Kisgum.

68. As alleged in a May 2020 indictment, Kisgum was a front company established by FTB Thailand.

69. This practice of sending funds in a circular manner is consistent with the money laundering practice known as layering. Criminals "layer" funds by moving them through multiple bank accounts to conceal the source, nature, and origin of the funds.

3. Apex Choice

70. On September 5, 2017, a company related to Apex Choice wired $400,000.00 to Company 2. As noted above, on May 31, 2017, this same company wired approximately $99,983.00 to Company 1.

4. Summary

71. The above-identified illicit payments involving Company 2 total at least $466,000.00.

72. Defendant Funds 2 are comprised of 3 subsequent transactions that Correspondent Banks in New York froze as they transited through the U.S. financial system. These 3 transactions with 3 counterparties, totaling 88,731.00, represent illicit funds that the government seized as part of this scheme. The 3 counterparties to these transactions were part of FTB's money launder and sanction evasion scheme

iii. Reconnaissance General Bureau Association with Company 1 and Company 2

73. According to OFAC, the Reconnaissance General Bureau ("RGB") is North Korea's primary intelligence organization and is involved, inter alia, in a range of activities to include conventional arms trade proscribed by numerous United Nations Security Council Resolutions. RGB was designated on January 2, 2017 pursuant to E.O 13687 and was previously listed in the annex to E.O. 13551 on August 30, 2010. RGB is responsible for collecting strategic, operational, and tactical intelligence for the Ministry of the People's Armed Forces. Many of North Korea's major cyber operations run through RGB.

74. A confidential reliable source (CS-1) revealed that Company 1 and Company 2 operated at the direction and guidance of an RGB officer.

75. CS-1 further revealed this RGB officer exchanged invoices / contracts and made related payment requests to Company 1 and Company 2. CS-1 provided a spreadsheet tracking these payments and the documents supporting such payments. According to the spreadsheet, the RGB officer was tracking millions of dollars of payments, including to a major Chinese oil company, Sunico, and a FTB Kuwait customer.

76. The RGB officer collected these documents to synchronize payments by Company 1 and Company 2 to the corresponding invoices. Tracking payments is a common problem for North Korean money launderers and their customers, because payments come from disassociated third parties, as opposed to the true customer.

77. The RGB officer informed Company 1 and Company 2 that he would create fabricated records, which would facilitate their business dealings. Such practice is commonly done to deceive banks that may ask for supporting documentation for an international U.S.-dollar wire transfer.

iv. Company 3 Laundered Funds to Company 4, both of which previously laundered funds for North Korea with Known North Korean Financial Facilitators

1. FTB Thailand

78. As noted above, Cooperating Company A entered into multiple contracts for products with Korea Rungrado, for which payments were laundered via FTB Thailand front companies.

79. According to information provided by Cooperating Company A, the commodities associated with these contracts were shipped to Dalian, China; however, the ultimate counterparties to the transactions were North Korean trade companies.

80. In 2017, Company 3 sent a wire for approximately $575,000.00 to Cooperating Company A for the benefit of FTB Thailand.

2. Chi Yupeng Network of Companies

81. Pursuant to Chief Judge Howell's May 22, 2017 opinion, this Court found that probable cause existed to show that:

a. Dandong Zhicheng Metallic Material Co., Ltd ("Dandong Zhicheng") (a/k/a Dandong Chengtai Trade Co. Ltd. ("Dandong Chengtai");

b. Rambo Resource Limited ("Rambo Resource") (formerly Tin Yee Resources Limited);

c. Tin Yee Resources Limited ("Tin Yee Resources");

d. Ruizhi Resources Limited ("Ruizhi Resources"); and

e. Shun Mao Mining Co., Limited ("Shun Mao Mining")

(emphasis added) (collectively "Chi Yupeng Network of Companies") were part of a related criminal network operated by Chi Yupeng, the majority owner of Dandong Zhicheng a/k/a Dandong Chengtai, which had illegally transacted over $600 million. *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. The Court further found that probable cause existed that all funds transacted by the Chi Yupeng Network of Companies were subject to seizure and forfeiture based on violations of the money laundering statute and IEEPA. *Id.* at 5.

82. In August 2017, OFAC designated Dandong Zhicheng. The designation noted that Dandong Zhicheng allegedly used the foreign exchange received from the end users of North Korean coal to purchase other items for North Korea, including nuclear and missile components, and that Chi Yupeng used a network of companies to engage in bulk purchases, wire transfers, and other transactions on behalf of North Korean interests.

83. Between October 2010 and September 2015, Company 4 received approximately 41 U.S.-dollar wire transfers totaling approximately $2,595,584.73 from the Chi Yupeng Network.

84. Between July and August 2014, Company 4 sent approximately six U.S.-dollar wire transfers totaling approximately $762,138.00 to the Chi Yupeng Network.

3. Summary

85. The above-identified illicit payments involving Company 3 and Company 4 total at least $3,932,722.73.

86. Defendant Funds 3 is comprised of 1 subsequent transaction between Company 3 and Company 4 that a Correspondent Bank in New York froze as it transited through the U.S. financial system. This transaction, totaling $456,820.00, represent illicit funds that the government seized as part of this scheme. The counterparties to this transactions were part of FTB's money launder and sanction evasion scheme

C. SUMMARY OF FACTS GIVING RISE TO FORFEITURE

87. In sum, Company 1, Company 2, Company 3, and Company 4 have acted for the benefit of sanctioned North Korean banks, including FTB, by laundering U.S. dollar payments.

88. These laundered payments went to known North Korean financial facilitators, who used such funds to illegally procure items.

89. Law enforcement intercepted payments by Company 1, Company 2, Company 3, and Company 4, which represent the Defendant Funds.

V. COUNTS

COUNT ONE -- FORFEITURE
(18 U.S.C. § 981(a)(1)(C))

90. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 80 as if fully set forth herein.

91. Company 1 and Company 2, 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.

92. As such, Defendant Funds 1 and Defendant Funds 2 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
(18 U.S.C. § 981(a)(1)(C))

93. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 92 as if fully set forth herein.

94. Company 3 and Company 4, 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.

95. As such, Defendant Funds 3 is 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 THREE -- FORFEITURE
(18 U.S.C. § 981(a)(1)(A))

96. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 92 above as if fully set forth herein.

97. Company 1 and Company 2 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 the penalties section of IEEPA, and 18 U.S.C. § 1344 (relating to bank fraud), in violation of 18 U.S.C. § 1956(a)(2)(A)).

98. Company 1 and Company 2, 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).

99. As such, Defendant Funds 1 and Defendant Funds 2 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 FOUR -- FORFEITURE
(18 U.S.C. § 981(a)(1)(A))

100. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 92 above as if fully set forth herein.

101. Company 3 and Company 4 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 the penalties section of IEEPA, and 18 U.S.C. § 1344 (relating to bank fraud), in violation of 18 U.S.C. § 1956(a)(2)(A)).

102. Company 3 and Company 4, 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).

103. As such, Defendant Funds 3 is 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.

VI. PRAYER FOR RELIEF

WHEREFORE, the United States of America prays as follows:

A. that notice issue on the Defendant Funds as described above;

B. that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed;

C. that a warrant of arrest *in rem* issue according to law;

D. that judgment be entered declaring that the Defendant Funds be forfeited to the United States of America for disposition according to law; and

E. that the United States of America be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

MICHAEL R. SHERWIN
Acting United States Attorney
N.Y. Bar No. 4444188

By: /s/ *Zia M. Faruqui*
Zia M. Faruqui, D.C. Bar No. 494990
Brian P. Hudak
Assistant United States Attorneys
555 Fourth Street, NW
Washington, DC 20530; (202) 252-7566 (main line)

Dated: July 23, 2020 *Attorneys for the United States of America*

VERIFICATION

I, Christopher Wong, 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 23rd day of July, 2020.

/s/ Christopher Wong
Christopher Wong
Special Agent
Federal Bureau of Investigation

I, Thomas Tamsi, a Special Agent with the Homeland Security Investigations, 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 23rd day of July, 2020.

/s/ Thomas Tamsi
Thomas Tamsi
Special Agent
Homeland Security Investigations