

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

_____	)	
UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	
\$1,071,251.44 OF FUNDS ASSOCIATED	)	
WITH MINGZHENG INTERNATIONAL	)	
TRADING LIMITED;	)	
	)	
\$347,446.93 OF FUNDS ASSOCIATED	)	
WITH MINGZHENG INTERNATIONAL	)	
TRADING LIMITED;	)	
	)	
\$42,632.00 OF FUNDS ASSOCIATED	)	
WITH MINGZHENG INTERNATIONAL	)	Civil Action No. _____
TRADING LIMITED;	)	
	)	
\$30,258.00 OF FUNDS ASSOCIATED	)	
WITH MINGZHENG INTERNATIONAL	)	
TRADING LIMITED;	)	
	)	
\$253,638.25 OF FUNDS ASSOCIATED	)	
WITH MINGZHENG INTERNATIONAL	)	
TRADING LIMITED; and	)	
	)	
\$157,749.07 OF FUNDS ASSOCIATED	)	
WITH MINGZHENG INTERNATIONAL	)	
TRADING LIMITED;	)	
	)	
Defendants.	)	
_____	)	

**VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

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 \$1,902,976.00 associated with Mingzheng International Trading Limited (Mingzheng) (the “Defendant Funds”), further described as: \$1,071,251.44 of funds associated

with Mingzheng; \$347,446.93 of funds associated with Mingzheng; \$42,632.00 of funds associated with Mingzheng; \$30,258.00 of funds associated with Mingzheng; \$253,638.25 of funds associated with Mingzheng; and \$157,749.07 of funds associated with Mingzheng, all which are being held at six U.S. financial institutions, and alleges as follows:

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

1. This *in rem* forfeiture action arises out of an investigation by the Federal Bureau of Investigation (“FBI”) of a scheme by Mingzheng International Trading Limited (“Mingzheng”), a front company incorporated in Hong Kong, to launder U.S. dollars on behalf of sanctioned North Korean entities. As described in detail below, North Korea has used the state-run Foreign Trade Bank (“FTB”) to work with a host of front companies in order to access the U.S. financial system and evade the U.S. sanctions imposed on FTB and its sanctioned affiliates. In particular, Mingzheng acts as a front company to make U.S. dollar payments on behalf of a covert foreign branch of FTB, which is otherwise barred from making such U.S. dollar payments. Consistent with front companies, Mingzheng has no website or purported business purpose in corporate documents. Specifically, between October and November 2015, Mingzheng was a counterparty to 20 illicit wire transfers in U.S. dollars, totaling \$1,902,976.00, which were routed through U.S. correspondent banking accounts, and which comprise the Defendant Funds. 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).

2. The Defendant Funds are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as property constituting or derived from proceeds traceable to violations of IEEPA and a conspiracy to violate IEEPA. In addition, the Defendant Funds are subject to forfeiture pursuant

to 18 U.S.C. § 981(a)(1)(A) as property involved in, and traceable to money laundering violations and a conspiracy to launder money, in violation of 18 U.S.C. § 1956(a)(2)(A), (h).

### **JURISDICTION AND VENUE**

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

4. Venue is proper pursuant to 28 U.S.C. § 1355(b)(1)(A) 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 coconspirators failed to seek or obtain licenses from the Department of the Treasury's Office of Foreign Asset Controls ("OFAC"), which is located in Washington, D.C., for conducting transactions with these funds, which licenses were required under United States law.

### **STATUTORY FRAMEWORK**

#### **I. THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT**

5. 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.

6. 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.

7. 18 U.S.C. § 371 criminalizes a conspiracy to violate IEEPA.

8. By the authority vested in the President by IEEPA, on or about June 28, 2005, the President signed Executive Order (“E.O.”) 13382 blocking the property of persons engaged in weapons of mass destruction proliferation activities and their support networks and denying designated proliferators access to the U.S. financial and commercial systems. This blocking program initially applied to eight organizations in North Korea, Iran, and Syria. The U.S. Department of the Treasury, together with the U.S. Department of State, is authorized to designate additional proliferators of weapons of mass destruction and their supporters under the authorities provided by E.O. 13382. When the Department of the Treasury so designates additional persons (individuals and entities), these persons are added to a list of Specially Designated Nationals (“SDN”).

9. On or about April 13, 2009, the Secretary of the Treasury promulgated the “Weapons of Mass Destruction Proliferators Sanctions Regulations” to implement E.O. 13382. 31 C.F.R. § 544.101 *et seq.* 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.

10. In March 2013, OFAC designated FTB as an SDN pursuant to E.O. 13382.

## **II. ANTI-MONEY LAUNDERING OBLIGATIONS**

11. 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.

12. 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 the U.S. dollar.

13. 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.

14. 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 transactions

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

15. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

16. 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.

17. Pursuant to 18 U.S.C. § 1956(c)(7)(D), the term “specified unlawful activity,” includes violations of IEEPA.

### **III. FORFEITURE**

18. 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 forfeiture.

19. 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.

### **FACTS GIVING RISE TO FORFEITURE**

#### **I. BACKGROUND ON NORTH KOREAN MONEY LAUNDERING**

20. 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. A violation of 31 U.S.C. § 5318A is punishable criminally pursuant to 31 U.S.C. § 5322. In order to protect the integrity of the U.S. financial system, a Section 311 finding legally prevents persons 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.

21. 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 primary jurisdiction of money-laundering concern. *See* Federal Register, Vol. 81, No. 107 (June 3, 2016).

22. FinCEN targeted the entire North Korean financial sector because it is comprised entirely 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.

23. 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).

## **II. ILLICIT NORTH KOREAN USE OF CORRESPONDENT BANKING CHANNELS**

### **A. NORTH KOREAN BANKS ENGAGE IN U.S. DOLLAR TRANSACTIONS BY LAUNDERING FUNDS THROUGH NUMEROUS FRONT COMPANIES**

24. Information gathered from Treasury Department designations, the FinCEN 311 finding, the February 17, 2017, report on North Korea by the United Nations Panel of Experts ("Panel of Experts"), and from related North Korean investigations, leads law enforcement to conclude that the North Korean financial institutions identified below have repeatedly utilized the U.S. financial system in violation of the U.S. economic sanctions.

25. Specifically, law enforcement has learned that these North Korean financial institutions employ front companies to 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. Although North Korean financial facilitators engage in U.S. dollar transactions

overseas, funds are still cleared through a U.S. correspondent bank account, thereby triggering the U.S. economic sanctions. These wire transfers often involve the remittance of payments denominated in U.S. dollars originating from foreign financial institutions located outside the United States which must clear through established correspondent banking relationships to U.S. financial institutions in the United States. Once the wire transfers are cleared through the U.S. financial institutions, payments are transmitted to offshore U.S. dollar accounts maintained by front companies on behalf of North Korean financial institutions.

26. The 2017 Report of the 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).

27. Similar to FinCEN, the Panel of Experts found that the North Korean financial network continues to process U.S. dollar transactions by employing “numerous front companies bearing no paper trail that leads to the Democratic People’s Republic of Korea.” *Id.* at 80.

28. The front companies engage in this scheme in support of purchases ultimately benefiting sanctioned North Korean end users, including North Korean military and North Korean weapons programs. In a 2013 designation of a North Korean financial institution, the Treasury Department noted that this North Korean bank was “part of the web of banks, front companies and government agencies that support North Korea’s continued proliferation activities.” <https://www.treasury.gov/press-center/press-releases/Pages/tg1828.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).

**B. RECENT CRIMINAL COMPLAINT AGAINST A RELATED NORTH KOREAN BANK HIGHLIGHTS HOW THE NORTH KOREAN FINANCIAL SECTOR HAS CONTINUED TO TRANSACT IN U.S. DOLLARS IN VIOLATION OF THE SANCTIONS**

29. In 2016, a criminal complaint was filed in the District of New Jersey against Dandong Hongxiang for laundering U.S. dollars on behalf of Korea Kwangson Banking Corporation (“KKBC”). KKBC (further described below to be a subsidiary of FTB) is a North Korean bank that was previously designated by OFAC and the U.N. for providing financial services for North Korea’s weapons of mass destruction proliferators. The investigation revealed

that Dandong Hongxiang was acting in part as a front for KKBC, to allow KKBC to engage in over \$1.3 billion in U.S. dollar transactions. Dandong Hongxiang used over 22 different front companies with offshore bank accounts to help KKBC evade U.S. sanctions after KKBC was designated as an SDN on August 11, 2009. This elaborate network helped North Korea conduct foreign trade using the U.S. financial system without detection for over seven years.

30. This use of front companies (*i.e.*, Dandong Hongxiang and related companies) to continue to transact in U.S. dollars is consistent with what the Panel of Experts found to be true for North Korea financial institutions. Specifically, the Panel of Experts noted in 2016 that “[t]ransactions originating in foreign banks have been processed through corresponding accounts in the United States and Europe.” *See* 2016 Report of the Panel of Experts, at 62. These sanction-violative transactions continue to be processed by 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.” *Id.* 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.

### **III. IN SPITE OF THE SANCTIONS, THE FOREIGN TRADE BANK, WHICH IS THE CENTRAL NORTH KOREAN BANK FOR FOREIGN CURRENCY TRANSACTIONS, ILLEGALLY TRANSACTS IN U.S. DOLLARS**

#### **A. BACKGROUND ON FTB**

31. 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.

32. 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.

B. FTB HAS LAUNDERED U.S. DOLLAR TRANSACTIONS, IN VIOLATION OF U.S. LAW

33. 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.

34. 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 KKBC 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).

35. 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.

36. FTB's integral role in the North Korean financial network is also evidenced by its processing of internal foreign currency transactions, and its stake in other North Korean banks. Specifically, FTB is known to be the parent bank of KKBC and Korea Kumgang bank (another designated bank).

C. CONFIDENTIAL SOURCES HAVE CONFIRMED MINGZHENG'S INVOLVEMENT IN LAUNDERING FUNDS FOR NORTH KOREA

37. Two reliable confidential sources have independently revealed that Mingzheng has laundered U.S. dollar payments on behalf of North Korea entities – in particular, FTB. Mingzheng also bears the hallmarks of a FTB front company. Mingzheng has no website, and gives no purported business purpose in corporate documents. A search of international wires reveals that it makes U.S. dollar payments for products in totally unrelated industries. As discussed below, this is consistent with how North Korea uses front companies to evade sanctions and procure items in U.S. dollars to sustain its proliferation program and economy. Mingzheng was incorporated in Hong Kong and is operated by at least one Chinese national.

38. The first reliable confidential source (CS-1) revealed that Mingzheng made illicit U.S. dollar payments directly for the benefit of the North Korean government between January 2012 and January 2015.

39. The second reliable confidential source (CS-2) confirmed that FTB has used Mingzheng to launder U.S. dollar payments. Specifically, CS-2 provided information tying FTB to Mingzheng and the wiring of the Defendant Funds.

40. CS-2 revealed that Mingzheng acts a front company for a covert Chinese branch of FTB. This branch is operated by a Chinese national who has historically been tied to FTB. This practice is consistent with the findings of the Panel of Experts as to how North Korean financial institutions have been able to evade sanctions, to wit:

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).

41. CS-2 further indicated that payment instructions in international wires sent by Mingzheng contained coded reference numbers used by FTB. These coded reference numbers reflect that Mingzheng was making U.S. dollar payments on behalf of FTB, which FTB was otherwise barred from doing.

42. Additionally, CS-2 identified several Mingzheng payments as being remitted to a Chinese Export and Import Company (Chinese Company 1) that had previous ties to Dandong Hongxiang. According to Chinese Company 1's corporate registry information, it is a Chinese export and import company that services North Korea, among other markets. Records from U.S. correspondent banks and documents obtained in the Dandong Hongxiang investigation revealed that Dandong Hongxiang and its related front companies made U.S. dollar payments to Chinese Company 1 totaling approximately \$3.19 million between November 2009 and December 2013.

43. A review of international wires revealed that Chinese Company 1 was frequently listed as a beneficiary of suspicious payments between 2012 and 2016. Many of these payments contained coded reference numbers used by FTB. CS-2 confirmed that the Mingzheng payments from this timeframe were on behalf of FTB.

44. Records from U.S. correspondent banks further revealed that Mingzheng paid Chinese Company 1 approximately \$1.8 million by between March 2013 and September 2014.

#### **IV. MINGZHENG PREVIOUSLY LINKED TO NORTH KOREAN MONEY LAUNDERING SCHEMES**

##### **A. MINZHENG'S ILLICIT FINANCIAL TRANSACTIONS IN OCTOBER AND NOVEMBER 2015**

45. From on or around October 19, 2015, to on or around November 18, 2015, Mingzheng sent or received a total of 20 wire transfers, which transited through the U.S. financial system through the use of correspondent U.S. banks, and represent the Defendant Funds. The Defendant Funds include 13 outgoing wires, totaling \$1,349,258.16, in which Mingzheng was listed as the remitter, and seven incoming wires, totaling \$553,717.53, in which Mingzheng was listed as the beneficiary. The details of these 20 wires, totaling \$1,902,975.69, are provided in the table below. Three different Mingzheng accounts were involved with the transactions identified below including China Merchants Bank (“CMB”) account ending in 2808, Bank of Communications (“BOC”) account ending in 3100, and Shanghai Pudong Development Bank (“SPDB”) account ending in 6150.

**TABLE 1: Illicit Mingzheng Wires on Behalf of FTB that Comprise Defendant Funds**

<b>#</b>	<b>Date</b>	<b>Wire Amount</b>	<b>Party Sending Wire</b>	<b>Party Receiving Wire</b>
1	10/19/2015	\$9,932.00	Mingzheng (SPDB)	Counterparty 1
2	10/19/2015	\$9,742.79	Mingzheng (BOC)	Counterparty 2
3	10/20/2015	\$162,018.00	Counterparty 3	Mingzheng (SPDB)
4	10/22/2015	\$96,345.42	Mingzheng (SPDB)	Counterparty 4
5	10/23/2015	\$9,945.00	Mingzheng (BOC)	Counterparty 1
6	10/28/2015	\$24,932.00	Mingzheng (CMB)	Counterparty 1

#	Date	Wire Amount	Party Sending Wire	Party Receiving Wire
7	10/29/2015	\$199,982.00	Mingzheng (CMB)	Counterparty 5
8	10/30/2015	\$79,151.51	Mingzheng (CMB)	Counterparty 4
9	11/2/2015.	\$42,632.00	Mingzheng (SPDB)	Counterparty 6
10	11/2/2015	\$174,982.00	Mingzheng (CMB)	Counterparty 7
11	11/4/2015	\$5,326.00	Mingzheng (CMB)	Counterparty 8
12	11/5/2015	\$205,536.23	Mingzheng (CMB)	Counterparty 9
13	11/5/2015	\$295,769.21	Mingzheng (CMB)	Counterparty 10
14	11/6/2015	\$194,982.00	Mingzheng (CMB)	Counterparty 7
15	11/6/2015	\$140,000.00	Counterparty 11	Mingzheng (SPDB)
16	11/12/2015	\$45,000.00	Counterparty 12	Mingzheng (SPDB)
17	11/17/2015	\$57,749.07	Counterparty 13	Mingzheng (SPDB)
18	11/17/2015	\$100,000.00	Counterparty 13	Mingzheng (SPDB)
19	11/17/2015	\$41,822.04	Counterparty 14	Mingzheng (BOC)
20	11/18/2015	\$7,128.42	Counterparty 14	Mingzheng (BOC)

46. These U.S. dollar payments, which cleared through U.S. correspondent banking accounts, violated U.S. law, because Mingzheng was surreptitiously making them on behalf of FTB, whose designation precluded such transactions.

**B. MINGZHENG'S FINANCIAL TRANSACTIONS ARE CLOSELY LINKED TO DANDONG HONGXIANG, A CHINESE COMPANY THAT WAS RECENTLY SANCTIONED FOR ITS TIES TO NORTH KOREAN WMD PROLIFERATION**

47. On September 26, 2016, OFAC announced sanctions against Dandong Hongxiang and four of its executives for having ties to the government of North Korea's weapons of mass destruction proliferation efforts. On the same day, the Department of Justice unsealed a criminal

complaint in the District of New Jersey (as referenced in paragraph 29) alleging Dandong Hongxiang and four of its executives conspired to violate U.S. laws by laundering U.S. dollar transactions on behalf of KKBC, a sanctioned North Korean bank.

48. The criminal complaint identified Luo Chuanxu as one of the Dandong Hongxiang co-conspirators. The complaint indicates that Luo is a Chinese National who established multiple front companies in Hong Kong, Anguilla, and the British Virgin Islands to facilitate payments on behalf of KKBC, a sanctioned North Korean bank. Luo handled these payments as an employee of Dandong Hongxiang, and was working to assist KKBC in violation of U.S. laws. The criminal complaint noted that Deep Wealth was owned or controlled by Dandong Hongxiang, at least as of June 10, 2015.

49. Additionally, Luo facilitated numerous payments to Mingzheng using Deep Wealth Ltd. (“Deep Wealth”), a Dandong Hongxiang front company established in Anguilla, in the months prior to the transactions related to the Defendant Funds.

50. Specifically, Luo received confirmation of two large payments to Mingzheng from Deep Wealth in 2015. On July 31, 2015, Luo received confirmation from China Merchants bank showing that Deep Wealth remitted \$660,000 to Mingzheng’s account ending in 6150. On August 04, 2015, Luo received another confirmation from China Merchants Bank showing that Deep Wealth remitted \$900,000 to the same Mingzheng account. These payments are consistent with the North Korean money laundering activities observed between sanctioned North Korean banks via related front companies.

51. Hong Jinhua, who was charged in the criminal complaint, is the deputy general manager of Dandong Hongxiang. Hong managed U.S. dollar bank accounts on behalf of Dandong Hongxiang and its front companies. Hong was associated with some of the front companies using

her own personal identifying information. One such front company is Nice Field International, Ltd. (“Nice Field”). Nice Field was established in Hong Kong on or about November 12, 2010. Its director is Hong. Nice Field is identified as a Dandong Hongxiang front company in the criminal complaint.

52. On March 06, 2015, Nice Field wired \$199,982.00 to Mingzheng’s BOC account ending in 3100.

53. In addition to the direct payments to Mingzheng from Dandong Hongxiang front companies, other similarities were identified between Mingzheng and Dandong Hongxiang front companies. Notably, Good Field Trading Limited (“Good Field”), Nice Field, and Flying Horse (HK) Ltd. (“Flying Horse”), made/received similar payments to the beneficiaries/remitters of payments made/received by Mingzheng as to the Defendant Funds. A table of Dandong Hongxiang front company payments with the same beneficiaries/remitters from Table 1 is provided below.

**TABLE 2: Dandong Hongxiang front company payments with Mingzheng counterparties**

#	Date	Wire Amount	Party Sending Wire	Party Receiving Wire
1	7/9/2014	\$99,662.00	Nice Field International Limited	Counterparty 3
2	7/14/2014	\$297,752.00	Good Field Trading Limited	Counterparty 9
3	11/10/2014	\$199,998.00	Good Field Trading Limited	Counterparty 5
4	12/5/2014	\$199,342.00	Good Field Trading Limited	Counterparty 3
5	12/19/2014	\$199,998.00	Good Field Trading Limited	Counterparty 5
6	12/22/2014	\$99,982.00	Nice Field International Limited	Counterparty 5
7	12/22/2014	\$164,998.00	Good Field Trading Limited	Counterparty 5
8	1/5/2015	\$209,982.00	Nice Field International Limited	Counterparty 5
9	1/27/2015	\$199,995.00	Flying Horse (HK) Limited	Counterparty 5

#	Date	Wire Amount	Party Sending Wire	Party Receiving Wire
10	3/25/2015	\$199,982.00	Nice Field International Limited	Counterparty 5
11	3/30/2015	\$89,982.00	Good Field Trading Limited	Counterparty 7
12	5/22/2015	\$6,726.34	Good Field Trading Limited	Counterparty 10
13	6/15/2015	\$39,847.00	Good Field Trading Limited	Counterparty 3
14	7/22/2015	\$49,935.00	Counterparty 12	Good Field Trading Limited
15	9/24/2015	\$90,871.00	Good Field Trading Limited	Counterparty 4
16	9/28/2015	\$4,138.20	Good Field Trading Limited	Counterparty 10
17	10/21/2015	\$43,599.71	Good Field Trading Limited	Counterparty 4
18	10/22/2015	\$98,080.00	Deep Wealth Limited	Counterparty 9
19	10/22/2015	\$490,146.65	Good Field Trading Limited	Counterparty 5
20	12/28/2015	\$6,677.00	Nice Field International Limited	Counterparty 12

54. A comparison of Table 1 and Table 2 shows that from July 9, 2015, through October 22, 2015, Dandong Hongxiang front companies (including Nice Field, Good Field, Flying Horse and Deep Wealth) had financial transactions with seven of the 14 companies that were included in Mingzheng's transactions comprising the Defendant Funds. Particularly of note, Counterparty 5 received three payments from Dandong Hongxiang front companies from November 10, 2014 through March 25, 2015, each in the amount of \$199,982.00. Mingzheng made a similar payment to Counterparty 5 on October 29, 2015, for the amount \$199,982.00. These U.S. dollar payments, which cleared through U.S. correspondent banking accounts, violated U.S. law, because Mingzheng was surreptitiously making them on behalf of FTB, whose designation precluded such transactions.

C. MINGZHENG FACILITATES DPRK PAYMENTS TO CHINESE SUPPLIER ZTE THROUGH CHINESE COMPANY 2

55. A search for other financial transactions related to Mingzheng determined that Mingzheng was linked to a series of financial transactions benefiting the Chinese telecommunication company ZTE Corporation (“ZTE”), which pled guilty to U.S sanction violations in March 2017.

56. According to an investigation led by FBI and the Department of Commerce, ZTE was identified as having a significant trade relationship with the Korea Posts and Telecommunications Company (“KPTC”), a North Korean state owned Telecommunications Company. KPTC utilized several intermediary companies to assist with various aspects of the business relationship with ZTE. As part of a U.S. government inquiry into ZTE’s illegal business practices, ZTE allowed an independent auditing company to examine their contract management system and business records. The audit identified at least four Chinese trade companies that were used as the intermediaries for KPTC’s business with ZTE. One of the Chinese trade companies identified as facilitating ZTE’s North Korean business was Chinese Company 2. Mingzheng wired Chinese Company 2 approximately \$2,295,728, while Chinese Company 2 was laundering funds on behalf of the North Korean government to ZTE.

57. CS-2 confirmed that Mingzheng’s SPDB account ending in 6150, one of the known Mingzheng accounts referenced in paragraph 45, was referenced in numerous payment instructions from FTB. These payment instructions included the \$96,345.42 Mingzheng payment to Counterparty 4 that is part of the Defendant Funds. CS-2 further indicated that Mingzheng received confirmation of eight additional payments to/from FTB involving Mingzheng’s CMB account ending in 2808.

58. Mingzheng's payments to ZTE further demonstrate Mingzheng's role as a major front company procuring products in U.S. dollars on behalf of North Korean entities. These U.S. dollar payments, which cleared through U.S. correspondent banking accounts, violated U.S. law, because Mingzheng was surreptitiously making them on behalf of FTB, whose designation precluded such transactions.

**V. SUMMARY OF FACTS GIVING RISE TO FORFEITURE**

59. Sanctions against North Korea make it illegal for North Korean banks, such as FTB, to make payments in U.S. dollars, without an OFAC license.

60. In sum, the investigation has revealed that Mingzheng is a front company acting on behalf of a covert foreign branch of FTB to launder U.S. dollar transactions, in violation of United States laws.

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

61. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 60 above as if fully set forth herein.

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

63. 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 violations of IEEPA and a conspiracy to violate IEEPA.

**COUNT TWO -- FORFEITURE**  
**(18 U.S.C. § 981(A)(1)(A))**

64. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 60 above as if fully set forth herein.

65. FTB, Mingzheng, and others, known and unknown, acted individually and conspired 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, in violation of 18 U.S.C. § 1956(a)(2)(A), (h).

66. 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), (h), or as any property traceable to such property.

\* \* \*



**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 14th day of June, 2017.

Benjamin Whitley  
Benjamin Whitley  
Special Agent  
Federal Bureau of Investigation