

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on November 18, 2022

UNITED STATES OF AMERICA

v.

SIM HYON SOP,

WU HUIHUI,

CHENG HUNG MAN,

and

FNU LNU, a/k/a

“LIVE:JAMMYCHEN0150,” a/k/a

“JAMMY CHEN,”

Defendants.

CRIMINAL NO.

VIOLATIONS:

18 U.S.C. § 1956(h)

(Conspiracy to Launder Monetary
Instruments)

FORFEITURE:

18 U.S.C. § 982(a)(1);

21 U.S.C. § 853(p)

Case: 1:23-cr-00129

Assigned To : Walton, Reggie B.

Assign. Date : 4/18/2023

Description: INDICTMENT (B)

Related Case: 23-cr-128 (RBW)

INDICTMENT

The Grand Jury charges that, at times material to this Indictment:

INTRODUCTION

1. The charges alleged in this Indictment arise from an illicit scheme by North Korean national SIM HYON SOP (심현섭) (“SIM”); Chinese national WU HUIHUI (吴会会) (“WU”); British National (Overseas) CHENG HUNG MAN (郑雄文) (“CHENG”); an unknown user of the online moniker “live:jammychen0150” (referred to herein as “JAMMY CHEN”) (collectively, the “Defendants”), and others to obtain goods for the benefit of the Democratic People’s Republic of Korea (“North Korea”) by laundering funds stolen from virtual asset service providers, converting

those stolen funds into U.S. dollars, and then directing payment for goods using those stolen funds, all in violation of U.S. and UN sanctions against North Korea.

2. Since at least 2014, North Korea has generated revenue by conducting a widespread destructive cyber intrusion campaign, targeting a variety of victim companies in the United States and elsewhere, including, but not limited to, virtual asset service providers. North Korean hackers gained access to the networks of these victim companies, including virtual asset service providers, through, among other methods, social-engineering operations and the use of malicious software (“malware”) exploits and the use of U.S.-based online infrastructure. As to the virtual asset service providers, after gaining access to these victims’ networks, North Korean cyber actors steal virtual currency, which the North Korean actors (and their money laundering co-conspirators) then launder using a variety of laundering techniques. One of these laundering techniques involves leveraging over-the-counter (“OTC”) traders based in China and Hong Kong. These OTC traders facilitate the conversion of stolen virtual currency into U.S. dollars. The purpose of this conversion to U.S. dollars is so that North Korea can use the stolen funds to buy goods for the regime. To buy those goods, North Koreans, such as SIM, along with their money laundering co-conspirators, such as WU, CHENG, and “JAMMY CHEN,” use front companies to obfuscate the fact that the goods are being purchased for the benefit of North Korea. North Korea engages in these criminal activities as a means of evading U.S. sanctions against North Korea, which, among other things, deny North Korea access to the U.S. financial system.

ENTITIES AND INDIVIDUALS

3. At all times relevant to this Indictment:

a. The Foreign Trade Bank of the Democratic People’s Republic of Korea (“FTB”), headquartered in Pyongyang, North Korea, was North Korea’s primary foreign exchange

bank. FTB was a wholly state-owned institution that represented the government of North Korea in international, inter-bank communications. FTB maintained correspondent relationships with different financial institutions in many countries and had offices in several regions of the world. FTB had more than 600 employees in its head office in Pyongyang, and approximately 300 employees worked in branches and subsidiaries. FTB performed functions for the North Korean government including, but not limited to, facilitating credit loans, making investments, regulating the use of foreign currency, setting the exchange rate for the North Korean Won, negotiating with foreign banks, facilitating foreign banking for North Koreans, buying and selling foreign currency, and facilitating the export and import of various commodities.

b. In light of North Korea's ballistic missiles and weapons of mass destruction (WMD) activity, FTB was sanctioned by the UN Security Council and under U.S. law. Under U.S. law, the North Korean government, North Korean entities, including state owned banks such as FTB, or entities acting on behalf of North Korea were barred from access to the U.S. financial system, including by using U.S. dollars via a U.S. correspondent bank, in order to impede North Korea's ballistic missile and weapons of mass destruction programs.

c. Defendant SIM HYONG SOP was a North Korean national and resident of United Arab Emirates (UAE), who had no residence or last known residence in the United States, and who was employed by FTB to act as its representative in Dubai, UAE.



d. Defendant WU HUIHUI was a Chinese resident and national acting as an OTC trader, who had no residence or last known residence in the United States. WU used the online handle “Wakemeupupup” to communicate with co-conspirators regarding this illicit scheme.



e. Defendant CHENG HUNG MAN was a British National (Overseas) living in Hong Kong and acting as an OTC trader, who had no residence or last known residence in the United States. CHENG was associated with the names and/or online monikers “Aiden221” and “Obama.”



f. Defendant FNU LNU, a/k/a “LIVE:JAMMYCHEN0150,” a/k/a “JAMMY CHEN,” was the user of the online moniker “live;jammychen0150,” who had no residence or last known residence in the United States, and who worked as a financial facilitator for SIM.

International Emergency Economic Powers Act

4. The International Emergency Economic Powers Act (“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.

5. The Departments of the Treasury, Commerce, and State enforce and administer sanctions under their respective authorities. 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.

6. 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 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.”

7. On June 28, 2005, the President, to take additional steps with respect to the national emergency described and declared in Executive Order 12938, issued Executive Order 13382 (“Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters”) to target proliferators of WMD and their support networks and to deny designated proliferators access to the U.S. financial and commercial systems. Executive Order 13382 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, as may be necessary to carry out the purposes” of the Executive Order. Pursuant to that authority, on April 13, 2009, the Secretary of the Treasury promulgated the “Weapons of Mass Destruction Proliferators Sanctions Regulations.” *See* 31 C.F.R. § 544.101 *et seq.* Executive Order 13382 and the Weapons of Mass Destruction Proliferators Sanctions Regulations prohibit transactions or dealings by any U.S. person or within the United States with individuals and entities placed on the SDN list, unless exempt or authorized by the Treasury Department’s Office of Foreign Assets Control (OFAC).

8. On March 15, 2016, the President, to take additional steps with respect to the previously described national emergency, issued Executive Order 13722 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 13722 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.

9. Executive Orders 13382 and 13722, the Weapons of Mass Destruction Proliferators Sanctions Regulations, and North Korea Sanctions Regulations also prohibit any transaction by any U.S. person or within the United States that evades or avoids, or has the purpose of evading or avoiding, any prohibition set forth in these regulations.

The Bank Secrecy Act and the USA Patriot Act

10. According to the U.S. Department of the Treasury, 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 anti-money laundering and countering the financing of terrorism requirements set forth in the Bank Secrecy Act (“BSA”), as well as sanctions and blocking programs administered by OFAC. The Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”), which is based in Washington, D.C., is responsible for administering the BSA in furtherance of its mission to safeguard the U.S. financial system.

11. Section 311 of the USA PATRIOT Act, codified at 31 U.S.C. § 5318A, as part of the BSA, gives FinCEN a range of options, called special measures, that can be adapted to target specific money laundering and terrorist financing concerns.

12. 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.

13. In order to protect the integrity of the U.S. financial system, a Section 311 finding can legally prevent 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.

14. In May 2016, FinCEN made a Section 311 finding against North Korea. Specifically, FinCEN's finding deemed the entire North Korean economy as a primary jurisdiction of money-laundering concern. *See* Federal Register, Vol. 81, No. 107 (June 3, 2016). To make such a finding, FinCEN was able to draw upon administrative subpoenas, prior law enforcement investigations, and voluminous BSA data.

15. In November 2016, FinCEN implemented the most severe special measure against the entire North Korean economy. *See* Federal Register, Vol. 81, No. 217 (November 9, 2016). The special measure bars domestic and foreign financial institutions from maintaining U.S. correspondent accounts for any North Korean financial institution or party acting on its behalf. Because of the finding that the entire North Korean financial sector was a primary money laundering concern, FinCEN cut all North Korean entities off from any trade in U.S. dollar transactions via correspondent banking.

16. FinCEN targeted the entire North Korean economy 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 [] and the development of ballistic missiles in violation of international and U.S. sanctions;" and because North Korean financial institutions are subject to "little or no bank supervision or anti-money laundering or combating the financing of terrorism [] controls." *See* Federal Register, Vol. 81, No. 217 at 78715.

The Correspondent Banking System

17. Foreign financial institutions regularly maintain accounts in the United States at banks that process U.S. dollar transactions (“Correspondent Banks”). Accounts at these Correspondent Banks 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. 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 in reserve, such as U.S. dollars. It is through these accounts at Correspondent Banks that the funds used in U.S. dollar transactions clear. SDNs are, among other things, prohibited from accessing Correspondent Banks in the United States through foreign financial institutions, either directly or indirectly.

18. Pursuant to the BSA, financial institutions, including U.S. Correspondent Banks, are required to monitor activity on their networks and report to FinCEN, which is based in Washington, D.C., any suspicious activity, including activity involving, among other things, money laundering and financial crimes.

North Korea’s Foreign Trade Bank

19. On March 11, 2013, the Department of the Treasury designated FTB, North Korea’s primary foreign exchange bank, pursuant to Executive Order 13382, for providing financial services that assisted in the proliferating of WMD. In the designation, Treasury stated, “North Korea uses FTB to facilitate transactions on behalf of actors linked to its proliferation network, which is under increasing pressure from recent international sanctions. . . . By designating FTB, the Treasury Department is targeting a key financial node in North Korea’s WMD apparatus and

cutting it off from the U.S. financial system. FTB is a state-owned bank established in 1959. FTB acts as North Korea's primary foreign exchange bank and has provided key financial support to [another designated entity, Korea Kwangson Banking Corp.].” As a result of the designation, FTB was added to the Treasury Department's Specially Designated National (“SDN”) List, which is published on its website.

North Korea's Reconnaissance General Bureau

20. The Reconnaissance General Bureau (“RGB”) is North Korea's primary intelligence and clandestine operations unit. OFAC designated the RGB on January 2, 2015, pursuant to Executive Order 13687, for being a controlled entity of the Government of North Korea.

21. RGB is known to have a cyber capability that has come to be known within the cybersecurity community as both Lazarus Group and Advanced Persistent Threat 38 (“APT38”). APT38 is a financially motivated North Korean regime-backed group responsible for conducting destructive cyber attacks since at least 2014. Specifically, these North Korean hackers have worked in concert to conduct cyber attacks against victims located in the United States and around the world, including hacks against financial institutions and virtual asset service providers. North Korean actors have gained unauthorized access to these victim networks as part of their fraudulent scheme through a variety of means, including through spear-phishing messages—electronic communications purportedly sent by false and fraudulent personas designed to induce victims to download and execute malicious software developed by the hackers—that were developed through social engineering operations. In furtherance of its global hacking campaign against victims located in the U.S. and elsewhere, North Korean hackers have used U.S.-based online infrastructure, including but not limited to servers located in the United States.

North Korea's Cyber Campaign Targeting Virtual Asset Services Providers

22. As part of its global cyber intrusion campaign, North Korea's RGB cyber actors have targeted and conducted cyberattacks against virtual currency exchanges around the world to generate revenue for the regime. Specifically, North Korean cyber actors have worked in concert to gain unauthorized access to the networks of virtual currency exchanges through a variety of means, including spear phishing campaigns that involve electronic communications sent to victims that contain false and fraudulent pretenses, representations, and promises. These spear phishing communications are designed to appear as though they originate from a trusted source when they are actually fraudulent messages from North Korean cyber actors. The purpose of the communications is to induce victims to download and inadvertently execute malicious software (malware) developed by the hackers.

23. In or around December 2017, as part of its global cyber intrusion campaign dating back to in or around 2014, North Korean cyber actors stole approximately \$75 million in virtual currency from the virtual currency wallets of a particular virtual currency company (referred to herein as "Victim VC Company-1"). The North Korean cyber actors were able to steal those funds after they gained unauthorized access to Victim VC Company-1's networks by sending a spear phishing communication to an employee of Victim VC Company-1. That spear phishing communication contained a malicious link that caused the employee to unintentionally download a file containing malware that was created by the North Korean cyber actors. The virtual currency proceeds from the fraud on Victim VC Company-1 by the North Koreans, along with the proceeds of other virtual currency heists conducted by the North Korean cyber actors, were eventually sent to a particular virtual currency address, 1G3Qj4Y4trA8S64zHFsaD5GtiSwX19qwFv ("BTC Address 1G3Qj4").

North Korea's Use of OTC Traders to Launder Stolen Virtual Currency

24. After North Korean cyber actors obtain stolen virtual currency from heists of virtual asset service providers, the stolen virtual currency needs to be laundered and converted to fiat currency so that the North Koreans can use the funds to circumvent the sanction regime. One mechanism for laundering these stolen funds and converting them to fiat currency is via OTC traders.

25. To buy and sell virtual currency assets, most virtual currency exchanges allow potential customers to create an account on the exchange's platform. This account creation process and/or the use of exchanger services on the platform typically requires, pursuant to the BSA, that the potential customer provide documentation about his/her identity (*i.e.*, know-your-customer or KYC information). If that potential customer does not want to register for an account at the exchange but would still like to trade virtual currency-for-virtual currency, virtual currency-for-fiat currency, or fiat currency-for-virtual currency, then it is possible for that potential customer to do so via an OTC trader.

26. In the virtual currency context, OTC traders act as middlemen, providing liquidity in virtual currency markets by matching buyers and sellers. An OTC trader can facilitate these transactions in a number of ways, including by using his/her account at a virtual currency exchange and/or traditional bank to conduct transactions (for a fee) on behalf of his/her customers who would like to exchange one type of currency for another but either do not have an account at said exchange or do not want to use their own account for transaction anonymity purposes. OTC traders operating for clients looking to avoid regulatory requirements typically charge a premium, at times as high as approximately fifteen percent of the transaction cost.

27. The UN Security Council's March 4, 2021 Report of the Panel of Experts noted North Korea's historical and continued use of OTC virtual asset brokers, especially those in China, as a laundering mechanism. *See* United Nations Security Council's 4 March 2021 Report of the Panel of Experts, at 56.

THE DEFENDANTS' SCHEME TO LAUNDER STOLEN VIRTUAL CURRENCY

28. From at least in or about 2018, and up to and including in or about 2021 (the "relevant time period"), SIM HYON SOP, WU HUIHUI, CHENG HUNG MAN, and "JAMMY CHEN," the Defendants, together with other co-conspirators known and unknown to the Grand Jury, conspired to convert virtual currency that had been stolen by North Korean cyber actors to U.S. dollars. The Defendants did so through the use of a variety of obfuscation techniques, such as utilizing sham front companies and creating fraudulent documents, to make payments for goods on behalf of North Korea. During the relevant time period, SIM, a North Korean FTB representative, directed payment instructions for goods in U.S. dollars. Those payment instructions were transmitted to "JAMMY CHEN." Once "JAMMY CHEN" received the payment instructions, "JAMMY CHEN" contacted WU and CHENG, both of whom operated as OTC traders, to enlist their assistance in facilitating the payments. To facilitate these payments, "JAMMY CHEN" used the proceeds of stolen bitcoin ("BTC") as the funding source; including BTC from BTC Address 1G3Qj4, which contained proceeds of, among other things, North Korea's heist of virtual currency from Victim VC Company-1.

29. WU, CHENG, and "JAMMY CHEN" then utilized a variety of sham companies, including four Hong Kong-based front companies (referred to herein as "Front Company-1," "Front Company-2," "Front Company-3," and "Front Company-4" individually, and collectively "Front Companies"), to make payments for goods in U.S. dollars. Each of the Front Companies

was registered to do business in Hong Kong and held an account at the same Hong Kong-based bank. Additionally, three of the four Front Companies used the same address in Hong Kong as their physical registration address. After choosing sham companies for each transaction, "JAMMY CHEN" sent BTC to WU and CHENG from BTC Address 1G3Qj4, and then WU and CHENG facilitated payment for goods in U.S. dollars via the Front Companies.

30. In turn, WU, CHENG, and "JAMMY CHEN" used the Front Companies to make payments in U.S. dollars to bank accounts owned by: (1) two individuals (referred to herein as "Payee Individual-1" and "Payee Individual-2," respectively) at a Thailand-based bank (referred to herein as "Bangkok Bank-1"); (2) a company involved in the procurement and/or distribution of tobacco products that was registered to do business in the UAE (referred to herein as "Payee Entity-1") at a UAE-based bank (referred to herein as "UAE Bank-1"); and (3) a licensed manufacturer of tobacco products in Bulgaria (referred to herein as "Payee Entity-2") at a Bulgaria-based bank (referred to herein as "Bulgaria Bank-1"). These payments were for tobacco-related products and communications equipment. The payments were effectuated through the use of correspondent bank accounts, including two correspondent bank accounts located at two different banks in the United States (referred to herein as "U.S. Correspondent Bank-1" and "U.S. Correspondent Bank-2").

31. Over the course of the relevant time period, SIM communicated with co-conspirators regarding the fact that intermediary banks were necessary to facilitate international wire transactions in fiat currency, including U.S. dollars. In those communications, the co-conspirators also made repeated references to the U.S. correspondent banks used in this scheme, including U.S. Correspondent Bank-1.

32. Over the course of the relevant time period, WU and “JAMMY CHEN” discussed the involvement of intermediary banks in transactions in fiat currency. They also discussed contacting a payee regarding which intermediary bank was involved in a particular transaction.

33. As part of their scheme, the Defendants caused, among other things, the following four payments to be made on behalf of North Korea, including using U.S. Correspondent Bank-1 and U.S. Correspondent Bank-2.

Payment #1

34. On or about July 9, 2018, SIM emailed payment instructions to his co-conspirators, instructing that a payment should be made in the amount of \$49,302 to Payee Individual-1 and Payee Individual-2 for a “Communication Device.” Shortly thereafter, “JAMMY CHEN” sent an online message to WU, containing the same payment instructions.

35. On or about July 10, 2018, “JAMMY CHEN” directed WU to send the funds to Payee Individual-1 and Payee Individual-2 via Front Company-1’s bank account in Hong Kong (referred to herein as “Hong Kong Bank-1”). In response, WU sent “JAMMY CHEN” a message that read “7.676 btc” and identified BTC address 1Bpf1be3DqGyL24ymhjbk5DRojjxQVpGLs (“BTC Address 1Bpf1b”). “JAMMY CHEN” then provided WU a link to a public blockchain explorer, an online tool that allows users to search and review transactional data for BTC addresses and transactions conducted on the BTC blockchain. That link confirmed that BTC Address 1G3Qj4 (*i.e.*, the virtual currency wallet containing funds traceable to North Korea’s hack of Victim VC Company-1) had sent 7.676 BTC to BTC Address 1Bpf1b. 7.676 BTC was worth approximately \$50,602.49 at the time of the transaction.

36. Later that day, WU provided “JAMMY CHEN” with a payment confirmation showing that a payment of \$49,302 had been sent from Front Company-1’s account at Hong Kong

Bank-1 to Payee Individual-1 and Payee Individual-2's bank account at Bangkok Bank-1. Included in the reference field for the payment confirmation was "Communication Device." This payment was executed through U.S. Correspondent Bank-1. SIM received and retained a copy of the same payment confirmation.

Payments #2 and #3

37. On or about July 9, 2018, SIM emailed payment instructions to his co-conspirators, instructing that a payment should be made in the amount of \$750,000 to UAE-based Payee Entity-1. Shortly thereafter, "JAMMY CHEN" sent an online message to WU requesting assistance in making a payment to Payee Entity-1 in the amount of \$385,320.

38. Between on or about July 9, 2018, and on or about July 11, 2018, WU and "JAMMY CHEN" communicated regarding options for using companies to remit payment in U.S. dollars to the UAE and their difficulty in finding companies willing to do so.

39. On or about July 11, 2018, "JAMMY CHEN" explained to WU that the full amount to be sent to Payee Company-1 was \$750,000, and that "JAMMY CHEN" had split the \$750,000 payment in two: (1) the \$385,320 that WU was meant to facilitate; and (2) \$364,680 that another OTC trader had already fulfilled on or about July 10, 2018. WU and JAMMY CHEN discussed that the OTC trader responsible for the July 10, 2018 payment was CHENG.

40. On or about July 11, 2018, WU shared the corporate registration documents for Front Company-2 with JAMMY CHEN, indicating that Front Company-2 may be an option for sending U.S. dollars to UAE-based Payee Company-1. "JAMMY CHEN" told WU that they could not use Front Company-2 to make the \$385,320 payment because CHENG had already used Front Company-2 to make the payment for \$364,680 on or about July 10, 2018. The payment for \$364,680 sent from Front Company-2's bank account (which was held at Hong Kong Bank-1) to

Payee Company-1's account at UAE Bank-1 was executed through U.S. Correspondent Bank-1. WU shared with CHENG a screenshot of WU's conversation with "JAMMY CHEN" regarding the use of Front Company-2.

41. Shortly after "JAMMY CHEN" informed WU that WU could not use Front Company-2 for the payment, WU shared corporate registration documents for Front Company-3. Subsequently, both WU and SIM received and retained an electronic copy of a payment confirmation from July 12, 2018, for a payment of \$384,320.98 from Front Company-3's Hong Kong-based bank account, which was also held at Hong Kong Bank-1, to Payee Entity-1's bank account at UAE Bank-1. This payment was executed through U.S. Correspondent Bank-2.

Payment #4

42. On or about July 11, 2018, SIM emailed payment instructions to his co-conspirators, instructing that a payment should be made to Bulgaria-based Payee Entity-2, in the amount of \$30,000, with a reference to a particular invoice as follows: "INV.NO: 2425/23.05.2018." Shortly thereafter, "JAMMY CHEN" sent an online message to WU with the same banking details, instructing that WU should use Front Company-1 to execute the payment the next day, July 12, 2018.

43. Thereafter, WU and SIM received and retained a copy of payment confirmation for \$30,000 on July 12, 2018, from Front Company-1's bank account at Hong Kong Bank-1 to Payee Company-2's bank account at Bulgaria Bank-1, under invoice number "2425/23,05.2018." This payment was executed through U.S. Correspondent Bank-1.

44. On or about August 3, 2018, "JAMMY CHEN" sent a communication to WU indicating that he had a problem with the July 12, 2018 payment to Payee Entity-2. WU asked what was wrong, and "JAMMY CHEN" sent WU a file labeled: "Letter payment-[Front Company-

1].pdf.” JAMMY CHEN asked WU to read, stamp, and sign the letter, which was backdated to July 12, 2018; shortly thereafter, WU returned the document to “JAMMY CHEN.”

45. On or about August 3, 2018, SIM sent an email to a representative of Payee Entity-2, with a copy of the letter that WU had sent to “JAMMY CHEN,” which was signed, stamped, and dated July 12, 2018. The letter indicated that Front Company-1 had remitted a payment in the amount of \$29,962.38 for “invoice No.2425/23.05.2018 to Invoice No. 0-31581 dated 19.06.2018.” The letter indicated that Payee Entity-2 issued the invoices to Front Company-4. Both WU and SIM retained electronic copies of the letter; WU’s version was stamped but not signed, while SIM’s version was both signed and stamped.

COUNT ONE
(Conspiracy to Launder Monetary Instruments)

46. The allegations set forth in paragraphs 1 through 45 of this Indictment are re-alleged and incorporated herein.

47. From at least in or about 2018, and up to and including in or about 2021, beginning out of the jurisdiction of any particular States or district and, pursuant to 18 U.S.C. § 3238, within the venue of the United States District Court for the District of Columbia, and continuing within the jurisdiction of the District of Columbia, pursuant to 18 U.S.C. § 3237(a), defendants SIM HYON SOP, WU HUIHUI, CHENG HUNG MAN, and “JAMMY CHEN,” together with other co-conspirators known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree to commit offenses against the United States, in violation of:

a. Title 18, United States Code, Section 1956(a)(1)(B)(i), by conducting and attempting to conduct financial transactions affecting interstate and foreign commerce, to wit, using front companies and fraudulent documents to facilitate at least four payments in U.S. dollars that required the use correspondent bank accounts, including two correspondent bank accounts

located at two different banks in the United States, for goods destined for North Korea, involving the proceeds of specified unlawful activity, to wit, a conspiracy to commit wire fraud to obtain virtual currency from virtual currency companies, in violation of Title 18, United States Code, Section 1349, knowing that the property involved in these financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity;

b. Title 18, United States Code, Section 1956(a)(2)(A), by transporting, transmitting, and transferring, and attempting to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States and to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, (i) a conspiracy to commit wire fraud to defraud financial institutions regarding the true originator and beneficiaries of illegal transactions , in violation of Title 18, United States Code, Section 1349; and (ii) the export of financial services from the United States to an SDN in North Korea without having first obtained the required license from OFAC, located in the District of Columbia, in violation of Title 50, United States Code, Sections 1702 and 1705; the Weapons of Mass Destruction Proliferators Sanctions Regulations, pursuant to Title 31, Code of Federal Regulations, Section 544.201, *et seq.*; and North Korea Sanctions Regulations, pursuant to Title 31, Code of Federal Regulations, Section 510.201, *et seq.*; and

c. Title 18, United States Code, Section 1956(a)(2)(B)(i), by transporting, transmitting, and transferring, and attempting to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United

States and to a place in the United States from and through a place outside the United States, knowing that the monetary instrument and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity, to wit, North Korea's scheme to obtain virtual currency via false, fraudulent pretenses, representations, and promises, and knowing that such transportation, transmission, and transfer was designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, to wit, a conspiracy to commit wire fraud to obtain virtual currency from virtual currency companies, in violation of Title 18, United States Code, Section 1349.

Goals

48. The goals and purposes of the conspiracy were, among others:
- a. to generate revenue for North Korea;
 - b. to access the U.S. financial system in violation of U.S. sanctions against North Korea; and
 - c. to promote the provision of financial services for an SDN without the necessary OFAC licenses.

Manner and Means

49. It was further a part of the conspiracy that the Defendants used the following manner and means, among others, to achieve the goals of the conspiracy:
- a. The Defendants and other co-conspirators caused payments to be sent by front companies to obfuscate North Korea's nexus to the transactions.
 - b. The Defendants and other co-conspirators caused false information to be listed on payment documents to hide North Korea's connection to those transactions.

- c. The Defendants and other co-conspirators concealed FTB's involvement in U.S. dollar payments from Correspondent Banks.
- d. The Defendants and other co-conspirators used email accounts and other messaging platforms to communicate about the payment schemes, the use of front companies, and the provision of false information, including to U.S. financial institutions.
- e. The Defendants and other co-conspirators caused Correspondent Banks to process over \$800,000 in illegal payments via Hong Kong-based front companies.

(Conspiracy to Launder of Monetary Instruments, in violation of Title 18, United States Code, Section 1956(h))

FORFEITURE ALLEGATION

50. The allegations contained in Count One of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 982(a)(1). Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of the offense alleged in Count One, violation of Title 18, United States Code, Section 1956(h), Defendants shall forfeit to the United States of America any property, real or personal, involved in such offense, and any property traceable to such property. The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, which constitutes, or is derived from proceeds traceable to this offense.


51. If any of the property described above, as a result of any act or omission of the Defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

A TRUE BILL

FOREPERSON


Attorney of the United States in
and for the District of Columbia