UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

January 2020 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

JON CHANG HYOK,
aka "Quan Jiang,"
aka "Alex Jiang,"
KIM IL,
aka "Julien Kim,"
aka "Tony Walker," and
PARK JIN HYOK,
aka "Jin Hyok Park,"
aka "Pak Jin Hek,"
aka "Pak Kwang Jin,"

Defendants.

CR 2:20-cr-00614-DMG

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud and Bank Fraud; 18 U.S.C. §§ 982, 1030: Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At times relevant to this Indictment:

A. The Conspiracy and Defendants

1. The Democratic People's Republic of Korea ("DPRK"), also known as ("aka") North Korea, operated a military intelligence agency called the Reconnaissance General Bureau ("RGB"). The RGB was headquartered in Pyongyang, DPRK, and comprised multiple units.

2. Defendants JON CHANG HYOK (전창혁), aka “Quan Jiang,” aka “Alex Jiang”; KIM IL (김일), aka “Julien Kim,” aka “Tony Walker”; and PARK JIN HYOK (박진혁), aka “Jin Hyok Park,” aka “Pak Jin Hek,” aka “Pak Kwang Jin” (collectively, the “defendants”), whose photographs are attached as Exhibit A through Exhibit C, respectively, were members of units of the RGB who knowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury (collectively, with the defendants, referred to as the “conspirators” and the “hackers”), to conduct criminal cyber intrusions.

3. The defendants and other conspirators resided in the DPRK, but, at times during the operation of the conspiracy, traveled to and worked from other countries -- including the People’s Republic of China and the Russian Federation -- while employed by units of the RGB. The conspirators included members of units of the RGB that have come to be known within the cyber-security community as both Lazarus Group and Advanced Persistent Threat 38 (“APT38”).

4. The conspirators hacked into the computers of victims to cause damage, steal data and money, and otherwise further the strategic and financial interests of the DPRK government and its leader, Kim Jong Un (the “DPRK regime”). In some instances, the hackers sought to cause damage through computer intrusions in response to perceived reputational harm or to obtain information furthering strategic interests of the DPRK regime. In many instances, the hackers intended the computer intrusions to steal currency and virtual currency (also known as “cryptocurrency”), or to obtain it through extortion, for the benefit of the DPRK regime -- and, at times, for their own private financial gain. The hackers attempted to steal or extort more than $1.3 billion from victims in

cyber-enabled heists and Automated Teller Machine ("ATM") cash-outs from banks, cyber-enabled heists from cryptocurrency companies, and cyber-enabled extortion schemes.

5. The hackers' victims and intended victims included entertainment companies, financial institutions, cryptocurrency companies (including cryptocurrency exchanges, traders, and marketplaces), online casinos, cleared defense contractors, energy utilities, and individuals. The hackers hacked and defrauded victims around the world -- including in Bangladesh, Malta, Mexico, Indonesia, Pakistan, the Philippines, Poland, the Republic of Korea, Slovenia, Taiwan, the United Kingdom, Vietnam, Central America, and Africa -- as well as in the United States and, specifically, the Central District of California. The hackers targeted victims in numerous other countries, as well, and used infrastructure and online accounts from around the world in furtherance of the computer intrusions, including infrastructure located in the Central District of California.

6. The computer intrusions often started with fraudulent, spear-phishing messages -- emails and other electronic communications designed to make intended victims download and execute malicious software ("malware") developed by the hackers. At other times, the spear-phishing messages would encourage intended victims to download or invest in a cryptocurrency-related software program created by the hackers, which covertly contained malicious code and/or would subsequently be updated with malicious code after the program was downloaded (a "malicious cryptocurrency application"). To hone the spear-phishing messages, the hackers would conduct internet research regarding their intended victims and would send "test" spear-phishing

messages to each other or themselves. The hackers employed false and fraudulent personas when they sent spear-phishing messages to victims.

7. Once they gained access to a victim computer system, the hackers would conduct research within the system, attempt to move laterally within a computer network, and attempt to locate and exfiltrate sensitive and confidential information. In both revenge- and financially-motivated computer attacks, the hackers would, at times, execute commands to destroy computer systems, deploy ransomware, or otherwise render the computers of their victims inoperable.

8. The hackers took steps to avoid detection and attribution of their computer intrusions to themselves, the RGB, and the DPRK. However, the computer infrastructure and online accounts used in the computer intrusions, and technical similarities in the malware employed, connected these computer intrusions with the hackers, showing that (a) the defendants and other hackers were conspiring with one another, (b) they were members of the RGB, and (c) the computer intrusions were part of a single hacking conspiracy.

B. The Hackers' Targets

Entertainment Companies

9. Sony Pictures Entertainment Inc. ("Sony Pictures") was an American entertainment company, headquartered in Culver City, California, that produced and distributed filmed entertainment, including the movie "The Interview," which depicted the fictionalized assassination of Kim Jong Un, whom it parodied. Sony Pictures maintained computer systems, including servers hosting employee data and servers hosting intellectual property, in Los Angeles County,

within the Central District of California, that operated in interstate and foreign commerce.

10. AMC Theatres was an American movie theater chain headquartered in Leawood, Kansas, which was set to show "The Interview" in its theaters prior to the cyber-attack on Sony Pictures.

11. Mammoth Screen was a United Kingdom television production company that was producing "Opposite Number," a ten-part fictional series about a British nuclear scientist on a covert mission who was taken prisoner in the DPRK.

Financial Institutions and Financial Regulators

12. The "African Bank" was a bank headquartered in a country in Africa.

13. Bangladesh Bank, the central bank of Bangladesh, was headquartered in Dhaka, Bangladesh.

14. Banco Nacional De Comercio Exterior, which is also known as "Bancomext," was a Mexican state-owned bank headquartered in Mexico City, Mexico.

15. The "Maltese Bank" was a bank headquartered in Malta.

16. BankIslami Pakistan Limited, which is also known as "BankIslami," was a bank headquartered in Karachi, Pakistan.

17. The "New York Financial Services Company" was a financial services company headquartered in New York, New York.

18. The Polish Financial Supervision Authority was the financial regulatory authority for Poland, and was based in Warsaw, Poland.

19. The "Philippine Bank" was a bank headquartered in Makati, Philippines.

20. Far Eastern International Bank was a bank headquartered in Taipei, Taiwan.

21. The "Vietnamese Bank" was a bank headquartered in Hanoi, Vietnam.

Cryptocurrency Companies

22. The "Indonesian Cryptocurrency Company" was a cryptocurrency exchange based in Jakarta, Indonesia.

23. The "South Korean Cryptocurrency Company" was a cryptocurrency exchange based in the Republic of Korea.

24. The "Slovenian Cryptocurrency Company" was a crypto-mining company headquartered in Ljubljana, Slovenia.

Online Casino Companies

25. "Central American Online Casino 1" was an online casino business headquartered in a Central American country.

26. "Central American Online Casino 2" was an online casino business headquartered in a Central American country.

C. Definitions

27. An Internet Protocol version 4 address, also known as an "IPv4 address," or more commonly an "IP address," is a set of four numbers or "octets," each ranging from 0 to 255 and separated by a period (".") that is used to route traffic on the internet. A single IP address can manage internet traffic for more than one computer or device, such as in a workspace or when a router in one's home routes traffic to one's desktop computer, as well as one's tablet or smartphone, while all using the same IP address to access the internet.

28. "Malware" is malicious computer software intended to cause a victim computer to behave in a manner inconsistent with the

intention of the owner or user of the victim computer, usually unbeknownst to that person. The hackers developed and used numerous types of malware, including worms, ransomware, credential-stealers, key-loggers, screen-grabbers, and backdoors.

29. "Brambul" is a type of "worm" malware that spreads through self-replication by infecting new victim systems via brute force attacks on the victim's Server Message Block ("SMB") protocol. SMB is a method that Microsoft systems use to share files on a network. A brute force attack is a computer network attack that attempts to login to a potential victim computer, server, or account using a predetermined list of possible username and password combinations, which lists often contain thousands of common combinations of usernames and passwords that include specific default settings used on certain applications and devices. Upon successfully gaining access to a victim computer, Brambul conducts a survey of the victim machine and collects information, including the victim's IP address, system name, operating system, username last logged in, and last password used. Brambul then sends that information via Simple Mail Transfer Protocol to one or more of the email addresses ("Brambul collector accounts") that are hard-coded in Brambul.

30. "Ransomware" is a type of malware that infects a computer and encrypts some or all of the data or files on the computer, and then demands that the victim pay a ransom in order to decrypt and recover the files, or in order to prevent the hacker from distributing or destroying the data.

31. A "watering hole" is a type of computer intrusion technique in which a hacker uses malware to compromise a website known to be visited by intended victims. The malware then infects the computers

of intended victims (and sometimes unintended victims) who visit the website, giving the hacker access to the victims' computers and networks.

32. "Command and control" IP addresses or domains -- sometimes referred to as "C2s" -- are computers with which malware communicates to send and receive data and commands.

33. A "spear-phishing" message is a tailored and personalized email or other electronic communication designed to appear legitimate in order to induce the targeted recipient(s) to take a certain action -- such as clicking on a link, or downloading or opening a file -- that would cause a victim's computer to be compromised by a hacker. Spear-phishing messages often include information that the hacker knows about the recipient(s) based on research or other sources of information about the intended victim.

34. "Cryptocurrency" or "virtual currency" is a digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units of the currency, and verify and transfer assets. Cryptocurrency is typically accessed using secret or private encryption "keys" which are commonly stored using a software "wallet." Cryptocurrency "exchanges" are clearinghouses that allow for the exchange between different types of cryptocurrencies, or between cryptocurrency and fiat currency. "Crypto-mining" is a means of generating new units of cryptocurrency.

35. An "initial coin offering" or "ICO" is the cryptocurrency equivalent of a stock's Initial Public Offering or "IPO" -- that is, a cryptocurrency developer's first offer to sell a stake in a cryptocurrency to the public.

COUNT ONE

[18 U.S.C. § 371]

36. The Grand Jury re-alleges and incorporates paragraphs 1 through 35 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECTS OF THE CONSPIRACY

37. Beginning on a date unknown to the Grand Jury, but no later than September 28, 2009, and continuing through at least December 8, 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendants JON CHANG HYOK, KIM IL, and PARK JIN HYOK, together with others known and unknown to the Grand Jury, knowingly conspired:

a. to intentionally access computers without authorization and obtain information from protected computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i)-(iii);

b. to knowingly and with intent to defraud access protected computers without authorization, and by means of such conduct further the intended fraud and obtain a thing of value, in violation of Title 18, United States Code, Section 1030(a)(4), (c)(3)(A);

c. to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct intentionally cause damage without authorization to protected computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI); and

d. to transmit in interstate and foreign commerce, with the intent to extort money and other things of value, a communication containing (i) a threat to cause damage to a protected computer, (ii) a threat to impair the confidentiality of information obtained from a protected computer without authorization, and (iii) a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Section 1030(a)(7)(A)–(C), (c)(3)(A).

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

38. The objects of the conspiracy were to be accomplished, in substance, as follows:

Development and Dissemination of Malware

a. The hackers would develop malware that could be transmitted to potential victims in order to gain unauthorized access to the computer(s) of the victims. Such malware would include the Brambul worm, ransomware, and other types of malware.

b. At times, the hackers would conceal the malware within seemingly legitimate word processing documents or software applications, including programs related to cryptocurrency trading (i.e., malicious cryptocurrency applications), which the hackers would falsely and fraudulently, and through the omission of material facts, market as being legitimate software applications. Malicious cryptocurrency applications would contain, or would through a subsequent software update process be updated to contain, malicious code that would provide the hackers with unauthorized access to the computers of persons who downloaded the applications.

c. At other times, the hackers would conceal the malware within legitimate websites in order to infect victims visiting the websites (i.e., a watering hole).

d. Defendants JON CHANG HYOK, KIM IL, PARK JIN HYOK, and other conspirators, would register and use email and social media accounts in false and fraudulent names -- including the names of real persons -- to use in gaining unauthorized access to victim computers, including to contact potential victims, send spear-phishing messages, register other accounts used by the hackers, and/or serve as Brambul collector accounts.

e. Hackers would use the internet to research potential victims with whom they would attempt to communicate.

f. Defendants JON CHANG HYOK, KIM IL, and other conspirators, would communicate with potential victims using false and fraudulent names, sending spear-phishing messages or electronic messages designed to establish a relationship with the intended victim before sending a later spear-phishing message. The hackers would communicate with individuals in a variety of sectors, including entertainment companies, financial institutions, hundreds of cryptocurrency companies, online casinos, cleared defense contractors, energy utilities, technology companies, and government agencies.

g. Defendants JON CHANG HYOK, KIM IL, and other conspirators, would send misleading and fraudulent communications to potential victims containing malware or directing the potential victims to download malware, including malicious cryptocurrency applications, ransomware, and other malware.

h. At times, to carry out computer intrusions or attempted intrusions, hackers would use or access computer infrastructure that they had compromised through the Brambul worm or a watering hole.

Destructive Cyberattacks, and Attempted Cyberattacks, on Entertainment Companies

i. After malware was installed on the computer(s) of an intended victim entertainment company, the hackers would use the malware to access the computer(s) without authorization and install other malware.

j. The hackers would then access the computer(s) of the victim entertainment company without authorization and attempt to access other computer systems connected to the computer(s) to steal confidential credentials, files, data, unreleased movies, and other information that could be damaging or embarrassing to the entertainment company.

k. The hackers would then install destructive malware on the victim entertainment company's computers, which malware could be used to destroy or impair the computers and render them inoperable, and to conceal forensic evidence of the hackers' unauthorized access.

l. After successfully installing destructive malware on computers of the victim entertainment company, the hackers would, at a later date, make threatening communications to the victim entertainment company using false and fraudulent personas, publicly disseminate the victim entertainment company's confidential internal information, and activate destructive capabilities of the malware the hackers previously installed in order to destroy or impair the victim entertainment company's computers and render them inoperable.

Bank Cyber-Enabled Heists

m. After malware was installed on the computer(s) of an intended victim bank, the hackers would use the malware to access the computer(s) without authorization and install other malware.

n. The hackers would access the computer(s) of the victim bank without authorization and attempt to move through the bank's network in order to access one or more computers that the victim bank used to send or receive messages through the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") communication system.

o. The hackers would develop and deploy malware customized to the computer network of the victim bank, in order to send fraudulent SWIFT messages from the victim bank's computer system, authorizing fraudulent wire transfers to bank accounts used and controlled by the hackers, including accounts at United States federally insured financial institutions.

p. The hackers also would develop and deploy destructive malware to conceal their point of access to the victim bank's computer network, their path through the victim bank's computer network, and the fraudulent wire transfers.

q. At times, the hackers would install, on the computer(s), malware designed to destroy, impair, or render inoperable the victim bank's computer network or computers within the network, and to conceal forensic evidence of the hackers' unauthorized access to the computer(s).

Cyber-Enabled Extortions

r. After malware was installed on the computer(s) of an intended extortion victim, the hackers would use the malware to

access the computer(s) without authorization and install other malware.

s. The hackers would then access the computer(s) of the extortion victim without authorization and attempt to access other computer systems connected to the computer(s) to steal confidential credentials, files, data, and other information that could be damaging or embarrassing to the extortion victim.

t. At times, the hackers would install ransomware on the computer(s) of the extortion victim in order to render the computer(s) inaccessible and inoperable.

u. The hackers would then communicate with the extortion victim, demanding a payment in a cryptocurrency, such as Bitcoin, in exchange for not publicly releasing the extortion victim's files that had been stolen or unencrypting any computers infected by ransomware.

v. The hackers would, at times, offer to tell the extortion victim how the hackers had accessed the extortion victim's computer(s) if additional ransom payments were made.

w. If the extortion victim did not pay the hackers' ransom demands, the hackers would threaten to -- and would in fact -- publicly disseminate confidential information stolen from the computer(s) of the extortion victim, destroy the information and not return a copy, or leave the computer(s) of the victim encrypted with ransomware.

Cryptocurrency Heists

x. After malware, such as a malicious cryptocurrency application, was installed on the computer(s) of an intended victim cryptocurrency company, the hackers would use the malware to access the computer(s) without authorization and install other malware.

y. The hackers would access the computer(s) of the victim cryptocurrency company without authorization and attempt to move through the victim cryptocurrency company's computer network in order to access a computer that would provide access to the victim cryptocurrency company's cryptocurrency wallet(s) and private keys to the wallet.

z. Once they had access to the wallet(s) and private keys of the victim cryptocurrency company, the hackers would fraudulently and without authorization transfer cryptocurrency from those wallets to wallets used and controlled by the hackers.

ATM Cash-Outs

aa. After malware was installed on the computer(s) of an intended victim bank, the hackers would use the malware to access the computer(s) without authorization and install other malware.

bb. The hackers would access the computer(s) of the victim bank without authorization and attempt to move through the victim bank's computer network in order to access one or more computers that the victim bank used to manage ATM transactions.

cc. The hackers would develop and deploy malware customized to the computer network of the victim bank, in order to intercept ATM transaction data and cause fraudulent ATM withdrawal requests to be approved, which would cause a requesting ATM to dispense cash to money-launderer coconspirators.

dd. The hackers also developed and deployed malware to conceal their point of access to the victim bank's computer network, their path through the victim bank's computer network, and the fraudulent ATM withdrawal requests.

C. OVERT ACTS

39. In furtherance of the conspiracy, and to accomplish its objects, defendants JON CHANG HYOK, KIM IL, and PARK JIN HYOK, together with others known and unknown to the Grand Jury, on or about the dates set forth below, committed and caused to be committed various overt acts, in the Central District of California and elsewhere, including, but not limited to, the following:

Destructive Cyberattacks, and Attempted Cyberattacks, on Entertainment Companies

Overt Act No. 1: Beginning on November 24, 2014, after sending threatening communications to Sony Pictures employees, the hackers initiated a destructive cyber-attack of Sony Pictures computers, publicly disseminated Sony Pictures' confidential data and communications stolen from its computers, and made further threats against the company and its employees.

Overt Act No. 2: On December 2 and 3, 2014, the hackers sent spear-phishing messages to AMC Theatres employees from multiple email accounts.

Overt Act No. 3: At an unknown date in 2015, the hackers gained unauthorized access to the computers of Mammoth Screen.

Cyber-Enabled Heists from, and Intrusions of, Banks

Overt Act No. 4: Beginning in or around November 2015, the hackers gained unauthorized access to the Philippine Bank's computer network, but did not succeed in making fraudulent wire transfers before the unauthorized access was detected and mitigated.

Overt Act No. 5: On December 9, 2015, having gained unauthorized access to the Vietnamese Bank's computer network at an earlier date, the hackers conducted false and fraudulent wire

transfers totaling approximately €2 million to bank accounts in Slovenia and Bulgaria, and attempted to conduct fraudulent wire transfers of approximately $3.4 million to Russia, A$1 million to Australia, and ¥90 million to Japan.

Overt Act No. 6: On February 4, 2016, having gained unauthorized access to Bangladesh Bank's computer network at an earlier date, the hackers attempted to conduct false and fraudulent wire transfers totaling approximately $951 million, and conducted false and fraudulent wire transfers totaling approximately $81 million to bank accounts in the Philippines and $20 million to a bank account in Sri Lanka, which moneys all belonged to Bangladesh Bank and were held in accounts at the Federal Reserve Bank of New York.

Overt Act No. 7: On July 20, 2016, having gained unauthorized access to the African Bank's computer network at an earlier date, the hackers conducted false and fraudulent wire transfers totaling approximately $104.1 million to bank accounts in Taiwan, Thailand, and Cambodia.

Overt Act No. 8: Beginning in or around October 2016, the hackers gained unauthorized access to the computer network of the Polish Financial Supervision Authority and made its website into a watering hole.

Overt Act No. 9: On October 3, 2017, having gained unauthorized access to Far Eastern International Bank's computer network at an earlier date, the hackers conducted false and fraudulent wire transfers totaling approximately $60.1 million to bank accounts in Sri Lanka, Cambodia, and the United States.

Overt Act No. 10: On January 9, 2018, having gained unauthorized access to Bancomext's computer network at an earlier date, the hackers conducted false and fraudulent wire transfers totaling approximately $110 million to bank accounts in the Republic of Korea, and then deployed malware on more than 400 of Bancomext's computers.

Overt Act No. 11: In January and February 2019, defendant KIM IL or another hacker communicated with unindicted coconspirator Ghaleb Alaumary regarding bank accounts that could receive false and fraudulent wire transfers from the Maltese Bank.

Overt Act No. 12: On February 12, 2019, having gained unauthorized access to the Maltese Bank's computer network at an earlier date, the hackers conducted false and fraudulent wire transfers totaling approximately $6.4 million and €7.1 million to bank accounts in Hong Kong, the United Kingdom, the United States, and the Czech Republic.

Cyber-Enabled Extortions and Ransomware

Overt Act No. 13: On or before May 12, 2017, the hackers authored the ransomware used in a global, destructive cyber-attack known publicly as WannaCry Version 2.

Overt Act No. 14: On June 29, 2017, having gained unauthorized access to a computer system at an earlier date and stolen confidential customer information of the South Korean Cryptocurrency Company, the hackers publicly released that information after the South Korean Cryptocurrency Company refused to pay a ransom of approximately $16 million in cryptocurrency.

Overt Act No. 15: On August 24, 2017, having gained unauthorized access to a computer system of a victim company at an

earlier date, the hackers deployed ransomware on the computer system and then extorted payments totaling approximately $100,000 in cryptocurrency from the victim.

Overt Act No. 16: On October 13, 2017, having gained unauthorized access to the computer network of Central American Online Casino 1 at an earlier date and stolen its confidential customer information, the hackers extorted payments totaling approximately $2.3 million in cryptocurrency from Central American Online Casino 1.

Overt Act No. 17: On November 2, 2017, having gained unauthorized access to the computer network of Central American Online Casino 2 at an earlier date and stolen its confidential customer information, the hackers extorted payments totaling approximately $361,500 in cryptocurrency from Central American Online Casino 2.

Malicious Cryptocurrency Applications

Overt Act No. 18: Beginning in March 2018, defendant JON CHANG HYOK and other hackers sent electronic communications, including spear-phishing messages, to numerous employees of cryptocurrency exchanges.

Overt Act No. 19: Beginning on or before May 15, 2018, defendant JON CHANG HYOK and other hackers developed Celas Trade Pro, which was purportedly cryptocurrency trading software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 20: Beginning on June 18, 2018, defendant JON CHANG HYOK and other hackers sent electronic communications advertising Celas Trade Pro to numerous employees of cryptocurrency exchanges.

Overt Act No. 21: Beginning on or before October 11, 2018, defendant JON CHANG HYOK and other hackers developed WorldBit-Bot, which was purportedly cryptocurrency trading software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 22: Beginning on November 14, 2018, defendant JON CHANG HYOK and other hackers sent electronic communications advertising WorldBit-Bot to employees of cryptocurrency exchanges.

Overt Act No. 23: Beginning on or before March 6, 2019, the hackers developed iCryptoFx, which was purportedly a "Cryptocurrency Algo-Trading Tool," but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 24: Beginning on April 27, 2019, defendant KIM IL or another hacker created online accounts using false and fraudulent personas for purported employees of iCryptoFx, which were designed to make iCryptoFx appear to be a legitimate cryptocurrency program.

Overt Act No. 25: Beginning on or before June 4, 2019, defendant JON CHANG HYOK and other hackers developed Union Crypto Trader, which was purportedly a cryptocurrency trading software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 26: On dates in April 2019 through July 2019, defendant JON CHANG HYOK and other hackers created online accounts using false and fraudulent personas for purported employees of Union Crypto Trader, which were designed to make Union Crypto Trader appear to be legitimate.

Overt Act No. 27: Beginning on or before February 21, 2020, defendant JON CHANG HYOK and other hackers developed Kupay Wallet,

which was purportedly cryptocurrency wallet software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 28: Beginning on or before February 28, 2020, defendant JON CHANG HYOK and other hackers developed CoinGo Trade, which was purportedly cryptocurrency trading software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 29: In early March 2020, defendant JON CHANG HYOK or another hacker sent electronic communications advertising and encouraging the download of Kupay Wallet.

Overt Act No. 30: In late March 2020, defendant JON CHANG HYOK or another hacker sent electronic communications advertising and encouraging the download of CoinGo Trade.

Overt Act No. 31: Beginning on or before March 30, 2020, defendant JON CHANG HYOK and other hackers developed Dorusio, which was purportedly cryptocurrency wallet software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 32: On March 30, 2020, defendant JON CHANG HYOK or another hacker sent electronic communications advertising and encouraging the download of Dorusio.

Overt Act No. 33: Beginning on or before May 6, 2020, defendant JON CHANG HYOK and other hackers developed CryptoNeuro Trader, which was purportedly cryptocurrency trading software, but which was, in reality, a malicious cryptocurrency application.

Overt Act No. 34: In late July 2020, defendant JON CHANG HYOK or another hacker sent electronic communications advertising and encouraging the download of CryptoNeuro Trader.

Overt Act No. 35: Beginning on or before September 1, 2020, a conspirator or conspirators developed Ants2Whale, which was

purportedly cryptocurrency trading software, but which was, in reality, a malicious cryptocurrency application.

Cryptocurrency Heists

Overt Act No. 36: On December 4, 2017, a conspirator sent a spear-phishing communication to an employee of the Slovenian Cryptocurrency Company, which included a hyperlink that redirected the employee to download a file containing malware.

Overt Act No. 37: On December 15, 2017, having gained unauthorized access to the computer network of the Slovenian Cryptocurrency Company at an earlier date, the hackers fraudulently transferred cryptocurrency, valued at approximately $75 million, from the wallets of the Slovenian Cryptocurrency Company.

Overt Act No. 38: In March 2018 and April 2018, a conspirator sent spear-phishing communications to employees of the Indonesian Cryptocurrency Company.

Overt Act No. 39: On September 27, 2018, having gained unauthorized access to the computer network of the Indonesian Cryptocurrency Company at an earlier date, the hackers fraudulently transferred cryptocurrency, valued at approximately $24.9 million, from the wallets of the Indonesian Cryptocurrency Company.

Overt Act No. 40: On August 7, 2020, having gained unauthorized access to the computer network of the New York Financial Services Company at an earlier date by using the CryptoNeuro Trader malicious cryptocurrency application, and using that unauthorized access to steal data that they would later use to attempt to extort the New York Financial Services Company, the hackers fraudulently transferred cryptocurrency, valued at approximately $11.8 million, from the wallets of the New York Financial Services Company.

ATM Cash-Outs

Overt Act No. 41: On October 27, 2018, having gained unauthorized access to the computer network of BankIslami, the hackers caused fraudulent ATM withdrawal requests to be approved, which caused requesting ATMs to dispense approximately $6.1 million to money-launderer coconspirators, including coconspirators acting at the direction of unindicted coconspirator Ghaleb Alaumary.

Additional Spear-Phishing Campaigns

Overt Act No. 42: Beginning in March 2016 and continuing through August 2016, conspirators sent numerous spear-phishing communications to employees of United States cleared defense contractors, energy companies, and aerospace companies.

Overt Act No. 43: Beginning in February 2017 and continuing through May 2017, conspirators sent numerous spear-phishing communications to United States cleared defense contractors.

Overt Act No. 44: In November 2019, conspirators sent spear-phishing communications to the employees of the United States Department of State.

Overt Act No. 45: In January and February 2020, conspirators sent numerous spear-phishing communications to employees of the United States Department of State, the United States Department of Defense, and multiple United States technology companies.

COUNT TWO

[18 U.S.C. § 1349]

40. The Grand Jury re-alleges and incorporates paragraphs 1 through 35 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECTS OF THE CONSPIRACY

41. Beginning on a date unknown to the Grand Jury, but no later than September 28, 2009, and continuing through at least December 8, 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendants JON CHANG HYOK, KIM IL, and PARK JIN HYOK, together with others known and unknown to the Grand Jury, knowingly conspired to commit the following offenses:

a. wire fraud, in violation of Title 18, United States Code, Section 1343; and

b. bank fraud, in violation of Title 18, United States Code, Section 1344(2).

B. THE MANNER AND MEANS OF THE CONSPIRACY

42. The objects of the conspiracy were to be accomplished, in substance, as follows:

a. The Grand Jury re-alleges and incorporates paragraphs 38.a through 38.dd of Section B of Count One of this Indictment.

Marine Chain

b. Defendant KIM IL and other conspirators would develop a plan to create a digital token called “Marine Chain Token,” which would allow investors to purchase fractional ownership interests in marine shipping vessels, such as cargo ships, supported by a blockchain.

c. Defendant KIM IL would contact individuals in Singapore, whom defendant KIM IL knew from when he previously lived in Singapore, regarding potential involvement in creating Marine Chain.

d. Defendant KIM IL and other conspirators would, at other times, use false and fraudulent names when contacting individuals who they hoped would be involved in creating Marine Chain. In those instances, defendant KIM IL and other conspirators would not disclose to these individuals that the conspirators were DPRK citizens or that they were communicating using false and fraudulent names.

e. Defendant KIM IL and other conspirators would raise funds for the Marine Chain platform through an ICO, which would, in part, entail communicating with potential investors using false and fraudulent names in order to convince them to invest in the Marine Chain platform. Defendant KIM IL and other conspirators would not disclose to these individuals that the conspirators were DPRK citizens or that they were communicating using false and fraudulent names. They also would not disclose to investors that a purpose of the Marine Chain Token was to evade United States sanctions on North Korea.

f. Defendant KIM IL and other conspirators would attempt to receive approval from the Securities and Futures Commission of Hong Kong to trade the Marine Chain Token as a security.

g. Defendant KIM IL and other conspirators would tokenize individual vessels on the Marine Chain platform, allowing investors to purchase ownership interests in marine shipping vessels.

C. OVERT ACTS

43. In furtherance of the conspiracy, and to accomplish its objects, defendants JON CHANG HYOK, KIM IL, and PARK JIN HYOK, together with others known and unknown to the Grand Jury, on or about the dates set forth below, committed and caused to be committed various overt acts, in the Central District of California and elsewhere, including, but not limited to, the following:

Overt Act Nos. 1–45: The Grand Jury re-alleges and incorporates Overt Act Number 1 through Overt Act Number 45 of Section C of Count One of this Indictment here.

Overt Act No. 46: Beginning no later than October 31, 2017, defendant KIM IL and other conspirators communicated with each other regarding development of Marine Chain.

Overt Act No. 47: Beginning on November 28, 2017, while in Russia, defendant KIM IL communicated with individuals in Singapore about establishing Marine Chain.

Overt Act No. 48: On May 1, 2018, defendant KIM IL sent a final business plan for Marine Chain to a conspirator.

FORFEITURE ALLEGATION ONE

[18 U.S.C. §§ 982 and 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1030(i), in the event of any defendant's conviction of the offense set forth in Count One of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

a. All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

b. Any property used or intended to be used to commit the offense; and

c. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, 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 that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 982]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 982(a)(2), in the event of any defendant's conviction of the offense set forth in Count Two of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

a. All right, title and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense; and

b. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, 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 that cannot be divided without difficulty.

A TRUE BILL

/S/

Foreperson

TRACY L. WILKISON
Attorney for the United States,
Acting Under Authority Conferred
by 28 U.S.C. § 515

CHRISTOPHER D. GRIGG
Assistant United States Attorney
Chief, National Security Division

CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, Cyber and Intellectual
Property Crimes Section

ANIL J. ANTONY
Assistant United States Attorney
Deputy Chief, Cyber and
Intellectual Property Crimes
Section

KHALDOUN SHOBAKI
Assistant United States Attorney
Cyber and Intellectual Property
Crimes Section

EXHIBIT A

JON CHANG HYOK,

aka “Quan Jiang,”

aka “Alex Jiang”

EXHIBIT B

KIM IL,

aka “Julien Kim,”

aka “Tony Walker”

EXHIBIT C

PARK JIN HYOK,

aka “Jin Hyok Park,”

aka “Pak Jin Hek,”

aka “Pak Kwang Jin”