UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. (1) ZHENXING WANG, a/k/a "Danny Wang" (2) JING BIN HUANG, a/k/a "靖斌 黄" (3) BAOYU ZHOU, a/k/a "周宝玉" (4) TONG YUZE, a/k/a "佟雨泽" (5) YONGZHE XU, a/k/a "徐勇哲" a/k/a "يونجزهي أكسو" (6) ZIYOU YUAN, a/k/a "زيـو" (7) ZHENBANG ZHOU, a/k/a "周震邦" (8) MENGTING LIU, and a/k/a "劉 孟婷" (9) ENCHIA LIU, a/k/a "刘恩嘉" Defendants.	Criminal No. 25cr10273 NMG-MPK Violations: Count One: Conspiracy to Commit Wire and Mail Fraud (18 U.S.C. § 1349) Count Two: Money Laundering Conspiracy (18 U.S.C. § 1956(h)) Count Three: Conspiracy to Commit Identity Theft (18 U.S.C. §§ 1028(a)(7) and (f)) Count Four: Conspiracy to Damage a Protected Computer (18 U.S.C. § 371) Count Five: Conspiracy to Violate the International Emergency Economic Powers Act (50 U.S.C. §§ 1705(a) and (c)) Forfeiture Allegations: (18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c); 18 U.S.C. §§ 981(a)(1) and (a)(2)(B), 1028(b)(5), 1030(i); and 19 U.S.C. § 1595a(d))

INDICTMENT

At all times relevant to this Indictment:

Introduction and General Allegations

1. Since 2003, the government of the Democratic People's Republic of Korea ("DPRK" or "North Korea") has been under sanction by the United Nations ("UN") due to, among other things, its nuclear weapons program. Since 2016, the United States has likewise had

comprehensive trade and economic sanctions against North Korea due to the national security threats posed by North Korea, including its nuclear weapons program. The sanctions effectively cut North Korea off from the U.S. marketplace and financial system and restricted the ability of U.S. persons and companies from doing business with DPRK institutions. As a result, North Korea has sponsored a variety of schemes to evade the U.S. and U.N. sanctions and earn money for the regime.

2. One such scheme involves the use of highly skilled information technology ("IT") workers to obtain remote, pseudonymous employment with companies around the world, including the United States, using false or stolen identities. According to a May 2022 advisory by the U.S. Department of State, the U.S. Department of Treasury, and the Federal Bureau of Investigation ("FBI"), North Korea has dispatched thousands of IT workers around the world (hereinafter, "overseas IT workers"), earning revenue that contributes to the North Korean weapons programs, in violation of U.S. and U.N. sanctions. These workers: (i) misrepresent themselves as foreign (non-North Korean) or U.S.-based remote workers using falsified or stolen identification documents (including U.S. driver's licenses and passports); (ii) obfuscate their location using virtual private networks ("VPNs"), virtual private servers ("VPS"), third country internet protocol ("IP") addresses, and proxy accounts; (iii) surreptitiously obtain remote IT jobs with companies spanning a range of sectors and industries around the world; (iv) develop applications and software for their employers; (v) in some instances, use privileged access gained through such employment for other illicit purposes, including obtaining sensitive, proprietary information from an employer's computer network without authorization; and (vi) use U.S. financial institutions to launder wages paid by victim companies to overseas accounts controlled by DPRK actors and their

money laundering co-conspirators. While some of these IT workers operate from cities inside North Korea, many work in the Peoples Republic of China ("China") in cities near the North Korean border, including in Dandong and Shenyang.

3. According to the same May 2022 advisory, North Korean IT workers often work on multi-member teams. One such team identified during this investigation is pictured below:

4. In order to circumvent any controls that targeted U.S. and global companies have designed and implemented to prevent the hiring of illicit IT workers, and to otherwise prevent unauthorized access and damage to the companies' computer networks, the overseas IT workers obtain assistance from persons residing in the United States. Among other assistance provided to the IT workers, these U.S. facilitators receive and host at their residences in the U.S. laptop computers and other hardware devices issued by U.S. victim companies. Using login credentials provided to them by the overseas IT workers—and unbeknownst to and without authorization from

the U.S. victim companies—the U.S. facilitators then enable remote access to the laptops by the overseas IT workers either by downloading remote desktop software to the computers (that is, software that allows a computer to remotely run another computer's desktop environment using a standard internet connection), or by connecting the laptop to a hardware device designed to allow for remote access (often referred to as a keyboard, video, and mouse switch or "KVM" switch). The DPRK IT workers use such software and hardware to access U.S.-based computers so that it appears they are performing their work from locations in the U.S. The U.S. facilitators also establish accounts at U.S. banks and online money transfer services to facilitate the movement of money paid by U.S. victim companies to the overseas IT workers and other persons located abroad. In exchange for these and other services, many U.S. facilitators are paid a substantial fee. Most of the money generated by this scheme, however, is funneled to the overseas IT workers and their overseas co-conspirators.

5. From in and around 2021 until approximately October 2024, a group of overseas IT workers, along with co-conspirator facilitators located in New Jersey, New York, California, and overseas, perpetrated such a coordinated scheme to obtain remote work from U.S. companies. The scheme resulted in the transmission of false and misleading information to dozens of U.S. companies, U.S financial institutions, and U.S. government agencies, including the U.S. Department of Homeland Security ("DHS"), the Internal Revenue Service ("IRS"), and the Social Security Administration ("SSA"). Specifically, this group of overseas IT workers and their co-conspirators compromised the identities of more than 80 U.S. persons; applied for and obtained remote jobs at more than 100 U.S. companies, including many Fortune 500 companies; caused false and fraudulent employment verification information to be sent to DHS, IRS, and SSA on

dozens of occasions; received laptops and other hardware from U.S. companies; accessed, without authorization, the internal systems of the U.S. companies using remote desktop software or other means; gained access to sensitive employer data and source code; and generated at least $5 million in revenue for the overseas IT workers, and caused U.S. victim companies to incur legal fees, computer network remediation costs, and other damages and losses of at least $3 million.

6. The overseas IT workers were assisted in this scheme by Kejia WANG, Zhenxing WANG, and at least four other identified U.S. facilitators. Among other things, Kejia WANG, Zhenxing WANG, and the other U.S. facilitators received and/or hosted laptops belonging to U.S. victim companies at their residences to deceive the U.S. companies into believing the IT workers were located in the United States; facilitated remote access to the computers by the overseas IT workers by, among other things, downloading software to the computers without authorization from the U.S. companies or connecting the U.S. companies' computers to internet-connected KVM switches; created shell companies with corresponding websites and financial accounts, including Hopana Tech LLC ("Hopana Tech"), Tony WKJ LLC ("Tony WKJ"), and Independent Lab LLC ("Independent Lab"), to make it appear as though the overseas IT workers were affiliated with legitimate U.S. businesses; and established accounts at U.S. financial institutions and online money transfer services to receive money from victimized U.S. companies, much of which was subsequently transferred to overseas co-conspirators. In exchange for their services, Kejia WANG, Zhenxing WANG, and the other U.S. facilitators collected at least $696,000 in fees.

7. Kejia WANG and Zhenxing WANG acted knowing that the overseas IT workers were, in fact, not located in the United States, that the overseas IT workers used false or stolen identities to gain employment as IT workers, and that the overseas IT workers were defrauding the

U.S. companies. Kejia WANG further acted knowing that the overseas IT workers were working on behalf of North Korea.

8. The conspiracy perpetrated a massive fraud that impacted U.S. companies in multiple industries across much of the United States, including Massachusetts, California, New York, New Jersey, Florida, New Mexico, Georgia, Maryland, Alabama, North Carolina, Illinois, Ohio, South Carolina, Michigan, Texas, Indiana, Arkansas, Missouri, Tennessee, Minnesota, Rhode Island, Wisconsin, Oregon, Pennsylvania, Washington, Utah, Colorado, and the District of Columbia. The victim companies also included a California-based defense contractor, from which an overseas actor stole sensitive documents and computer files, many of which related to sensitive U.S. military technology controlled under the International Traffic in Arms Regulations or "ITAR."

The International Emergency Economic Powers Act

9. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C § 1701 *et seq*., authorizes the President of the United States to impose trade and economic sanctions in response to an unusual and extraordinary threat to the national security, foreign policy, or economy of the United States. Pursuant to that authority, the President may declare a national emergency through Executive Orders that have the full force and effect of law. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to the statute. 50 U.S.C. § 1705.

10. Pursuant to IEEPA, the President and the Executive Branch have issued Executive Orders and regulations governing and prohibiting certain transactions involving North Korea. Specifically, on June 26, 2008, the President issued Executive Order 13466, finding that that "the

existence and risk of the proliferation of weapons-usable fissile material on the Korean Peninsula constituted an unusual and extraordinary threat to the national security and foreign policy of the United States" and declaring a "national emergency to deal with that threat." The President has imposed additional sanctions with respect to North Korea. *See* Executive Orders 13551 (Aug. 30, 2010), 13570 (Apr. 18, 2011), 13722 (Mar. 15, 2016), and 13810 (Sept. 20, 2017). To implement these Executive Orders, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued the North Korea Sanctions Regulations (the "NKSR") in 2010 and they have been amended several times since. 31 C.F.R. Part 510.

11. On March 15, 2016, the President, took additional steps with respect to the national emergency described in Executive Order 13466, and issued Executive Order 13722 to address the Government of North Korea's continuing pursuit of its nuclear and missile programs. Among other things, Executive Order 13722 imposed a comprehensive blocking of the property and interests in property of the Government of North Korea and the Workers' Party of Korea. As a result, U.S. persons, including U.S. financial institutions and companies, are generally prohibited from transacting with North Korea.

12. On March 5, 2018, OFAC amended and reissued the NKSR in their entirety to implement Executive Order 13722, among others. 83 Fed. Reg. 9182 (Mar. 5, 2018). Absent a license from OFAC, the NKSR prohibits, among other things, the exportation or re-exportation, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods, services, or technology to North Korea. 31 C.F.R. § 510.206(a); *see also* Executive Order 13722 § 3. This prohibition applies to services, including financial services, performed on behalf of a person in North Korea or the Government of North Korea or where the benefit of such services is

otherwise received in North Korea. 31 C.F.R. § 510.405. Additionally, the benefit of services performed anywhere in the world on behalf of the North Korean government is presumed to be received in North Korea. *Id.* The NKSR also prohibited any transaction that evaded or avoided, had the purpose of evading or avoiding, caused a violation of, attempted to violate, or any conspiracy formed to violate any of the prohibitions set forth in the NKSR. 31 C.F.R. § 510.212; *see also* Executive Order 13722 § 7.

The Co-Conspirators

13. Kejia WANG, a/k/a "Tony," was a United States citizen residing in New Jersey. Kejia WANG founded two New Jersey-based limited liability companies, Hopana Tech and Tony WKJ, that purported to specialize in software development. In fact, Kejia WANG and his co-conspirators used Hopana Tech and Tony WKJ to facilitate the criminal schemes described in this Indictment. Among other things, Kejia WANG communicated with overseas IT workers and other overseas co-conspirators about the scheme via text-based communication platforms and email; traveled to Shenyang and Dandong, cities near the North Korean border, to meet with overseas co-conspirators about the scheme, including defendants Jing Bin HUANG, Tong YUZE, and Baoyu ZHOU; received laptops belonging to U.S. victim companies at his residence addressed to persons whose identities had been stolen or fabricated; caused the laptops to be sent to the residences of other U.S. facilitators, including Zhenxing WANG and at least four other U.S. facilitators, where they were remotely accessed by overseas IT workers; and received money from U.S. victim companies into bank and other financial accounts that he established and controlled, a significant portion of which he subsequently transferred to accounts owned and controlled by overseas co-conspirators.

14. Defendant Zhenxing WANG, a/k/a "Danny," was a United States citizen residing in New Jersey. Zhenxing WANG founded a New Jersey based limited liability company, Independent Lab, that purported to specialize in software development. In fact, Zhenxing WANG and his co-conspirators used Independent Lab to facilitate the criminal schemes described is this Indictment. Among other things, Zhenxing WANG received laptops belonging to U.S. victim companies addressed to persons whose identities had been stolen or fabricated; hosted the laptops at his residence; accessed, without authorization, U.S. victim companies' laptops; facilitated remote access to the laptops by overseas IT workers by installing remote access software without authorization; and received money from U.S. victim companies into bank and other financial accounts that he established and controlled, a significant portion of which he subsequently transferred to accounts owned and controlled by overseas co-conspirators.

15. Defendant Jing Bin HUANG was a Chinese citizen residing in Dandong, China, a city on the border with North Korea. Among other things, HUANG registered accounts with money transfer services ("MTS") and foreign banks that were used to receive and transfer proceeds generated through the conspiracy, including from Kejia WANG and Zhenxing WANG. In 2023, HUANG twice met in person with Kejia WANG and other co-conspirators in Shenyang, China.

16. Defendant Baoyu ZHOU was a Chinese citizen residing in China. Among other things, ZHOU registered MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Kejia WANG and Zhenxing WANG. In 2023, ZHOU met in person with Kejia WANG and other co-conspirators in Shenyang, China.

17. Defendant Tong YUZE was a Chinese citizen residing in China. Among other things, YUZE registered MTS and foreign bank accounts that were used to receive and transfer

proceeds generated through the conspiracy, including from Kejia WANG and Zhenxing WANG. The Hopana Tech website identified YUZE as a China-based representative of the company. In 2023, YUZE met in person with Kejia WANG and other co-conspirators in Shenyang, China.

18. Defendant Yongzhe XU was a Chinese citizen, born in the Yanbian Korean Autonomous Prefecture located in China, residing in the United Arab Emirates ("UAE"). Among other things, XU registered MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Kejia WANG and Zhenxing WANG. The Hopana Tech website identified XU as a Dubai-based representative of the company.

19. Defendant Ziyou YUAN was a Chinese citizen residing in the UAE. Among other things, YUAN registered and paid for multiple online accounts and other infrastructure that were used in furtherance of the conspiracy, including the Hopana Tech, Tony WKJ, and Independent Lab web domains, and an account with an online background check service provider used to conduct searches concerning stolen U.S. person identities.

20. Defendant Zhenbang ZHOU was an individual residing outside the United States. Among other things, ZHOU registered MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Baoyu ZHOU. ZHOU also registered and paid for multiple online accounts and other infrastructure that were used in furtherance of the conspiracy, including a server used to host the Tony WKJ, Tony Wang Tech, and Independent Lab web domains.

21. Defendants Mengting LIU and Enchia LIU were individuals residing in Taiwan. Among other things, Mengting LIU and Enchia LIU registered MTS and foreign bank accounts

that were used to receive and transfer proceeds generated through the conspiracy, including from Kejia WANG and U.S. Companies A and D.

22. Individual A was a resident of New York who, in exchange for a fee, received and hosted U.S. victim company laptops at Individual A's residence and facilitated remote access to the laptops by overseas IT workers.

23. Individual B was a resident of California who, in exchange for a fee, received and hosted U.S. victim company laptops at Individual B's residence and facilitated remote access to those computers by overseas IT workers. In 2024, Individual B recruited Individuals C and D, both California residents, to join the scheme by hosting laptops belonging to U.S. victim companies at their respective residences.

24. Individual C was a California resident, an active-duty member of the United States military, and a Secret clearance holder who, in exchange for a fee, hosted U.S. victim company laptops at Individual C's residence and facilitated remote access to the laptops by overseas IT workers.

25. Individual D was a resident of California and sibling of Individual B who, in exchange for a fee, hosted U.S. victim company laptops at Individual D's residence and facilitated access to the laptops by overseas IT workers.

26. Individual E was a Chinese national who, among other things, managed an information technology company based in North Korea, directed Kejia WANG to create a U.S. company through which Individual E's employees could obtain remote IT work with other U.S. companies, and directed Kejia WANG to establish corresponding financial accounts to receive

payments from the U.S. companies on behalf of his IT workers. Twice in 2023, Individual E met with Kejia WANG and other co-conspirators in Shenyang and Dandong, China.

COUNT ONE
Conspiracy to Commit Wire Fraud and Mail Fraud
(18 U.S.C. § 1349)

The Grand Jury charges:

27. The Grand Jury re-alleges and incorporates by reference paragraphs 1-26 of the Indictment.

28. From in or around 2021, the exact date being unknown to the Grand Jury, and continuing until in or around October 2024, in the District of Massachusetts and elsewhere, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE,
(5) YONGZHE XU,
(6) ZIYOU YUAN, and
(7) ZHENBANG ZHOU

conspired with each other and with others known and unknown to the Grand Jury to commit the following offenses:

a. wire fraud, that is, having devised and intending to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures and sounds, for the purpose of executing the scheme to defraud, in violation of Title 18, United States Code, Section 1343; and

b. mail fraud, that is, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did, for the purpose of executing and attempting to execute the scheme, knowingly cause to be delivered by mail and by any private and commercial interstate carrier according to the direction thereon, in violation of Title 18, United States Code, Section 1341.

Objects and Purposes of the Conspiracy

29. The objects of the conspiracy were to commit mail fraud and wire fraud. The purposes of the conspiracy were, among other things, to obtain employment for the overseas IT workers with U.S. companies using false and stolen identities in violation of U.S. laws, and to generate revenue for North Korea, the overseas IT workers, and their U.S. facilitators.

Manner and Means of the Conspiracy to Defraud

30. Among the manner and means by which the defendants and co-conspirators known and unknown to the Grand Jury carried out the conspiracy and the scheme to defraud were the following:

a. Stealing, or otherwise obtaining previously stolen, identities of U.S. persons;

b. Creating, or otherwise obtaining, fake U.S. identity documents;

c. Validating the stolen U.S. person identities using online background check services and public records searches;

d. Identifying remote IT jobs of interest at U.S. companies, including cleared

defense contractors, and developing fictitious personas, resumes, and online profiles to match the requirements of those IT jobs;

e. Creating forged identity documents, including U.S. passports, Social Security cards, and driver's licenses, containing the pictures of the overseas IT workers paired with the names and other personal identifying information of U.S. persons whose identities were stolen;

f. Establishing shell companies and corresponding web domains to create the false appearance that the overseas IT workers were affiliated with legitimate U.S. software development firms and were authorized to work in the U.S.;

g. Applying for remote IT jobs at U.S. companies using forged identity documents and other false and misleading information, including false information about their eligibility to work in the United States;

h. Directing the U.S. companies to send their company-issued laptops to the U.S. residences of Kejia WANG, Zhenxing WANG, and other U.S. facilitators;

i. Hosting the company-issued laptops at the U.S. facilitators' residences and logging into the U.S. companies' networks using credentials provided by the IT workers that the IT workers obtained from U.S. companies through fraud and deceit;

j. Coordinating activities domestically with and through Kejia WANG, who in turn managed several U.S.-based facilitators, including Zhenxing WANG and Individuals A, B, C, and D, by tracking the number of laptops the

facilitators received, which companies those laptops belonged to, and the amount of money each facilitator generated;

k. Enabling the overseas IT workers to connect remotely to the laptops being hosted in the United States through the use of remote desktop software and KVM devices;

l. Conducting remote IT work on behalf of the U.S. companies;

m. Directing the U.S. companies to deposit payroll and wages issued in the names of stolen or fake U.S. person identities into accounts at U.S. banks, MTSs, and online payment platforms opened and controlled by the defendants and other co-conspirators; and

n. Transferring money between and among U.S. bank accounts, MTSs, and online payment platforms, much of which was further transferred to other co-conspirators abroad, including co-conspirators who claimed to be living in Dandong, China, a city along the North Korean border, and Shenyang, China.

Acts in Furtherance of the Conspiracy and the Scheme to Defraud

31. In furtherance of the conspiracy and scheme to defraud, and to accomplish its goals, the following acts, among others, were committed in the District of Massachusetts and elsewhere:

Identifying and Targeting U.S. Identity Theft Victims

a. On or about May 11, 2021, Ziyou YUAN registered an account with a U.S.-based online background check service provider ("OBCS-1"). The purpose of this account was to search for and verify the personal identifying

information—names, addresses, dates of birth, social security numbers, etc.—of U.S. persons whose identities the overseas IT workers intended to use to apply for remote IT positions at U.S. companies.

b. Between on or about May 11, 2021, and on or about May 13, 2022, a U.S. money transfer service ("MTS-1") account registered to YUAN was used to pay the fees associated with YUAN's OBCS-1 account.

c. Between on or about September 29, 2021, and on or about September 5, 2023, co-conspirators used YUAN's OBCS-1 account to conduct public records searches concerning, and to verify the personal information of, more than 700 U.S. persons, including the following 39 stolen U.S. person identities used in furtherance of the conspiracy and scheme to defraud:

Sub ¶	U.S. Identity
1	Alexis C.
2	Andrew M.
3	Bradley N.
4	Charles B.
5	Charles R.
6	Damian T.
7	Daniel A.
8	Dennis L.
9	Deven C.
10	Don C.
11	Donald R.
12	Eric J.
13	Eric P.
14	Erin H.
15	Gary F.
16	Gerardo A.
17	Hanjay W.
18	Jacob B.
19	James B.
20	James E.
21	Jason R.
22	Jeffrey W.
23	Jeremy A.
24	Jeremy J.

Sub ¶	U.S. Identity
25	Jie L.
26	Kevin W.
27	Lan Duc N.
28	Marcus C.
29	Matthew M.
30	Michael A.
31	Michael C.
32	Nate L.
33	Robert L.
34	Steven F.
35	Steven L.
36	Steven R.
37	Thomas H.
38	Wandee C.
39	William R.

d. Between in or around February 2023 and in or around December 2023, co-conspirators used a second online background check service ("OBCS-2") to search for and verify the personal identifying information of U.S. persons whose identities the overseas IT workers intended to use to apply for remote IT positions at U.S. companies.

e. Between approximately February 2023 and December 2023, a MTS-1 account registered to Zhenbang ZHOU and credit cards associated with Kejia WANG and Ziyou YUAN were used to pay various fees associated with the OBCS-2 account.

The Fraudulent Use of Front Companies

f. On or about November 27, 2020, Yongzhe XU created an account with a U.S.-based domain registrar ("Domain Registrar 1"). That same day, using his Domain Registrar 1 account, XU registered and paid for the Hopana Tech website domain (www.hopanatech.com) using his account at MTS-1.

g. In 2021, on a date unknown to the Grand Jury, Individual E instructed Kejia WANG to create a U.S. company through which his employees could obtain remote IT work with other U.S. companies, and directed Kejia WANG to establish corresponding financial accounts to receive payments from the U.S. companies on behalf of his IT workers.

h. On or about January 11, 2021, consistent with instructions he received from Individual E, Kejia WANG registered Hopana Tech LLC, a company purporting to specialize in IT and software development, with the New Jersey Secretary of State, listing his home address in New Jersey as the company's principal place of business.

i. On or about May 27, 2021, Zhenxing WANG registered Independent Lab LLC, a company purporting to specialize in IT and software development, with the New Jersey Secretary of State, listing his residence in New Jersey as the company's principal place of business.

j. On or about February 18, 2022, Kejia WANG registered Tony WKJ LLC, a company purporting to specialize in IT and software development, with the New Jersey Secretary of State, listing his home address in New Jersey as the company's principal place of business.

k. On or about May 8, 2022, Yongzhe XU's Domain Registrar 1 account was used to register the website domains for Independent Lab (www.inditechlab.com) and Tony WKJ (www.wkjllc.com). The fees

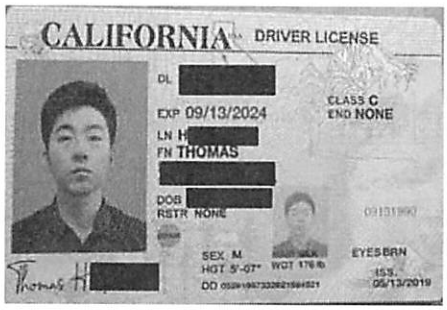
associated with these domain registrations and subsequent renewals were paid using YUAN's MTS-1 account.

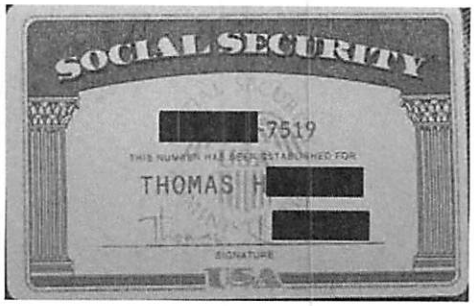
l. On or about May 8, 2022, using an account registered in his name with a U.S.-based VPS provider, Zhenbang ZHOU registered a VPS used to host the website domains for Independent Lab (www.inditechlab.com) and Tony WKJ (www.wkjllc.com).

m. On or about November 1, 2023, a Domain Registrar 1 account registered to Kejia WANG and Kejia WANG's credit card were used to register and pay for the website domain for a company called Shenyang Tonywang Technology LTD (www.tonywangtech.com), a "top Software consulting company [that] develops bespoke solutions."

Fraudulent Employment with U.S. Company A

n. In or around December 2022, an overseas co-conspirator using the stolen identity of "Thomas H.," a United States citizen, applied for a remote IT position at Company A, a California-based software development firm. The overseas co-conspirator posing as Thomas H. falsely told Company A that he was a United States citizen residing in California, and provided Company A with a copy of the following fake California driver's license and U.S. Social Security card containing Thomas H.'s personal identifying information:





o. On or about January 17, 2023, the overseas co-conspirator posing as Thomas H. obtained full-time, remote employment at Company A as a software engineer.

p. In or around January 2023, the overseas co-conspirator posing as Thomas H. completed, signed, and transmitted to Company A an I-9 Eligibility Verification Form, in which he falsely affirmed, under penalty of perjury, that he was a resident of California and a citizen of the United States.

q. To receive direct deposits of salary and wages from Company A, via email dated in or around January 2023, the overseas co-conspirator posing as Thomas H. provided Company A with financial account information associated with a U.S. Bank that, unbeknownst to Company A, was linked to an online MTS (hereinafter, "MTS-2") account registered by defendant Mengting LIU.

r. After gaining employment with Company A, the overseas co-conspirator posing as Thomas H. instructed Company A to send his company-issued laptop to Kejia WANG's residence in New Jersey, which the overseas co-conspirator falsely claimed was Thomas H.'s address. Kejia WANG

subsequently caused the Company A computer to be transferred to Zhenxing WANG.

s. Between in or around January 2023 and on or about June 6, 2023, the exact date being unknown to the Grand Jury, Zhenxing WANG, while hosting the Company A laptop at his residence, logged into the Company A laptop using credentials provided to him by Tony WANG and installed remote desktop software without authorization from Company A.

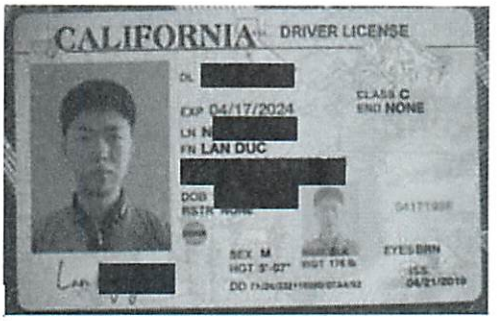
t. Between on or about January 21, 2023, and on or about May 6, 2024, the defendants and other co-conspirators caused Company A to deposit wages associated with employee Thomas H. totaling approximately $198,849.73 into an online MTS account registered by Mengting LIU.

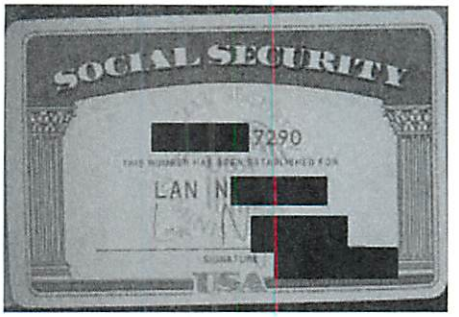
u. As a result of their fraudulent conduct, the defendants caused Company A to pay approximately $282,297.55 in network and device remediation expenses, legal fees, and other losses.

Fraudulent Employment with U.S. Company B

v. In or around January 2023, an overseas co-conspirator using the stolen identity of "Lan Duc N.," a United States citizen, applied for a remote IT position at Company B, a Massachusetts-based semiconductor distributor. The overseas co-conspirator posing as Lan Duc N., who also claimed to go by the name "Jason," falsely told Company B that he was a United States citizen residing in California, and provided Company B with a copy of the

following fake California driver's license and U.S. Social Security card containing Lan Duc N.'s personal identifying information:





w. In or around January 2023, the overseas co-conspirator posing as Lan Duc N. obtained full-time, remote employment at Company B as a software engineer.

x. In or around January 2023, the overseas co-conspirator posing as Lan Duc N. completed, signed, and transmitted to Company B an I-9 Eligibility Verification Form, in which he falsely affirmed, under penalty of perjury, that he was a resident of California and a citizen of the United States.

y. To receive direct deposits of salary and wages from Company B, the overseas co-conspirator posing as Lan Duc N. provided Company B with financial account information associated with a U.S. Bank that, unbeknownst to Company B, was linked to an MTS account registered by an unidentified co-conspirator.

z. After gaining employment with Company B, the overseas co-conspirator posing as Lan Duc N. instructed Company B to send his company-issued laptop to Kejia WANG's residence in New Jersey, which the co-conspirator

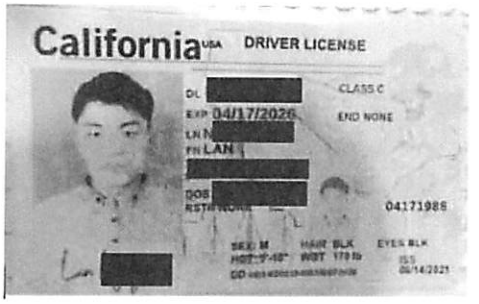
falsely claimed was Lan Duc N.'s residence. Kejia WANG subsequently caused the Company B computer to be transferred to Zhenxing WANG.

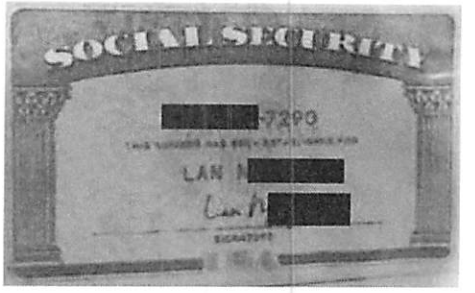
aa. Between on or about January 25, 2023, and on or about November 23, 2023, the exact date being unknown to the Grand Jury, Zhenxing WANG, while hosting the Company B laptop at his residence, logged into the Company B laptop and installed remote desktop software without authorization from Company B.

bb. Between on or about January 30, 2023, and on or about November 23, 2023, the defendants and other co-conspirators caused Company B to deposit wages associated with employee "Lan Duc N." totaling approximately $117,643.37 into an online MTS account registered by an unidentified co-conspirator.

Fraudulent Employment with U.S. Company C

cc. On or about December 7, 2023, an overseas co-conspirator IT worker using the stolen identity of "Lan Duc. N.," a United States citizen, applied for a remote IT position at Company C, a California-based defense contractor that develops artificial intelligence-powered equipment and technologies. The overseas co-conspirator, who also claimed to go by the name "Jason," falsely told Company C that he was a United States citizen residing in California, and provided Company C with a copy of the following fake California driver's license and United States Social Security Card containing Lan Duc N.'s personal identifying information:





dd. On or about January 9, 2024, the overseas co-conspirator posing as Lan Duc N. obtained full-time, remote employment at Company C as a software engineer.

ee. In or about January 2024, the overseas co-conspirator posing as Lan Duc N. completed, signed, and transmitted to Company C via email an I-9 Eligibility Verification Form in which he falsely affirmed, under penalty of perjury, that he was a resident of California and a citizen of the United States.

ff. In order to receive direct deposits of salary and wages from Company C, the overseas co-conspirator posing as Lan Duc N. provided Company C with financial account information associated with a U.S. Bank that was, unbeknownst to Company C, linked to an MTS account registered to unidentified overseas co-conspirator.

gg. After gaining employment with Company C, the overseas co-conspirator posing as Lan Duc N. instructed Company C to send a company-issued laptop to Kejia WANG's residence in New Jersey.

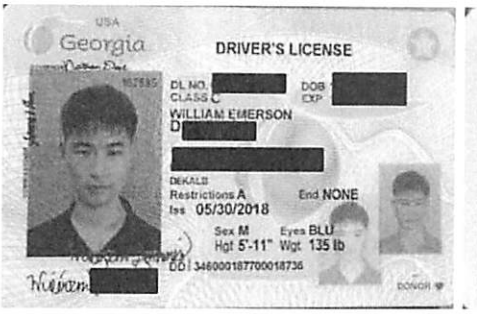
hh. On or about January 6, 2024, Kejia WANG received the Company C laptop and caused it to be transferred to Zhenxing WANG.

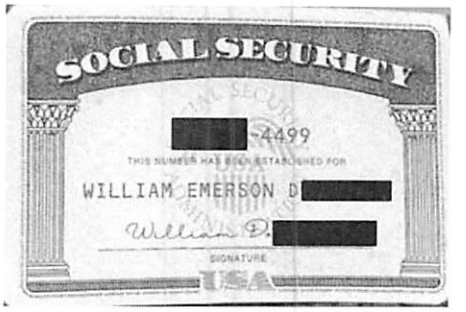
ii. On or about January 19, 2024, Zhenxing WANG logged into the Company C computer and installed two remote desktop applications, without authorization, from Company C.

jj. Between on or about January 19, 2024, and on or about April 2, 2024, an overseas co-conspirator remotely accessed the Company C computer without authorization and, during such remote access, downloaded computer files containing technical data and other information from Company C's servers, including information marked as being controlled under the ITAR.

kk. Between on or about January 9, 2024, and April 4, 2024, the defendants and other co-conspirators caused Company C to deposit wages associated with employee Lan Duc N. totaling approximately $33,757.10 into an overseas co-conspirator's MTS account.

ll. On or about December 7, 2023, an overseas co-conspirator using the stolen identity of "William D.," a United States citizen, applied for a remote IT position at Company C. The overseas co-conspirator falsely told Company C that he was a United States citizen residing in Georgia, and provided Company C with a copy of the following fake Georgia driver's license and U.S. Social Security card containing William D.'s personal identifying information:





mm. On or about January 25, 2024, the overseas co-conspirator posing as William D. obtained full-time, remote employment at Company C as a software engineer.

nn. In or around January 2024, the overseas co-conspirator posing as William D. completed, signed, and transmitted to Company C via email an I-9 Eligibility Verification Form in which he falsely affirmed, under penalty of perjury, that he was a resident of California and citizen of the United States.

oo. In order to receive direct deposits of salary and wages from Company C, the overseas co-conspirator posing as William D. provided Company C with financial account information associated with a U.S. Bank that was, unbeknownst to Company C, linked to an MTS account registered to Shenyang Pengzhou Trading Co. Ltd.

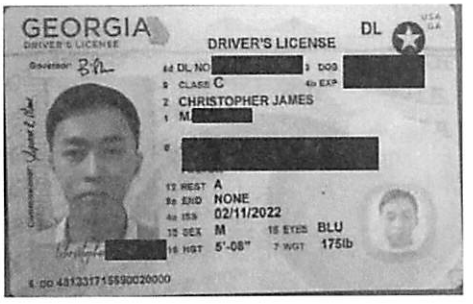
pp. The overseas co-conspirator instructed Company C to send a company-issued laptop to the address of Individual A in New York. Individual A received a package addressed to William D. containing the Company C laptop on or about January 22, 2024.

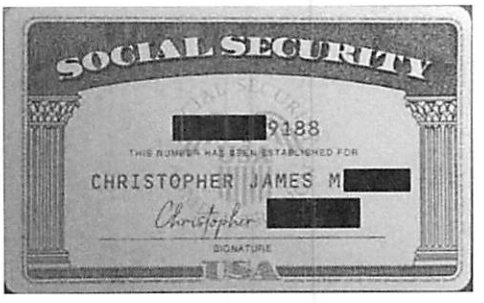
qq. Between on or about January 22, 2024, and on or about April 4, 2024, the exact date being unknown to the Grand Jury, Individual A logged into the

Company C laptop and installed two remote desktop applications, without authorization, from Company C.

rr. Between on or about January 25, 2024, and on or about April 4, 2024, the defendants and other co-conspirators caused Company C to deposit wages associated with employee "William D." totaling approximately $26,277.55 into the Shenyang Pengzhou Trading Co. Ltd. MTS account.

ss. On or about January 21, 2024, an overseas co-conspirator using the stolen identity of "Christopher M.," a United States citizen, applied for a remote IT position at Company C. The overseas co-conspirator told Company C that he was a United States citizen residing in Georgia, and provided Company C with a copy of the following fake California driver's license and U.S. Social Security card containing Christopher M.'s personal identifying information:





tt. On or about February 21, 2024, the overseas co-conspirator posing as Christopher M. obtained full-time, remote employment at Company C as a software engineer.

uu. In or around February 2024, the overseas co-conspirator posing as Christopher M. completed, signed, and transmitted to Company C via email

an I-9 Eligibility Verification Form in which he falsely affirmed, under penalty of perjury, that he was a resident of California and citizen of the United States.

vv. In order to receive direct deposits of salary and wages from Company C, the overseas IT worker posing as William D. provided Company C with financial account information associated with a U.S. Bank that was, unbeknownst to Company C, linked to an MTS account registered to an unidentified overseas co-conspirator.

ww. In or about February 2024, an overseas co-conspirator posing as Christopher M. instructed Company C to send a company-issued laptop to address of Individual B in California. On or about February 21, 2024, Individual B received a package addressed to Christopher M. containing a Company C laptop.

xx. Between on or about February 21, 2024, and on or about February 23, 2024, Kejia WANG provided Individual B, via text message, with login credentials for the Company C computer assigned to employee Christopher M., told Individual B to power on the computer, and instructed Individual B to send him screenshots of the powered-on device. Kejia WANG specifically instructed Individual B not to install remote access software at that time.

yy. On or about March 12, 2024, via text message, Kejia WANG instructed Individual B to connect the Company C laptop to a specific KVM device.

zz. On or about March 30, 2024, Individual B installed remote access software, without authorization, on the Company C laptop.

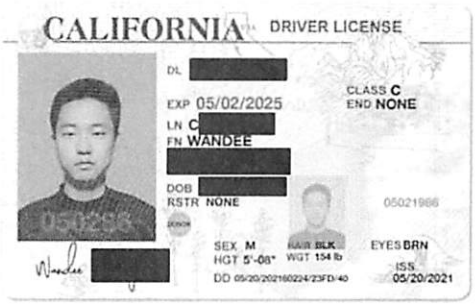
aaa. On or about April 4, 2024, the day after Company C fired "Christopher M.," Kejia WANG instructed Individual B to send the Company C laptop back to Company C.

bbb. Between on or about January 25, 2024, and on or about April 4, 2024, the defendants caused Company C to deposit wages associated with employee "Christopher M." totaling approximately $17,038.45 into an MTS account registered by an overseas co-conspirator.

ccc. As a result of their fraudulent conduct, the defendants caused Company C to pay approximately $106,200 in network and device remediation expenses, legal fees, and other losses.

Fraudulent Employment with U.S. Company D

ddd. On or about March 20, 2022, an overseas co-conspirator used the stolen identity of "Wandee C.," a United States citizen, to apply for a remote IT position at Company D, a Massachusetts-based online media company. The overseas co-conspirator falsely told Company D that he was a United States citizen residing in California, and provided Company D with a copy of the following fake California driver's license containing Wandee C.'s personal identifying information:



eee. On or about April 18, 2022, the overseas co-conspirator posing as Wandee C. obtained full-time, remote employment at Company D as a software engineer.

fff. In or around April 2022, the overseas co-conspirator posing as Wandee C. completed, signed, and transmitted to Company D an I-9 Eligibility Verification Form in which he falsely affirmed, under penalty of perjury, that he was a resident of California and citizen of the United States.

ggg. In order to receive direct deposits of salary and wages from Company D, the overseas IT worker posing as Wandee C. provided Company C with financial account information associated with a U.S. Bank that was, unbeknownst to Company C, linked to an MTS account registered by defendant Yongzhe XU on behalf of the company Al Naseeh Consultancy FZE.

hhh. On or about April 26, 2022, the overseas co-conspirator posing as Wandee C. instructed Company D to send a company-issued laptop to Kejia WANG's residence in New Jersey. Kejia WANG subsequently received the computer and caused it to be transferred to Zhenxing WANG.

iii. Between on or about April 26, 2022, and on or about September 14, 2022, the exact date being unknown to the Grand Jury, Zhenxing WANG logged into the Company D computer, without authorization, and facilitated unauthorized remote access by an overseas IT worker.

jjj. On or about September 21, 2022, approximately one week after Company D terminated employee Wandee C.'s employment, Tony WANG instructed Zhenxing WANG via text message to return the Company D laptop to Company D's offices in Massachusetts.

kkk. Between on or about April 18, 2022, and in or around September 2022, the defendants caused Company D to deposit wages associated with employee "Wandee C." totaling approximately $31,365.21 into defendant Yongzhe XU's MTS account.

lll. As a result of their fraudulent conduct, the defendants caused Company D to pay approximately $63,750 in network and device remediation expenses, legal fees, and other losses.

The Fraudulent Use of the U.S. Mail

mmm. Between on or about June 1, 2022, and on or about June 28, 2024, overseas co-conspirators caused hundreds of packages containing laptops and other items to be delivered via the U.S. mail and private postal carriers to Kejia WANG's residence in New Jersey, all in the names of false or stolen U.S. person identities, including but not limited to Wandee C., Kevin Z., Lucas H., and Jason N.

nnn. On or about the following dates, overseas co-conspirators caused packages containing laptops and other items to be delivered via the U.S. mail and private postal carriers in the names of stolen U.S. person identities to Zhenxing WANG's residence in New Jersey:

Sub ¶	Delivery Date	Victim Company (if known)	Recipient Identity
1.	2022-12-01	Company D	Bradley H.
2.	2023-09-01	Company E	Ryan C.
3.	2023-09-09	-	Ryan C.
4.	2022-12-01	Company D	Bradley H.

ooo. On or about the following dates, overseas co-conspirators caused packages containing laptops and other items to be delivered via the U.S. mail and private postal carriers in the names of stolen U.S. person identities to Individual B's residence in California.

Sub ¶	Delivery Date	Victim Company (if known)	Recipient Identity
1.	2023-04-06	U.S. Company F	Matthew M.
2.	2023-06-22	U.S. Company G	Steven F.
3.	2023-07-14	U.S. Company H	Damian T.
4.	2023-08-03	U.S. Company I	Steven R.
5.	2023-08-10	-	James B.
6.	2023-08-29	U.S. Company G	Steven F.
7.	2023-04-06	U.S. Company F	Matthew M.
8.	2023-06-22	U.S. Company G	Steven F.
9.	2023-07-14	U.S. Company H	Damian T.
10.	2023-08-03	U.S. Company I	Steven R.
11.	2023-08-10	-	James B.
12.	2023-08-29	U.S. Company G	Steven F.
13.	2024-02-21	U.S. Company C	Chis M.

ppp. On or about the following dates, overseas co-conspirators caused packages containing laptops and other items to be delivered via the U.S. mail and private postal carriers in the names of stolen U.S. person identities to Individual A's residence in New York.

Sub ¶	Delivery Date	Victim Company (if known)	Recipient Identity
1.	2023-12-01	-	Michael C.
2.	2023-12-04	U.S. Company J	Kevin W.
3.	2023-12-06	-	Michael C.
4.	2023-12-08	-	Michael C.
5.	2023-12-11	U.S. Company K	Matthew D.
6.	2023-12-17	U.S. Company L	William R.
7.	2024-01-02	U.S. Company M	Donald R.
8.	2024-01-13	U.S. Company N	Nathaniel G.
9.	2024-01-15	-	Nathaniel G.
10.	2024-01-22	U.S. Company C	William D.
11.	2024-01-25	-	Nathaniel G.
12.	2024-02-02	U.S. Company O	Robert L.
13.	2024-02-08	U.S. Company P	Don C.
14.	2024-03-08	U.S. Company Q	Jacob B.
15.	2024-03-08	U.S. Company R	Donald R.
16.	2024-03-21	U.S. Company C	Bill D.
17.	2024-03-22	-	William D.
18.	2024-03-29	U.S. Company S	Nathaniel G.
19.	2024-04-29	U.S. Company T	Nathaniel G.
20.	2024-05-06	U.S. Company U	Jacob B.
21.	2024-05-08	-	William D.

The Fraudulent Use of Bank and other Financial Accounts Related to Kejia WANG, Hopana Tech, and Tony WKJ

qqq. In furtherance of the conspiracy and scheme to defraud, the co-conspirators established bank and other financial accounts in their names, and the names of sham IT development firms and other corporate entities, including Hopana Tech, Tony WKJ, and Independent Lab, for the purpose of receiving salary and wage payments from U.S. victim companies and sharing those funds with their overseas co-conspirators.

rrr. On or about January 15, 2022, Kejia WANG registered a business checking account in the name of Hopana Tech at a U.S. bank (hereinafter, "U.S. Bank 1"). Between on or about January 20, 2022, and on or about April 26, 2024, multiple U.S. victim companies deposited approximately $464,532.56 into

the Hopana Tech account at U.S. Bank 1.

sss. On or about the dates indicated below, the following funds, totaling approximately $375,995.76, were transferred from the Hopana Tech account at U.S. Bank 1 to various accounts controlled by or associated with defendant Jing Bin HUANG, Baoyu ZHAO, Enchia LIU, and other overseas co-conspirators:

HOPANA TECH – U.S. BANK 1				
Sub ¶	**Sender**	**Recipient / Financial Institution**	**Amount**	**Date**
1	Hopana Tech	Shenyang Xiwang Technology LTD / Bank of China	$50,211.07	5/23/2022
2	Hopana Tech	Shenyang Ximang Tech LTD / Bank of China	$21,552.99	5/23/2022
3	Hopana Tech	Shenyang Xinxiwang Technology LTD / Bank of China	$25,636.83	8/31/2022
4	Hopana Tech	Shenyang Deep Technology LTD / Bank of China	$35,891.18	9/1/2022
5	Hopana Tech	Shenyang Di Di Technology LTD / Bank of China	$40,821.17	9/2/2022
6	Hopana Tech	Shenyang Wan Xiang Yu Technology / Bank of China	$20,456.77	10/31/2022
7	Hopana Tech	Shenyang Du Sang Technology LTD / Bank of China	$20,176.54	11/2/2022
8	Hopana Tech	JING BIN HUANG / Standard Chartered Bank Hong Kong	$50,000.00	12/4/2023
9	Hopana Tech	Shenyang Aolien Technology LTD / Bank of China	$25,525.92	12/23/2022
10	Hopana Tech	Shenyang Wan Xiang Yu Technology / Bank of China	$20,027.39	12/27/2022
11	Hopana Tech	Shenyang Wan Xiang Yu Technology Ltd / Bank of China	$25,695.90	3/17/2023
12	Hopana Tech	JING BIN HUANG / Standard Chartered Bank Hong Kong	$40,000.00	4/8/2024

ttt. On or about April 29, 2021, Kejia WANG registered an account at an MTS-2 in the name of Tony WKJ LLC. Between on or about May 24, 2021, and on or about August 2, 2023, multiple U.S. victim companies deposited

approximately $1,635,240.80 into the Tony WKJ account at MTS-2.

uuu. In or around the date ranges indicated below, the following funds were transferred from the Tony WKJ account at MTS-2 to bank accounts associated with defendant Enchia LIU and other overseas co-conspirators:

TONY WKJ – MONEY TRANSFER SERVICE 2					
Sub ¶	**Sender**	**Recipient / Financial Institution**	**Amount**	**No. of Transfers**	**Date Range**
1	Tony WKJ	Food Yard Trading FZ LLC / Dubai Islamic Bank	$201,087.22	19	7/13/2021 - 11/15/2021
2	Tony WKJ	Shenyang Sun-Lotus Tech LTD / Hua Xia Bank	$467,788.95	27	4/4/2022 - 1/5/2023
3	Tony WKJ	Shenyang Wan Xiang Yu Technology LTD / Bank of China	$214,970.68	12	1/17/2023 - 6/26/2023

vvv. Between on or about July 27, 2021, and on or about August 31, 2023, Kejia WANG transferred approximately $218,127.01 from the Tony WKJ account at MTS-2 to his personal checking account at U.S. Bank 2.

www. On or about April 25, 2021, Kejia WANG registered an account in his own name at MTS-2. Between on or about May 3, 2021, and on or about July 5, 2023, Kejia WANG transferred approximately $412,220.81 from the Tony WKJ account at MTS-2 to his personal account at MTS-2.

xxx. Between on or about February 16, 2022, and on or about July 21, 2023, multiple U.S. victim companies deposited approximately $237,654.62 into Kejia WANG's personal MTS-2 account. During this same time period, over the course of 43 separate transactions, Kejia WANG transferred approximately $208,127.00 from his personal MTS-2 account to accounts registered to and controlled by Jing Bin HUANG and Tong YUZE, among

other overseas co-conspirators.

yyy. Between on or about April 3, 2023, and on or about April 1, 2024, using his personal checking account at U.S. Bank 1, Kejia WANG sent 19 transfers totaling $36,456.50 to U.S. bank accounts controlled by Individual A. Most of these transfers contained notes that referenced "NY" and "laptops." For example, "NY November Laptops" and "NY December Laptops."

zzz. Between on or about April 28, 2023, and on or about March 29, 2024, using his personal checking account at U.S. Bank 1, Kejia WANG sent 22 transfers totaling $18,714.83 to a U.S. bank account controlled by Individual B, who was living in California. Most of these transfers contained notes that referenced the month the transfer took place and "CA laptops."

aaaa. On or about May 5, 2022, Kejia WANG registered a business checking account in the name of Tony WKJ at a U.S. financial technology services company and MTS (hereinafter "MTS-3"). In application documents, Kejia WANG falsely described Tony WKJ as a "VC-backed startup" specializing in "custom software development."

bbbb. Between on or about September 14, 2023, and on or about August 20, 2024, multiple U.S. victim companies deposited approximately $352,949.24 into the Tony WKJ account at MTS-3.

cccc. On or about September 27, 2023, an employee of MTS-3 emailed Kejia WANG to inquire about a deposit into the Tony WKJ MTS-3 account from

a U.S. victim company ("U.S. Company E") in the name of "Wandee C." In response, Kejia WANG falsely told the MTS-3 employee that "Wandee C[] is a software engineer who was initially hired by TONY WKJ LLC. However, he was later outsourced to [U.S. Company E] under a C2C condition. As a result, [U.S. Company E] sent a payment for Wandee [C] to TONY WKJ LLC." In fact, Tony WKJ was a front company with no employees, and "Wandee C." was a stolen identity used by an overseas worker to obtain remote employment with U.S. Company E.

The Fraudulent Use of Bank and Other Financial Accounts Related to Zhenxing WANG and Independent Lab

dddd. On or about May 27, 2021, Zhenxing WANG registered an account at MTS-2 in the name of Independent Lab. Between on or about June 15, 2021, and on or about June 15, 2024, multiple U.S. victim companies deposited approximately $2,093,166.64 into the Independent Lab account at MTS-2.

eeee. In or around the date ranges indicated below, the following funds were transferred from the Independent Lab account at MTS-2 to bank and money transfer service accounts registered to and controlled by defendants Jing Bin HUANG, Tong YUZE, Yongzhe XU, and other overseas co-conspirators:

INDEPENDENT LAB – MONEY TRANSFER SERVICE 2					
Sub ¶	**Sender**	**Recipient**	**Amount**	**No. of Transfers**	**Date Range**
1	Independent Lab	Zhenxing Wang - Wise	$260,981.34	37	7/9/2021 - 5/31/2024
2	Independent Lab	Xu yong zhe	$369,163.45	29	07/13/2021 - 4/6/2022

INDEPENDENT LAB – MONEY TRANSFER SERVICE 2					
Sub ¶	**Sender**	**Recipient**	**Amount**	**No. of Transfers**	**Date Range**
3	Independent Lab	Hopana-Tech Ltd.	$140,043.53	3	12/13/2021 - 12/27/2021
4	Independent Lab	Hi-Devs E-commerce LTD	$145,612.22	8	3/7/2022 - 8/16/2022
5	Independent Lab	Shenyang Ximang Tech LTD	$113,542.72	7	4/18/2022 - 7/5/2022
6	Independent Lab	Shenyang Labo Technology LTD	$28,022.43	1	6/6/2022
7	Independent Lab	Shenyang Di Ke Technology LTD	$504,597.80	27	09/16/2022 - 6/6/2023
8	Independent Lab	Shenyang Haidefushi Computer Network	$209,058.37	24	11/1/2023 - 7/9/2024
9	Independent Lab	Beijing Houpana Keji Youxiangongsi	$75,382.23	8	9/7/2023 – 10/13/2023

ffff. Between on or about May 2, 2022, and on or about June 28, 2024, Zhenxing WANG transferred approximately $17,009.15 from the Independent Lab account at Money Transfer Service 1 to his personal checking account at U.S. Bank 2.

gggg. On or about May 27, 2021, Zhenxing WANG registered an account in his own name at MTS-2.

hhhh. Between on or about July 9, 2021, and on or about July 15, 2024, multiple U.S. victim companies deposited approximately $140,550 into Zhenxing WANG's account at MTS-2. During this same period, Zhenxing WANG transferred approximately $140,168.60 of those funds to his personal checking account at U.S. Bank 2.

All in violation of Title 18, United States Code, Sections 1349 and 3238.

COUNT TWO
Money Laundering Conspiracy
(18 U.S.C. § 1956(h))

The Grand Jury further charges:

32. The Grand Jury re-alleges and incorporates by reference paragraphs 1-26 of this Indictment.

33. As described above, members of the conspiracy obtained payments from U.S. victim companies for IT work. Such payments were frequently made by Automated Clearing House ("ACH") transfers between banks and other financial services companies. After receiving the money, members of the conspiracy wired or otherwise transferred all or most of it to bank accounts in China or the UAE.

34. From in or about 2021, the exact date being unknown to the Grand Jury, through in or about October 2024, in the District of Massachusetts and elsewhere, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE,
(5) YONGZHE XU,
(6) ZIYOU YUAN,
(7) ZHENBANG ZHOU
(8) MENGTING LIU, and
(9) ENCHIA LIU,

conspired with each other and with others known and unknown to the Grand Jury to:

(a) conduct, cause others to conduct, and attempt to conduct financial transactions affecting interstate and foreign commerce, knowing that the property involved in such transactions represented the proceeds of some form of unlawful activity, and which in fact involved the proceeds of

specified unlawful activity, that is, conspiracy to commit wire and mail fraud in violation of Title 18, United States Code, Section 1349, as described in Count One, with the intent to promote the carrying on of the specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and

(b) conduct, cause others to conduct, and attempt to conduct financial transactions affecting interstate and foreign commerce, knowing that the property involved in such transaction represented the proceeds of some form of unlawful activity, and which in fact involved the proceeds of specified unlawful activity, that is, conspiracy to commit wire fraud and mail fraud in violation of Title 18, United States Code, Section 1349, as described in Count One, and knowing that the transactions were designed, in whole and in part, to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Sections 1956(h) and 3238.

COUNT THREE
Conspiracy to Commit Identity Theft
(18 U.S.C. §§ 1028(a)(7) and (f))

The Grand Jury further charges:

35. The Grand Jury re-alleges and incorporates by reference paragraphs 1-26 of this Indictment.

36. From in or about 2021, the exact date being unknown to the Grand Jury, through in or about October 2024, in the District of Massachusetts and elsewhere, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE,
(5) YONGZHE XU,
(6) ZIYOU YUAN, and
(7) ZHENBANG ZHOU,

did knowingly combine, conspire, and agree with each other and other persons known and unknown to the Grand Jury to transfer, possess, and use, without lawful authority, in and affecting interstate and foreign commerce, the means of identification of another person, to wit, the names, Social Security numbers, dates of birth, passport numbers, and state issued driver's license and identification numbers, with the intent to commit, and to aid and abet, and in connection with, any unlawful activity that constitutes a violation of Federal Law, to wit, conspiracy to commit wire fraud and mail fraud in violation of Title 18, United States Code, Section 1349, and conspiracy to commit money laundering in violation of Title 18, United States Code, Section 1956(h).

All in violation of Title 18, United States Code, Sections 1028(a)(7) and (f) and 3238.

COUNT FOUR
Conspiracy to Damage a Protected Computer
(18 U.S.C. § 371)

37. The Grand Jury re-alleged and incorporates by reference paragraphs 1-26 and 31 of this Indictment.

38. From in and about 2021, the exact date being unknown to the Grand Jury, through in or about October 2024, in the District of Massachusetts and elsewhere, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU, and
(4) TONG YUZE,

did knowingly and willfully combine, conspire, confederate, and agree with each other, and with others known and unknown to the Grand Jury, to commit and offense against the United States, that is to cause damage to protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 1030(c)(4)(A)(i)(I), having knowingly caused the unauthorized transmission of a program, information, code, and command to a protected computer, and as a result of such conduct, intentionally caused damage to a protected computer and computer system, resulting in loss to one or more persons during a one-year period, and resulting from a related course of conduct affecting one or more protected computers aggregating at least $5,000 in value.

39. The objects of the conspiracy were to gain unauthorized access and cause damage to protected U.S. company computers and computer networks. The purposes of the conspiracy were, among other things, to obtain employment for the overseas IT workers with U.S. companies using false and stolen identities in violation of U.S. laws, and to generate revenue for North Korea, the overseas IT workers, and their U.S. facilitators. The manner and means by which the

defendants and co-conspirators known and unknown to the Grand Jury carried out the conspiracy are described in paragraph 30 of this Indictment and are incorporated herein by reference.

All in violation of Title 18, United States Code, Sections 371 and 3238.

COUNT FIVE
Conspiracy to Violate the IEEPA
(50 U.S.C. §§ 1705(a) and (c))

The Grand Jury further charges:

40. The Grand Jury re-alleges and incorporates by reference paragraphs 1-26 of this Indictment.

41. From in or around 2021, the exact date being unknown to the Grand Jury, through in or around October 2024, in the District of Massachusetts and elsewhere, the defendants,

(1) JING BIN HUANG,
(2) BAOYU ZHOU,
(3) TONG YUZE, and
(4) YONGZHE XU,

did knowingly and willfully combine, conspire, confederate, and agree with each other, and with others known and unknown to the Grand Jury, to export and reexport, and cause U.S. persons and entities to export and reexport, goods and services, including banking and other financial services, to North Korea, without prior authorization and license from the U.S. Department of the Treasury, in violation of 50 U.S.C. § 1705(a) and (c).

All in violation of Title 18, United States Code, Section 3238, Title 50, United States Code, Sections 1705(a) and (c), Executive Order 13722, and Title 31, Code of Federal Regulations, Sections 510.206 and 510.212.

FORFEITURE ALLEGATIONS
(18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c); 18 U.S.C. §§ 981(a)(1) and (a)(2)(B), 1028(b)(5), 1030(i); and 19 U.S.C. § 1595a(d))

1. Upon conviction of the offense in violation of Title 18, United States Code, Section 1349, set forth in Count One, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE,
(5) YONGZHE XU,
(6) ZIYOU YUAN, and
(7) ZHENBANG ZHOU

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

2. Upon conviction of the offense in violation of Title 18, United States Code, Section 1956(h), set forth in Count Two, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE,
(5) YONGZHE XU,
(6) ZIYOU YUAN,
(7) ZHENBANG ZHOU
(8) MENGTING LIU, and
(9) ENCHIA LIU,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in such offense, and any property traceable to such property.

3. Upon conviction of the offense in violation of Title 18, United States Code, Section 1028(a)(7) and (f), set forth in Count Three, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE,
(5) YONGZHE XU,
(6) ZIYOU YUAN, and
(7) ZHENBANG ZHOU

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1028(b)(5), any personal property used or intended to be used to commit the offense and, pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such offense.

4. Upon conviction of the offense in violation of Title 18, United States Code, Section 371, set forth in Count Four, the defendants,

(1) ZHENXING WANG,
(2) JING BIN HUANG,
(3) BAOYU ZHOU, and
(4) TONG YUZE,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any personal property used or intended to be used to commit or to facilitate the commission of such offense and, pursuant to Title 18, United States Code, Sections 1030(i) and 982(a)(2)(B), any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such offense.

5. Upon conviction of the offense in violation of Title 50, United States Code, Section 1705(a) and (c), set forth in Count Five, the defendants,

(2) JING BIN HUANG,
(3) BAOYU ZHOU,
(4) TONG YUZE, and
(5) YONGZHE XU,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, that constitutes, or is derived from, proceeds traceable to the commission of the offense and, pursuant to Title 19, United States Code, Section 1595a(d), any merchandise exported or sent from the United States or attempted to be exported or sent from the United States contrary to law, or the proceeds or value thereof, and any property used to facilitate the exporting or sending of such merchandise, the attempted exporting or sending of such merchandise, or the receipt, purchase, transportation, concealment, or sale of such merchandise prior to exportation.

6. If any of the property described in Paragraphs 1 through 5, above, as being forfeitable pursuant Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c); Title 18, United States Code, Sections 982(a)(1), 982(a)(2)(B), 1028(b)(5), and Section 1030(i); and Title 19, United States Code, Section 1595a(d), 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;

it is the intention of the United States, pursuant to Title 18, United States Code, Sections 982(b)(2), 1028(g), and 1030(i)(2) and Title 28, United States Code, Section 2461(c), each incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the property described in Paragraphs 1 through 5 above.

All pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c); Title 18, United States Code, Sections 982(a)(1), 982(a)(2)(B), 1028(b)(5), and Section 1030(i); and Title 19, United States Code, Section 1595a(d).

A TRUE BILL.

Bruce Reeder
FOREPERSON

JASON A. CASEY
Assistant United States Attorney
District of Massachusetts

FOR
GREGORY NICOSIA
Trial Attorney
National Security Division
National Security Cyber Section
United States Department of Justice

District of Massachusetts: June 26th, 2025
Returned into the District Court by the Grand Jurors and filed.

11:57am
DEPUTY CLERK