UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. KEJIA WANG, a/k/a "Tony Wang," Defendant.	Criminal No. 25cr10274 NMG 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)) 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))

INFORMATION

At all times relevant to this Information:

Introduction and General Allegations

1. Since 2003, 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 illicit purposes, including obtaining sensitive, proprietary information from an employer's computer network without authorization; and (vi) use U.S. financial institutions to funnel wages paid by victimized 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 China in cities near the North Korean border, including in Dandong and Shenyang.

3. In order to circumvent 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 obtained assistance from persons residing in the United States. Among other things, these U.S. facilitators received and hosted multiple laptop computers and other hardware issued by U.S.

victim companies at their residences in the U.S. 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. enablers then facilitated remote access to the laptops by the overseas IT workers either by downloading remote desktop software to the computers, or by utilizing a hardware device designed to allow for remote access (often referred to as a keyboard, video, and mouse switch or "KVM" switch). The U.S. facilitators also established 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 were paid a substantial fee. Most of the money generated by this scheme, however, was funneled to the overseas IT workers and their overseas co-conspirators.

4. From in and around 2021 until approximately October 2024, one group of overseas IT workers, along with defendant KEJIA WANG and other co-conspirator facilitators in New Jersey, New York, California, and overseas, perpetrated such a coordinated scheme to conduct remote work for 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 DPRK IT workers and their co-conspirators stole the identities of U.S. citizens; applied for and obtained remote jobs at hundreds of U.S. companies, including many Fortune 500 companies; caused false and fraudulent employment verification information to be sent to DHS; received laptop computers 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; and received millions of dollars from the U.S. companies, much of which was falsely reported to the

IRS and SSA in the name of the actual U.S. persons whose identities were stolen.

5. The overseas IT workers were assisted in this scheme by defendant KEJIA WANG and at least four other U.S. persons. Among other things, KEJIA WANG and other U.S. facilitators received and/or hosted laptop computers belonging to U.S. victim companies at their residences so that the U.S. companies believed 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 and Tony WKJ LLC, 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 his services, defendant KEJIA WANG and other co-conspirators in the U.S. collected substantial fees. Defendant KEJIA WANG acted knowing that the overseas IT workers were, in fact, not located in the United States, that the overseas IT workers used false and/or stolen identities to gain employment as IT workers, and that the overseas IT workers were defrauding the U.S. companies.

6. The conspiracy perpetrated a massive fraud that impacted more than 100 U.S. companies, compromised the identities of more than 80 U.S. persons, caused false information to be conveyed to DHS, IRS, and SSA on dozens of occasions, 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. The victimized U.S. companies spanned 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 Co-Conspirators

7. Defendant KEJIA WANG, a/k/a "Tony Wang," was a United States citizen residing in New Jersey. KEJIA WANG was the founder of two New Jersey-based limited liability companies, Hopana Tech and Tony WKJ, that purported to specialize in software development. In fact, Hopana Tech and Tony WKJ were both shell companies used by KEJIA WANG and his co-conspirators to facilitate the criminal schemes described in this Information. Among other things, KEJIA WANG communicated with overseas IT workers and other overseas co-conspirators about the scheme via text message and email; traveled to Shenyang and Dandong, cities near the North Korean border, to meet with overseas co-conspirators about the scheme, including 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.

8. Zhenxing Wang, a/k/a "Danny," was a United States citizen residing in New Jersey. Zhenxing Wang was the founder of Independent Lab, a New Jersey based limited liability company that purported to specialize in software development. In fact, Independent Lab was a

shell company used by Zhenxing Wang and others to facilitate the criminal schemes described is this Information. Among other things, Zhenxing Wang received laptops belonging to U.S. victim companies addressed to persons whose identities had been stolen; hosted the laptop computers at his residence; accessed, without authorization, U.S. victim companies' laptops; facilitated remote access to the laptops 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.

9. Jing Bin Huang was a Chinese citizen residing in Dandong, China, a city near the border of North Korea, who, among other things, registered multiple 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.

10. aoyu 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.

11. 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.

12. 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.

13. 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.

14. 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.

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

16. Individual B was a resident of California who, in exchange for a fee, received and hosted U.S. victim company laptop computers at Individual B's residence and facilitated remote access to those computers by overseas IT workers.

17. Individual C 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 C'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 C 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 United States Attorney alleges:

18. The United States Attorney re-alleges and incorporates by reference paragraphs 1-17 of the Information.

19. From in or around 2021, the exact date being unknown to the United States Attorney, and continuing until in or around October 2024, in the District of Massachusetts and elsewhere, the defendant,

KEJIA WANG,

conspired with others known and unknown to the United States Attorney 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.

Object and Purposes of the Conspiracy

20. The object of the conspiracy was to commit wire fraud and mail fraud. The goals of the conspiracy were, among other things, to obtain employment for the overseas IT workers with U.S. companies using false or stolen identities in violation of U.S. laws, and to generate revenue for the DPRK IT workers, the defendant, and his co-conspirators.

Manner and Means of the Conspiracy to Defraud

21. Among the manner and means by which the defendant and his co-conspirators carried out the conspiracy and the scheme to defraud were the following:

a. Stealing the identities of U.S. persons;

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

c. Identifying remote IT jobs of interest at U.S. companies, including cleared defense contractors, and developed fictitious personas, resumes, and online profiles to match the requirements of those IT jobs;

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

e. 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;

f. Directing the U.S. companies to send their company-issued laptops and other equipment to the defendant's residence and the residences and other U.S. facilitators;

g. Causing U.S. company laptop computers to be transferred to the homes of other U.S. enablers, who then used credentials provided to them by the defendant and the overseas IT workers to access the U.S. companies' computer networks and facilitate remote access to the computers by the overseas IT workers;

h. 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, MTS, and online payment platforms opened and controlled by the defendant and other co-conspirators;

i. Transferring and causing the transfer of money between and among U.S. bank accounts, MTS, 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; and

j. Establishing domestic 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.

Acts in Furtherance of the Conspiracy and the Scheme to Defraud

22. In furtherance of the conspiracy and scheme to defraud, and to accomplish its goals, the following overt 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 DPRK IT workers intended to steal and use to apply for remote IT positions at U.S. companies, including companies whose laptop computers were received and/or hosted at the residences of KEJIA WANG, Zhenxing Wang, and Individuals A and B.

b. Between on or about September 29, 2021, and on or about September 5, 2023, Yuan's OBCS-1 account was used 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.

Sub ¶	U.S. Identity
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.
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.

c. Between approximately February 2023 and December 2023, 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 steal and use to apply for remote IT positions

at U.S. companies, including companies whose laptop computers were received at KEJIA WANG's residence.

The Fraudulent Use of Front Companies

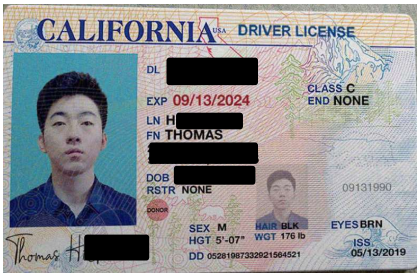
d. In 2021, the exact date being unknown, Individual C instructed KEJIA WANG to establish a U.S. company and corresponding financial accounts to be used in furtherance of the conspiracy and scheme to defraud.

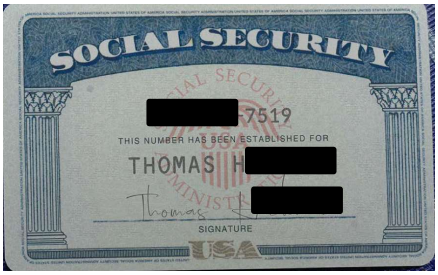
e. On or about January 11, 2021, consistent with instructions he received from Individual C, KEJIA WANG registered Hopana Tech LLC, a company purporting to specialize in IT and software development, with the New Jersey Secretary of State, listing his home address in New Jersey as the company's principal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

f. 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.

Fraudulent Employment with U.S. Company A

g. On or about 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 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:





h. The co-conspirator posing as Thomas H. obtained full-time, remote employment at Company A as a software engineer on or about January 17, 2023.

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

j. In order to receive direct deposits of salary and wages from Company A, 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 account registered to Mengting Liu.

k. After gaining employment with Company A, the overseas co-conspirator posing as Thomas H. instructed Company A to send his company-issued laptop computer to KEJIA WANG's residence in New Jersey. KEJIA WANG subsequently caused the Company A computer to be transferred to Zhenxing Wang.

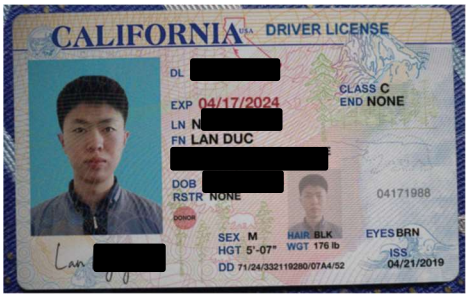
l. Between on or about January 2023 and June 6, 2023, Zhenxing Wang logged into the Company A computer using credentials provided to him by KEJIA

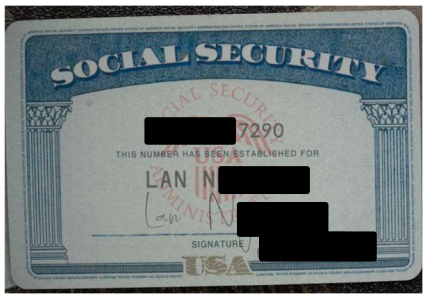
WANG and installed remote desktop software, all without authorization from Company A.

m. Between on or about January 21, 2023, and on or about May 6, 2024, KEJIA WANG and his co-conspirators caused Company A to deposit wages associated with employee Thomas H. totaling approximately $198,849.73 into a MTS account registered to Mengting Liu.

Fraudulent Employment with U.S. Company B

n. On or about 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, 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:





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

p. In or about January 2023, the overseas co-conspirator 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 citizen of the United States.

q. In order 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 was, unbeknownst to Company B, linked to an MTS account registered to an unidentified co-conspirator.

r. The overseas co-conspirator posing as Lan Duc N. instructed Company B to send his company-issued laptop computer to KEJIA WANG's residence in New Jersey. KEJIA WANG received a package addressed to "Jason N." containing a Company B laptop computer on or about January 25, 2023, and, in turn, caused the Company B computer to be transferred to Zhenxing Wang.

s. Between on or about January 25, 2023, and on or about November 23, 2023, Zhenxing Wang logged into the Company B laptop computer and, without authorization from Company B, installed a remote desktop application for the purpose of enabling overseas IT workers to access the Company B computer remotely.

t. Between on or about January 30, 2023, and on or about November 23, 2023, KEJIA WANG and his co-conspirators caused Company B to deposit wages associated with employee "Lan Duc N." totaling approximately $117,643.37 into a MTS account controlled by an unidentified co-conspirator.

Fraudulent Employment with U.S. Company C

u. 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. 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:

v. The overseas co-conspirator posing as Lan Duc N. obtained full-time, remote employment at Company C as a software engineer on or about January 9, 2024. The overseas co-conspirator subsequently completed, signed, and transmitted to Company C 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.

w. In order to receive direct deposits of salary and wages from Company C, the overseas IT worker 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.

x. After gaining employment with Company C, the overseas co-conspirator posing as Lan Duc N. instructed Company C to send a company-issued laptop computer to KEJIA WANG's residence in New Jersey. On or about January 6, 2024, KEJIA WANG received the Company C laptop computer and caused it to be transferred to Zhenxing Wang.

y. On or about January 19, 2024, Zhenxing WANG logged into the Company C computer and installed two remote desktop applications for the purpose of enabling overseas IT workers to access the computer remotely.

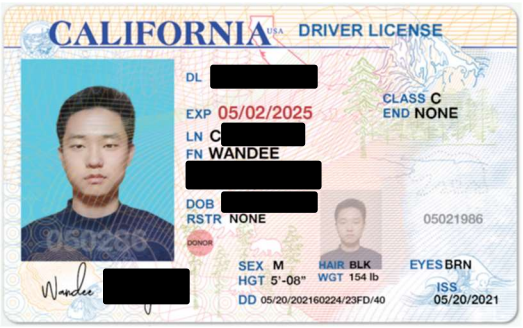
z. Between on or about January 19, 2024, and on or about April 2, 2024, without authorization from Company C, an overseas coconspirator accessed and downloaded computer files containing technical data and other information from Company C's servers, including information controlled under the ITAR and clearly marked as such.

aa. Between on or about January 9, 2024, and April 4, 2024, KEJIA WANG and his 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.

Fraudulent Employment with U.S. Company D

bb. 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 coconspirator

overseas IT worker 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:



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

dd. In or about 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.

ee. 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 D, linked to an MTS account registered to Yongzhe Xu on behalf of the company "Al Naseeh Consultancy FZE."

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

gg. Between on or about April 26, 2022, and on or about September 14, 2022, Zhenxing Wang logged into the Company D computer, without authorization, and facilitated remote access by an overseas IT worker.

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

ii. Between on or about April 18, 2022, and September 2022, KEJIA WANG and his co-conspirators caused Company D to deposit wages associated with employee "Wandee C." totaling approximately $58,167.92 into Yongzhe Xu's MTS account.

The Fraudulent Use of the U.S. Mail

jj. On or about the following dates, overseas co-conspirators caused packages containing laptop computers and other items belonging to U.S. victim companies 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 the following stolen U.S. person identities:

Sub ¶	Delivery Date	Recipient Identity
1.	2022-06-01	Jeffrey P.
2.	2022-06-08	Marcus C.
3.	2022-06-09	William S.
4.	2022-06-20	Marcus C.
5.	2022-06-20	Jason C.
6.	2022-06-27	Marcus J.
7.	2022-06-27	Allen H.
8.	2022-06-30	Marcus J. B.
9.	2022-07-09	Wandee C.
10.	2022-07-12	Marcus C.
11.	2022-07-14	Harold T.
12.	2022-07-14	Marcus B.
13.	2022-07-15	Marcus J .
14.	2022-07-16	Michael W.
15.	2022-07-18	Marcus B.

Sub ¶	Delivery Date	Recipient Identity
16.	2022-07-30	Marcus C.
17.	2022-08-01	Marcus J. B.
18.	2022-08-04	Kevin C.
19.	2022-08-11	William M.
20.	2022-08-18	Damian T.
21.	2022-09-01	Robert W.
22.	2022-09-01	Bradley H.
23.	2022-09-07	Bradley S.
24.	2022-09-10	Michael L.
25.	2022-09-12	William M.
26.	2022-09-16	rhomas [sic] H.
27.	2022-09-26	Chris B.
28.	2022-09-28	Steven J. F.
29.	2022-10-07	Chris B.
30.	2022-10-12	Jake B.
31.	2022-10-20	Steven F.
32.	2022-10-21	Jeffrey S.
33.	2022-11-07	Jeffrey W.
34.	2022-11-12	Bradley S.
35.	2022-11-16	Lee S.
36.	2022-11-29	Jeffrey S.
37.	2022-12-05	Lucas C.
38.	2022-12-16	Jeffrey S.
39.	2022-12-16	Lucas H.
40.	2022-12-27	Harold H.
41.	2022-12-29	Jeffrey S.
42.	2023-01-05	Jeffrey S.
43.	2023-01-26	Jason N.
44.	2023-01-30	Jason N.
45.	2023-02-02	Robert L.
46.	2023-02-03	Michael C.
47.	2023-02-11	Jake B.
48.	2023-02-13	Harold H.
49.	2023-02-22	Michael C.
50.	2023-02-27	Tannika R.
51.	2023-03-29	Brian C.
52.	2023-03-30	Michael C.
53.	2023-03-31	Robert L.
54.	2023-03-31	Brian C.
55.	2023-04-05	Michael L.
56.	2023-04-14	Gary F.
57.	2023-04-17	Lucas C.
58.	2023-04-20	Brian C.
59.	2023-05-13	Daniel A.
60.	2023-05-15	William M.
61.	2023-05-25	Gary F.
62.	2023-05-25	Gary F.
63.	2023-06-05	Michael C.
64.	2023-07-17	Michael C.
65.	2023-08-04	Charles L.
66.	2023-09-08	Jeremy J.
67.	2023-09-11	James B.
68.	2023-09-13	Robert L.
69.	2023-09-15	Gary F.
70.	2023-09-15	Harold H.
71.	2023-09-19	Gary F.
72.	2023-09-25	Deven C.
73.	2023-10-02	James L.

Sub ¶	Delivery Date	Recipient Identity
74.	2023-10-04	Robert L.
75.	2023-10-06	Steven L.
76.	2023-10-13	Jeremy A.
77.	2023-10-13	Jason N.
78.	2023-10-20	Jeremy A.
79.	2023-10-20	Deven C.
80.	2023-10-23	John L.
81.	2023-10-26	Edjose C.
82.	2023-11-10	Lucas F.
83.	2023-11-10	Charles L.
84.	2023-11-20	Jeremy J.
85.	2023-12-14	Jason N.
86.	2023-12-15	Lucas H.
87.	2023-12-20	John H.
88.	2023-12-23	Lan N.
89.	2023-12-29	Lucasn H.
90.	2024-01-04	Kevin C.
91.	2024-01-12	John H.
92.	2024-01-12	Phillip P.
93.	2024-01-26	Jason H.
94.	2024-02-08	Mitchell M.
95.	2024-02-23	Jamie M.
96.	2024-02-29	Matthew D.
97.	2024-03-07	Michael A.
98.	2024-03-12	Zackary L.
99.	2024-03-15	Matthew D.
100.	2024-03-21	Zackary L.
101.	2024-03-22	Tanikka R.
102.	2024-03-25	Jeff S.
103.	2024-04-02	John L.
104.	2024-04-04	Jamie M.
105.	2024-04-06	Chris B.
106.	2024-04-11	Matt D.
107.	2024-04-17	Matthew D.
108.	2024-04-19	Jamie M.
109.	2024-04-24	Lucas H.
110.	2024-04-26	Matt D.
111.	2024-05-03	Charles C.
112.	2024-05-10	John H.
113.	2024-05-11	James B.
114.	2024-05-21	Christopher C.
115.	2024-05-22	Christopher C.
116.	2024-06-12	John H.
117.	2024-06-28	Jamie M.

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

kk. In furtherance of the conspiracy and scheme to defraud, the 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.

ll. 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, approximately $464,532.56 was deposited into the Hopana Tech account at U.S. Bank 1 by multiple U.S. victim companies.

mm. On or about the dates indicated below, the following funds were transferred from the Hopana Tech account at U.S. Bank 1 to various accounts controlled by Jing Bin Huang, 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

nn. On or about April 29, 2021, KEJIA WANG registered an account at a money transfer service (hereinafter, "MTS-2") in the name of Tony WKJ LLC. Between on or about May 24, 2021, and on or about August 2, 2023, approximately $1,635,240.80 was deposited into the Tony WKJ account at MTS-2 from multiple U.S. victim companies.

oo. On or about the date ranges indicated below, the following funds were transferred from the Tony WKJ account at MTS-2 to bank accounts associated with Enchia Liu and other overseas co-conspirators:

TONY WKJ – MONEY TRANSFER SERVICE 1					
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

pp. 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.

qq. 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.

rr. Between on or about February 16, 2022, and on or about July 21, 2023, approximately $ 237,654.62 was deposited into KEJIA WANG's personal MTS-2 account by multiple U.S. victim companies. 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.

ss. 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 A, who was living in California. Most of these transfers contained notes that referenced the month the transfer took place and "CA laptops." For example, "September CA laptops," "October CA laptops," "November Electric," and "CA laptops #7 & 11 shipping fee."

tt. 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 B. Most of these transfers contained notes that referenced "NY" and "laptops." For example, "NY November Laptops" and "NY December Laptops."

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

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

ww. 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 a DPRK IT worker to obtain remote employment with [U.S. Company E].

All in violation of Title 18, United States Code, Section 1349.

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

The United States Attorney further alleges:

23. The United States Attorney re-alleges and incorporates by reference paragraphs 1-17 of this Information.

24. 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 the People's Republic of China ("PRC" or "China") or the UAE.

25. From in or about 2021, the exact date being unknown to the United States Attorney, through in or about October 2024, in the District of Massachusetts and elsewhere, the defendant,

KEJIA WANG,

conspired with others known and unknown to the United States Attorney 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, Section 1956(h).

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

The United States Attorney further alleges:

26. The United States Attorney re-alleges and incorporates by reference paragraphs 1-17 of this Information.

27. From in or about 2021, the exact date being unknown to the United States Attorney, through in or about October 2024, in the District of Massachusetts and elsewhere, the defendant,

KEJIA WANG,

did knowingly combine, conspire, and agree with other persons known and unknown to the United States Attorney 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).

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 defendant,

KEJIA WANG,

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 defendant,

KEJIA WANG,

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 defendant,

KEJIA WANG

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

Respectfully submitted,

LEAH B. FOLEY
United States Attorney

By: */s/ Jason A. Casey*
JASON A. CASEY
Assistant United States Attorney

/s/ Gregory J. Nicosia, Jr.
GREGORY J. NICOSIA, Jr.
Trial Attorney
National Security Division
National Security Cyber Section
United States Department of Justice