

FILED

OCT -1 2026

CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF OHIO
CLEVELAND

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

SUN SHENG MING, aka 孙圣明,

PEI LI GUANG,

WENG SHOU CHENG,

[REDACTED]

HAN GUO BIN, aka 韩国彬,

WANG JIAN JUN, aka 王建钧,

SHENG ZHANG KUN,

ZHANG WEI PING, aka 张卫平,

ZHANG LI PING,

YU YANG, aka 于洋,

JIN LONG,

[REDACTED]

MICHAEL JAMES BOSTELLE,

JUAN CECILIO PENA CARRILLO,

Defendants.

) INDICTMENT

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

)

CASE NO.

1726 CR 00429

Title 18, United States Code,
Sections 1028(a)(7) and (f),
1028A(a)(1), 1349, 1956(h), and
2

JUDGE FLEMING

GENERAL ALLEGATIONS

At all times relevant to this Indictment:

1. Since 2003, the Democratic People's Republic of Korea ("DPRK" or "North Korea") has been under sanctions by the United Nations ("UN") due to, among other things, its nuclear weapons program. Since 2016, the United States ("U.S.") 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 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 U.S., using false or stolen identities. According to a May 2022, advisory by the U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (“FBI”), North Korea had dispatched thousands of IT workers around the world (hereinafter, “overseas IT workers”), earning revenue that contributed 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. The overseas IT workers obtain assistance from persons residing in the United States to circumvent any controls that targeted U.S. and global companies had designed and implemented to prevent the hiring of illicit IT workers, and to otherwise prevent unauthorized access and damage to the companies' computer networks.

4. Among other ways to accomplish this scheme, these U.S. facilitators receive and host multiple laptop computers ("laptops") and other hardware issued by U.S. victim companies at their residences in the U.S., referred to as "laptop farms."

5. 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 enabled remote access to the laptops for the overseas IT workers either by downloading remote desktop software to the laptop or connecting the laptop to a hardware device designed to allow for remote access (such as a keyboard, video, and mouse switch or "KVM" switch).

6. 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.

7. 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.

8. From in and around 2019, to in or around July 2025, one group of overseas IT workers, SUN SHENG MING, aka 孙圣明; PEI LI GUANG; WENG SHOU CHENG; [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬; WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN; ZHANG WEI PING, aka 张卫平; ZHANG LI PING; YU YANG, 于洋; JIN LONG; [REDACTED] [REDACTED]; along with named and charged U.S.-based co-conspirators

MICHAEL JAMES BOSTELLE and JUAN CECILIO PENA CARRILLO, and Trey Michael Nolte, ("Nolte"), named but not charged herein, and others known and unknown to the Grand Jury, perpetrated a fraudulent scheme to conduct remote work for U.S. companies.

9. The scheme resulted in the transmission of false and misleading information to dozens of U.S. companies, financial institutions, and U.S. government agencies, including the Department of Homeland Security ("DHS"), Internal Revenue Service ("IRS"), and Social Security Administration ("SSA").

10. Specifically, this group of overseas IT workers and their co-conspirators stole the identities of U.S. citizens; applied for and obtained remote jobs at dozens of U.S. companies; caused false and fraudulent employment verification information to be sent to DHS; 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; 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 U.S. persons whose identities the IT workers had stolen.

11. The overseas IT workers SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] and [REDACTED] supervised overseas co-conspirators HAN GUO BIN, SHENG ZHANG KUN, WANG JIAN JUN, ZHANG WEI PING, ZHANG LI PING, YU YANG, JIN LONG, and directed PENA, Nolte and at least four other U.S. persons in the scheme. Nolte, in turn, recruited, managed and trained the U.S.-based facilitators, including BOSTELLE, each of whom, among other things, allowed their names and personal information to be used to further the overseas IT worker scheme in return for a share of the scheme's proceeds.

12. Among other things, the U.S.-based facilitators received and/or hosted laptops 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 DarkFalls, 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.

13. In exchange for performing these services, the overseas IT workers paid PENA, Nolte and other co-conspirators in the U.S. from the proceeds of the fraudulent worker scheme.

14. PENA and Nolte 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.

15. The conspiracy perpetrated a massive fraud that impacted more than 70 U.S. companies, compromised the identities of more than 25 U.S. persons, caused false information to be conveyed to DHS, IRS, and SSA on dozens of occasions, generated approximately \$3 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.

16. The victimized U.S. companies spanned multiple industries across much of the United States, including Massachusetts, California, New York, New Jersey, Florida, Georgia,

Minnesota, Maryland, North Carolina, Illinois, Ohio, Virginia, Michigan, Texas, Arkansas, Pennsylvania, Washington, and the District of Columbia.

THE CO-CONSPIRATORS

17. Nolte was a United States citizen residing in the Northern District of Ohio. Nolte was the founder of an Ohio-based limited liability company, Dark Falls LLC, that purported to specialize in software development. In fact, Dark Falls was a shell company used by Nolte and his co-conspirators to facilitate the criminal schemes described in this Indictment. Among other things, Nolte communicated with overseas IT workers and other overseas co-conspirators about the scheme via text message and email; sent packages containing electronics and other materials to Shenyang and Dandong, China, at the request of SUN SHENG MING; 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 to persons using the actual names of K.F., P.B., V.J., N.M., and additional U.S. facilitators, known and unknown to the Grand Jury, where they were remotely accessed by overseas IT workers; and received money from U.S. victim companies into bank and other financial accounts that Nolte established and controlled, a significant portion of which he subsequently transferred to accounts owned and controlled by overseas co-conspirators.

18. SUN SHENG MING, aka 孙圣明, also known by the online moniker “GOLDLINE 1,” and the names Wang Caihong and Chunayn, resided in Dandong, China, and, 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 Nolte and other co-conspirators. SUN also functioned as a supervisor of overseas co-conspirators posing as employees and domestic co-conspirators facilitating the overseas

worker scheme.

19. PEI LI GUANG, also known by the online moniker "GOLDLINE 2," resided in China. Among other things, PEI received packages shipped by Nolte which contained, among other items, two laptops acquired from companies which had unknowingly hired overseas members of the conspiracy. PEI also functioned as a supervisor of overseas co-conspirators posing as employees and domestic co-conspirators facilitating the overseas worker scheme.

20. WENG SHOU CHENG, also known by the online monikers "GOLDENSEA787," "GOLDENCENTAUR55," and "GOLDLINE 3," was a Chinese citizen residing in China. Among other things, WENG registered MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Nolte and other co-conspirators. WENG also functioned as a supervisor of overseas co-conspirators posing as employees and domestic co-conspirators facilitating the overseas worker scheme.

21. [REDACTED] [REDACTED] also known by the monikers [REDACTED] and [REDACTED] functioned as a supervisor of overseas co-conspirators posing as employees and domestic co-conspirators facilitating the overseas worker scheme. [REDACTED] shared responsibility of managing the email using the moniker "GOLDENCENTAUR55" with other members of the conspiracy.

22. HAN GUO BIN, aka 韩国彬, resided in China. Among other things, HAN GUO received and transferred proceeds generated through the conspiracy, including to or from Nolte and other co-conspirators.

23. WANG JIAN JUN, aka 王建钧, who also used the online monikers “JAMES WANG,” “MING WANG JIAN HOOK,” and “CARROT7277,” was a Chinese citizen residing in China. Among other things, WANG registered MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Nolte and other co-conspirators.

24. SHENG ZHANG KUN resided in China. Among other things, SHENG ZHANG KUN also received packages shipped by Nolte including, among other items, laptops acquired from companies which had unknowingly hired overseas members of the conspiracy.

25. ZHANG WEI PING, aka 张卫平, was a Chinese citizen residing in China. Among other things, ZHANG WEI PING received and transferred proceeds generated through the conspiracy, including to or from Nolte and other co-conspirators.

26. ZHANG LI PING was a Chinese citizen residing in China. Among other things, ZHANG LI PING received and transferred proceeds generated through the conspiracy, including to or from Nolte and other co-conspirators.

27. YU YANG, aka 于洋, resided in China. Among other things, YU YANG registered MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Nolte and other co-conspirators.

28. JIN LONG, also known by the online monikers “PATRICK BONNER,” and “JOHN ANTHONY NEVAREZ,” resided in China. Among other things, JIN LONG registered multiple MTS and foreign bank accounts that were used to receive and transfer proceeds generated through the conspiracy, including from Nolte and other co-conspirators. LONG, using the name PATRICK BONNER, also functioned as a supervisor of overseas co-conspirators posing as employees and domestic co-conspirators facilitating the overseas worker scheme.

LONG also incorporated the company B SUCCEED, LLC, in the state of Texas in an effort to create a purported legitimate U.S.- based company who could provide validation of past employment for fraudulent overseas IT worker applications.

29. [REDACTED] [REDACTED] also known by the moniker [REDACTED] [REDACTED] was a [REDACTED] citizen who maintained a banking relationship with MTS-2. [REDACTED] functioned as a supervisor of overseas co-conspirators posing as employees and domestic co-conspirators facilitating the overseas worker scheme with other members of the conspiracy.

30. MICHAEL JAMES BOSTELLE was a resident of Pennsylvania who, in exchange for a fee, received and caused to be sent laptops to Nolte's residence and that Nolte hosted to facilitate remote access to those computers by overseas IT workers.

31. JUAN CECILIO PENA CARRILLO, also known as JUAN PENA, was a resident of Texas, who in exchange for a fee, received and hosted U.S. victim company laptop computers and facilitated remote access to those computers by overseas IT workers, including, but not limited to allowing co-conspirators to register, maintain and use the email whose address was identifiably based on PENA's name.

VICTIM BANKS AND FINANCIAL INSTITUTIONS

At all times relevant to the Indictment:

32. MTS-1 was a money transfer service that used the Internet to host its services, which included banking and money remittal transaction support. MTS-1 clients registered accounts with their actual names, but then selected a username linked both to an email account and a bank with branches in the United States.

33. MTS-2 was a money transfer service that used the Internet to host its services, which included banking and money remittal transaction support.

34. MTS-3 was a money transfer service that used the Internet to host its services, which included banking and money remittal transaction support.

35. MTS-4 was a money transfer service that used the Internet to host its services, which included banking and money remittal transaction support.

36. MTS-5 was a money transfer service that used the Internet to host its services, which included banking and money remittal transaction support.

37. MTS-6 was a money transfer service that uses the Internet to host its services, which include banking and money remittal transaction support.

38. BANK-1 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

39. BANK-2 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

40. BANK-3 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

41. BANK-4 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

42. BANK-5 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

43. BANK-6 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

44. BANK-7 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

45. BANK-8 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

46. BANK-9 was a China-based bank, and which conducted business via electronic banking via web-based applications as well.

47. BANK-10 was a United States-based bank with branches in the Northern District of Ohio, and which conducted business via electronic banking via web-based applications as well.

48. BANK-11 was a United States-based Internet-based bank, and which conducted business via electronic banking via web-based applications as well.

49. BANK-12 was a United States-based Internet-based bank, and which conducted business via electronic banking via web-based applications as well.

50. BANKS 1-12 were Federally insured banking institutions, as defined by 18 U.S.C. § 20.

DOMESTIC VICTIM COMPANIES

51. Victim Company 1 was a company located in California.

52. Victim Company 2 was a company located in New Jersey.

53. Victim Company 3 was a company located in Virginia.
54. Victim Company 4 was a company located in Virginia.
55. Victim Company 5 was a company located in California.
56. Victim Company 6 was a company located in Massachusetts.
57. Victim Company 7 was a company located in Texas.
58. Victim Company 8 was a company located in Delaware.
59. Victim Company 9 was a company located in Washington state.
60. Victim Company 10 was a company located in Florida.
61. Victim Company 11 was a company located in Colorado.
62. Victim Company 12 was a company located in Michigan.
63. Victim Company 13 was a company located in Pennsylvania.
64. Victim Company 14 was a company located in Illinois.
65. Victim Company 15 was a company located in California.
66. Victim Company 16 was a company located in Nevada.
67. Victim Company 17 was a company located in California.
68. Victim Company 18 was a company located in Florida.
69. Victim Company 19 was a company located in Minnesota.
70. Victim Company 20 was a company located in New Jersey.
71. Victim Company 21 was a company located in California.
72. Victim Company 22 was a company located in Texas.
73. Victim Company 23 was a company located in New York.
74. Victim Company 24 was a company located in Virginia.
75. Victim Company 25 was a company located in Michigan.

76. Victim Company 26 was a company located in Pennsylvania.
77. Victim Company 27 was a company located in California.
78. Victim Company 28 was a company located in New Jersey.
79. Victim Company 29 was a company located in Ohio.
80. Victim Company 30 was a company located in Michigan.
81. Victim Company 31 was a company located in Oregon.
82. Victim Company 32 was a company located in Washington state.
83. Victim Company 33 was a company located in Colorado.

COUNT 1

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

The Grand Jury charges:

84. Paragraphs 1-83 of the Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

85. From on or about February 1, 2019, to on or about January 21, 2026, in the Northern District of Ohio and elsewhere, defendants SUN SHENG MING, aka 孙圣明; PEI LI GUANG; WENG SHOU CHENG; [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬; WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN; ZHANG WEI PING, aka 张卫平; ZHANG LI PING; YU YANG, aka 于洋; JIN LONG; [REDACTED] [REDACTED] MICHAEL JAMES BOSTELLE; and JUAN CECILIO PENA CARRILLO conspired together and with each other and 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.

Object and Purposes of the Conspiracy

86. 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 overseas IT workers, the government of the Democratic People's Republic of Korea, and other co-conspirators.

Manner and Means of the Conspiracy to Defraud

87. Among the manner and means by which the defendants carried out the conspiracy and the scheme to defraud were the following:

- a. Identifying remote IT jobs of interest at U.S. companies, and developing fictitious personas, resumes, and online profiles to match the requirements of those IT jobs;

- b. Stealing, or otherwise obtaining previously stolen, identities of U.S. persons;
- c. Validating the stolen U.S. person identities using falsified identity documents, fraudulently notarized attestations, fraudulent college diplomas, fictional employment references based on fraudulent email addresses and telephone numbers, and fictitious resumes;
- 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 fraudulent and fictitious 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 PENA and Nolte's residences and the residences of other U.S. facilitators;
- g. Causing U.S. company laptop computers to be transferred to the homes of other U.S. facilitators, who then used credentials provided to them by the defendants 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 defendants and other co-conspirators; and,

- 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 defendants and co-conspirators abroad, including defendants who lived or claimed to be living in Dandong, Shenyang, Shenzhen, and Hong Kong, China, among other locations.

Acts in Furtherance of the Conspiracy and the Scheme to Defraud

88. In furtherance of the conspiracy, and to effect the objects and conceal the existence thereof, Defendants and others performed acts in the Northern District of Ohio and elsewhere, including, but not limited to, the following:

Acquiring and Creating Fraudulent Personas Based on U.S. Identity Theft Victims

89. From on or about February 1, 2019, to on or about January 21, 2026, Nolte, PENA, BOSTELLE, and K.F. received from overseas co-conspirators fraudulently created and fictitious identity documents and identifiers of actual persons to present to companies and banks in order to fraudulently verify employment eligibility or satisfy Know-Your-Customer (“KYC”) requirements for banking.

90. From on or about February 1, 2019, to on or about January 21, 2026, Nolte and PENA maintained various forms of fraudulent and fictitious identification and Personally Identifiable Information (“PII”) for employment validation, system access and KYC requirements including, but not limited to, drivers licenses, Social Security cards, resumes, IP

addresses, login credentials, college diplomas from the unaccredited non-U.S.-based online college Charter University, photographs, addresses, and bank account information.

91. From on or about February 1, 2019, to on or about January 21, 2026, PENA, BOSTELLE, and K.F. allowed their names, images, and PII to be used by Nolte, PENA, SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED] [REDACTED] and others known and unknown to the Grand Jury to present to potential employers.

92. On or about July 15, 2025, Nolte possessed the following names, forms of identification, and PII for the purpose of furthering the conspiracy and scheme to defraud:

Sub ¶	U.S. Identity	Types of PII Identifiers
1	D.B	Charter University diploma; index card with usernames and passwords
2	B.B	2022 W-2 from Victim Company 26; Post-it note with username and password
3	B.K	Mail from Victim Company 28; paystub from Victim Company 28; mail from Victim Company 14
4	S.R	Index cards with usernames and passwords; packaging for laptop; paper with username, password and VPN instructions; mail re: pre-employment background check with Victim Company 30; Charter University diploma; notarized background check paperwork; Post-it note with username and password
5	T.H	Packaging from computer monitor; handwritten paycheck from Victim Company 27.
6	R.M.	Packaging from computer monitor
7	J.B.	Paper with usernames and passwords; two paychecks from Victim Company 22; driver's license; social security card
8	P.B.	Paper with usernames and passwords; mailer addressed to P.B.; mail piece from non-victim bank credit card addressed to P.B.; index card with login information for Victim Company 31
9	P.B.	Paper with usernames and passwords; mail addressed to P.B. at Akron address; index card with usernames and passwords; debit card with the name of P.B.; UPS shipping label with Wyomissing, PA address

Sub ¶	U.S. Identity	Types of PII Identifiers
10	A.S.	Paper with usernames and passwords; driver's license
11	M.R.	Paper with usernames and passwords; Charter University diploma; index card with usernames and passwords; social security card; driver's license
12	M.B.	Packaging for Lenovo ThinkPad; mail addressed to M.B.; Post-it note with username and password
13	D.G.	Packaging for Lenovo ThinkPad; Post-it note with username and password
14	Jo.B.	Packaging for laptop,
15	M.A.	Two pieces of mail addressed to M.A.
16	J.J.	Index card with login information for Victim Company 32
17	R.G.	Charter University diploma
18	Pa.B.	Charter University diploma
19	C.B.	Mail from Victim Company 23
20	S.I.	Mail from Victim Company 12; W-2 from Victim Company 29; W-2 from Victim Company 11; W-2 from Victim Company 33
21	R.D.	Piece of certified mail addressed to R.D.
22	P.P.	Mail with instructions to activate MTS-3 card; driver's license
23	K.H.	Mail from attorneys

93. On or about January 21, 2026, PENA possessed the following names, forms of identification, and PII for the purpose of furthering the conspiracy and scheme to defraud:

Sub ¶	U.S. Identity	Type of PII Identifier
1	A.M.	Visa card from BANK-11
2	A.S.	Driver's License
3	J.C.	1099-NEC
4	R.D.	Packing slip for shipment of an Apple MacBook Pro

Conspiracy to Use Fraudulent Identities to Further the Fraud Scheme

94. From on or about February 1, 2019, to on or about March 19, 2019, Nolte and SUN, using the moniker "GOLDLINE," had conversations in which SUN directed Nolte to obtain a laptop and install various remote access software programs on it, then provide login

information, cellphone access and bank account information to SUN so SUN could begin using Nolte's identity to apply for domestic positions.

95. From on or about February 1, 2019, to on or about March 19, 2019, Nolte and SUN, using the moniker "GOLDLINE," had conversations in which SUN directed Nolte to create Linked In and other professional accounts so SUN could post fraudulent resumes and job credentials to attract domestic employers to offer Nolte, or fraudulent personas using his platform, employment.

96. On or about March 21, 2019, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to confirm a verification using a telephone number and account with an employment agency entirely created by SUN using Nolte's credentials and personal information.

97. On or about March 29, 2019, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte how to behave during an interview SUN set up with a U.S.-based employer, telling Nolte, in sum and substance, that employers just want to see an American and he, SUN, would type all the answers to the interview questions.

98. On or about November 7, 2019, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to pose as an applicant named J.D. from Michigan during an online video interview.

99. On or about November 9, 2019, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to make sure SUN was still able to access database libraries on a remote server. Nolte replied that as long as the laptop set up by SUN and maintained by Nolte was kept on using a remote access program, access would be assured.

100. On or about March 16, 2021, Nolte and SUN, using the moniker “GOLDLINE,” had a conversation in which SUN directed Nolte to conduct an interview providing fraudulent information about a fictitious domestic worker and their purported work history during an interview. Nolte complained that he was tired of always lying to companies, but conducted the interview as directed.

101. On or about November 15, 2022, Nolte and LONG, using the moniker “PATRICK BONNER,” had a conversation in which LONG directed Nolte to join a Discord channel to receive information from SUN concerning the use of the fraudulent name J.N. and acquire a laptop, in order to load AnyDesk on to it, for use by overseas co-conspirators in the remote worker scheme.

102. On or about February 3, 2023, and February 7, 2023, Nolte and LONG, using the moniker “PATRICK BONNER,” had a conversation in which LONG directed Nolte to register a fraudulent company in the state of Texas to assist in the opening of bank accounts to be used by SUN and other members of the criminal scheme. Nolte responded, “It looks like money laundering.”

103. On or about February 16, 2023, Nolte and LONG, using the moniker “PATRICK BONNER,” had a conversation in which LONG asked Nolte to use his U.S.-based telephone number to verify an identity LONG was using in the scheme to defraud.

104. On or about March 14, 2023, Nolte and SUN, using the moniker “GOLDLINE,” had a conversation over Discord in which SUN directed Nolte to set up four U.S.-based telephone numbers for use by overseas co-conspirators to verify applicant accounts, so the overseas co-conspirators appeared to be domestic workers. Nolte set up four application accounts and provided SUN with the telephone numbers and account log-in credentials.

105. On or about March 15, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to work with [REDACTED] and [REDACTED] if SUN was not available.

106. On or about March 17, 2023, Nolte and LONG, using the moniker "PATRICK BONNER," had a conversation in which LONG asked Nolte to provide his telephone number for additional account verifications because it was not a VOIP number.

107. On or about April 4, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to provide updates on approximately 24 laptops Nolte was maintaining for SUN using fraudulent employee identification including C.B., A.S., J.B., R.G., and others known and unknown to the Grand Jury.

108. On or about June 1, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to stop using the fraudulent identification A.S. because Nolte received paperwork requesting the fingerprints of A.S. SUN stated, "That sucks because we've been using A.S. for over a year."

109. On or about July 11, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN informed Nolte that SUN was setting up a fraudulent account for K.F. in order to use K.F.'s name and identifiers in the same manner they used Nolte's. Nolte responded by offering suggestions to SUN about responses K.F. could provide during interviews with victim companies so K.F. sounded more qualified for positions.

110. On or about February 23, 2024, Nolte and [REDACTED] using the moniker "[REDACTED]" had a conversation in which [REDACTED] explained that Nolte needed to send approximately five laptops provided by victim companies, involving four different

fraudulent identities, to another location, in order to ensure that the companies would not detect the scheme through IP tracing and potentially implicate Nolte.

111. On or about April 8, 2024, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker "[REDACTED] [REDACTED]" directed Nolte to provide JAMES WANG with "real US info," like he did with K.F.

112. On or about May 8, 2024, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker "[REDACTED] [REDACTED]" directed Nolte not to discuss R.D. with law enforcement if they asked Nolte about the use of R.D.'s identity. [REDACTED] suggested to Nolte that he should reply, "a strange online guy wanted help from [you] and [you] know nothing about him."

113. On or about June 20, 2024, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker "[REDACTED] [REDACTED]" introduced an overseas programmer using the moniker "SYDROM9265." After discussing the programmer's connection to the moniker GOLDLINE, [REDACTED] stated, "He's like my team."

114. On or about July 2, 2024, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker "[REDACTED] [REDACTED]" provided Nolte with instructions regarding recipients of money transfers and cryptocurrency. [REDACTED] also identified SYDROM9265 as GOLDLINE's biological brother.

115. On or about October 9, 2024, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker "[REDACTED] [REDACTED] [REDACTED]" directed Nolte to send him a list of company names who have sent laptops to Nolte. The purpose of the list was to ensure that a company was not sending laptops for multiple fraudulent employees to the same address.

116. On or about June 10, 2025, SUN, using the moniker "GOLDLINE," provided Nolte the identity and associated email account Sxxx.Bxxx@gmail.com, with a corresponding password that was to be used to further the fraudulent scheme.

117. On or about June 10, 2025, SUN, using the moniker "GOLDLINE," provided Nolte the identity J.R., with an address in Texas, to activate a Nokia cellular telephone that was to be used to further the fraudulent scheme by providing a domestic telephone number that could be used for two-party verification and authentication.

118. On or about July 1, 2024, SUN, using the moniker "GOLDLINE," directed Nolte to create a new domestic telephone account to obtain telephone numbers to be used in fraudulent employment verification schemes using the below fraudulent driver's license and persona.

119. On or about July 2, 2024, Nolte, SYNDROM9265 and [REDACTED] [REDACTED] using the moniker "[REDACTED]" had a conversation in which [REDACTED] directed Nolte to set up two laptops for SYNDROM9265, so the laptops will show domestic IP addresses when connecting to the victim companies' networks and can be verified as located within the United States if victim companies sought to verify the location of the fraudulent employee.

120. On or about July 7, 2024, SUN, using the moniker "GOLDLINE," directed Nolte to hire an actor to portray S.B. during an in-person job interview with a local hiring manager in Akron, Ohio, knowing that the identification information for employment verification presented prior to the interview was fraudulent.

121. On or about July 8, 2025, SUN, using the moniker "GOLDLINE," directed Nolte to pay for advertisements to recruit actors with a stolen credit card and billing information in the name of C.J.

122. On or about July 17, 2024, during a conversation between Nolte and [REDACTED] using the moniker "[REDACTED] [REDACTED]" direct Nolte to provide him with the number of active laptops managed by Nolte, as well as, the number of telephones maintained by Nolte for the benefit of overseas co-conspirators. Nolte did not list the number of laptops actively used, but identified at least six phones used by the conspiracy, five of which had Akron-area area codes.

123. On or about August 16, 2024, Nolte and LONG, using the moniker "PATRICK BONNER," had a conversation in which LONG directed Nolte to install various remote access software onto two laptops for use by overseas co-conspirators in the fraudulent scheme.

124. On or about August 30, 2024, and September 2, 2024, Nolte and LONG, using the moniker "PATRICK BONNER," had a conversation in which LONG directed Nolte to load AnyDesk and Zoom onto a laptop provided to the fraudulent employee D.G., and two other laptops, and to run that laptop for an overseas co-conspirator.

Use of Fraudulent Identifications to Profit by Employment with Victim Companies 1-29

125. From on or about February 1, 2019, until on or about January 21, 2026, SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED] [REDACTED] other overseas co-conspirators, used the proceeds of the fraudulent overseas IT worker scheme to pay Nolte, and PENA, and other uncharged domestic co-conspirators for using fraudulent and fictitious identifiers to help overseas IT workers pose as U.S.-based remote employees.

Use of Fraudulent Identification to Gain and Maintain Employment with Company 1

126. On or about March 16, 2022, Nolte created the email address michael.j.bostelle[REDACTED]gmail.com, a fraudulent email account in the name of BOSTELLE.

127. On or about January 3, 2023, SUN and other overseas co-conspirators used BOSTELLE's name, the email address michael.j.bostelle[[@](mailto:michael.j.bostelle@gmail.com)]gmail.com and a fraudulent driver's license in BOSTELLE's name to be hired by Victim Company 1.

128. On or about January 3, 2023, SUN and other overseas co-conspirators caused Victim Company 1 to send electronic devices, including a laptop, to BOSTELLE's address in Pennsylvania.

129. From on or about January 3, 2023, through on or about April 15, 2024, Nolte used an IP address in Akron, Ohio, to access the michael.j.bostelle[[@](mailto:michael.j.bostelle@gmail.com)]gmail.com for communications with Victim Company 1 relating to the employment of the BOSTELLE persona.

130. From on or about January 2023, to on or about April 2024, Nolte installed TeamViewer and VNC Viewer immediately after his first/initial log on to the MacBook provided by Victim Company 1 to allow for SUN and other co-conspirators to have remote access, file sharing, and collaboration capabilities, making it suitable for both individual and team use, especially in IT support and remote work scenarios.

131. From on or about March 2023, to on or about March 2024, Nolte installed additional software that allowed for the execution of Android applications used by SUN and other co-conspirators to remotely access victim company computers running Microsoft Windows or macOS.

132. From on or about March 2022, to on or about March 2024, Nolte, using his computer, made domain name server (DNS) requests to multiple suspicious sites related to fake document creation websites, malvertising sites, and identify verification sites.

133. From on or about March 2022, to on or about March 2024, Nolte installed and used multiple remote management tools (RMM) on the MacBook provided by Victim Company

1, including Chrome Remote Desktop and GetScreen.me, allowing SUN and other co-conspirators to remotely access another computer provided by an unknown victim company and managed by Nolte as part of the criminal scheme through Chrome browser or a Chromebook, and also to allow users to remotely access and manage their PCs and Macs from any device, including iOS and Android.

134. From on or about January 2023, to on or about April 2024, Nolte allowed SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED] [REDACTED] and other overseas co-conspirators known and unknown to the Grand Jury to log in to electronic devices provided by Victim Company 1 via VPN/Proxy networks and second factor multi-factor authentication (MFA) approvals from Chinese mobile IP addresses. As a result of Nolte's use of fraudulent credentials, MFA was accepted approximately 95% of the time from IP 39.152.179.72, which is owned by China Mobile Communications Corporation and resolves to China, which access otherwise would have been denied.

135. On or about April 15, 2024, Victim Company 1 terminated the employment of the BOSTELLE persona and asked the BOSTELLE persona to return the company's electronic devices. Nolte, using michael.j.bostelle[.]gmail.com, asked Victim Company 1 to send to his Akron, Ohio address mailing boxes to return the devices.

136. On or about April 16, 2024, Nolte returned a laptop to Victim Company 1 that had been badly damaged and burned.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 2

137. From on or about January 1, 2024, to on or about March 1, 2024, PENA used the name of an actual person, R.D., to gain employment with Victim Company 2.

138. On or about March 1, 2024, using the name R.D., PENA caused to be sent from Victim Company 2 to PENA's home address, a package containing a laptop computer addressed to R.D.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 3

139. On or about December 31, 2024, PENA applied to Victim Company 3 using a fraudulent form of identification.

140. On or about January 14, 2025, an individual claiming to be PENA conducted an online interview with Victim Company 3. Victim Company 3 offered PENA employment at the end of the interview

141. On or about January 21, 2025, the individual using the identity of PENA accepted the offer of employment.

142. On or about January 23, 2025, using his own name, PENA caused to be sent from Victim Company 3 to his home address a package containing a laptop computer.

143. On or about January 27, 2025, a second individual using PENA's identity engaged in an online onboarding meeting with Victim Company 3.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 4

144. On or about February 4, 2025, an individual using PENA's identity accepted a position of employment with Victim Company 4 and provided PENA's name and his home address as the address to which to send a laptop.

145. On or about February 10, 2025, PENA and other co-conspirators installed Chrome Remote Desktop, AnyDesk, and Team Viewer software on the laptop sent by Victim Company 4. These programs allow a computer to be controlled remotely.

146. From on or about February 12, 2025, to on or about February 17, 2025, PENA, using an email account set up by an unidentified overseas co-conspirator, responded to questions from Victim Company 4 about the prohibited software.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 5

147. On or about March 17, 2025, an individual using the identity of PENA provided fraudulent identification documents to Victim Company 5 during an interview, was hired, and sent a laptop to PENA at his home address.

148. On or about March 17, 2025, an individual presented fictitious and fraudulent identification, including a Texas driver's license and Social Security card, bearing PENA's PII.

149. PENA communicated with Victim Company 5 using the same fraudulent Gmail address set up by unidentified overseas co-conspirators to communicate as PENA and provided a telephone number fraudulently established in his name to be used by co-conspirators to serve as a U.S.-based telephone number for account validation.

150. On or about March 17, 2025, PENA opened a bank account into which, during the term of employment, Victim Company 5 deposited approximately \$15,638.31 in wages.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 6

151. On or about April 21, 2025, an individual using PENA's identity was hired by Victim Company 6.

152. On or about April 21, 2025, during the interview process, the individual fraudulently posing as PENA provided a resume, W-4, I-9, and banking information with BANK-12.

153. On or about April 21, 2025, PENA caused Victim Company 6 to mail a laptop and other electronic equipment to PENA at his home address.

154. PENA received approximately \$6,288.85 into a bank account in his name from Victim Company 6.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 7

155. On or about April 7, 2025, an individual using PENA's identity was hired by Victim Company 7, with an anticipated start date of April 21, 2025.

156. During the interview process, the co-conspirator fraudulently using the identity of PENA provided a fraudulent Texas driver's license and Social Security card in PENA's name.

157. On or about April 15, 2025, PENA caused Victim Company 7 to mail a laptop and other electronic equipment to PENA at his home address.

158. PENA received \$43,080.13 into an MTS-3 account in his name as salary from Victim Company 7.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 8

159. On or about April 14, 2025, PENA was hired by Victim Company 8 as a result of an individual representing himself to be PENA appearing on a video interview and providing a fictitious Gmail and telephone number, and false Texas driver's license.

160. On or about April 14, 2025, that individual representing himself to be PENA caused Victim Company 8 to mail a laptop and other electronic equipment to PENA at his home address.

161. On or about May 10, 2025, PENA attempted to connect the laptop provided by Victim Company 8 to a remote software device in violation of Victim Company 8's policies.

162. On or about May 12, 2025, the unidentified co-conspirator using PENA's identity made excuses in order to evade attending in-person meetings, video calls, or responding promptly to requests; as a result of this behavior, Victim Company 8 terminated the unidentified

co-conspirator using PENA's identity. Prior to termination, PENA received approximately \$13,728 by check from Victim Company 8.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 9

163. On or about May 7, 2025, a co-conspirator using PENA's identity was hired by Victim Company 9 and the individual representing himself to be PENA caused Victim Company 9 to mail a laptop and other electronic equipment to PENA at his home address.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 10

164. On or about April 9, 2025, a co-conspirator using PENA's identity was hired by Victim Company 10.

165. On or about April 9, 2025, the individual representing himself to be PENA caused Victim Company 10 to mail a laptop and other electronic equipment to PENA at his home address.

166. During the interview process, PENA communicated using a fraudulent Gmail address and telephone number set up by co-conspirators to use for domestic authentication but did not provide any identification documents.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 11

167. On or about March 4, 2024, Nolte used the name of an actual person, R.D., to gain employment with Victim Company 11.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 12

168. On or about December 11, 2023, Nolte used the name of an actual person, R.D., to gain employment with Victim Company 12.

169. On or about December 21, 2023, Victim Company 12 received a fraudulent I-9 containing a fraudulent Ohio driver's license and Social Security card of R.D.

170. On or about December 21, 2023, an individual claiming to be R.D. opened a bank account at BANK-10 that could send and receive international transfers.

171. On or about January 1, 2024, Nolte caused a laptop to be sent to Nolte's address in the Northern District of Ohio in the name of R.D.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 13

172. On or about February 27, 2024, PENA used the name of an actual person, R.D. to gain employment with Victim Company 13.

173. On or about March 1, 2025, PENA, using the name R.D., caused to be sent from Victim Company 13 to PENA's home address, a package containing a laptop computer addressed to R.D.

174. On or about April 16, 2025, PENA, using his own name, caused to be sent from Victim Company 13 to PENA's home address, a package containing a laptop computer addressed to PENA.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 14

175. From on or about September 3, 2024, until on or about November 15, 2024, Nolte, using the fraudulent identity B.K., caused to be deposited into an account Nolte controlled at BANK-4 under the name "Dark Falls, LLC," 8 deposits from Victim Company 14 with the notation "Payroll: B.K." The total deposits were \$42,591.74.

176. From on or about September 4, 2024, until on or about November 15, 2024, Nolte transferred from the Dark Falls, LLC bank account to an MTS-6 account in Nolte's name, and to an account at BANK-1 in Nolte's name, monies totaling \$41,106.74.

177. On or about July 15, 2025, during the search of Nolte's residence, Nolte possessed mail, paystubs and other documents in B.K.'s name that Nolte received from Victim Company 14.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 15

178. On or about May 2022, through May 2024, Nolte used the name C.P. to establish employment with Victim Company 15.

179. At some time in May 2022, Nolte caused Victim Company 15 to send a laptop to Nolte, who established credentials for C.P., and maintained those credentials at Nolte's address in the Northern District of Ohio.

180. On or about April 4, 2024, during discussions with SUN, using the moniker "GOLDLINE," GOLDLINE directed Nolte to "check [Victim Company 15] laptop," to ensure it was still active and running.

181. As a result of the fraudulent employment, Nolte caused Victim Company 15 to transfer over \$600,000 to Nolte using the identity C.P.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 16

182. On or about January 6, 2025, SUN, using the moniker "GOLDLINE," and [REDACTED] using the moniker "[REDACTED] [REDACTED]" provided Nolte with credentials of PATRICK BONNER to gain employment with Victim Company 16.

183. On or about January 6, 2025, Nolte caused Victim Company 16 to mail a payroll check in the amount of approximately \$4,582.00 to the fraudulent name PATRICK BONNER (PB) to the address of Nolte in the Northern District of Ohio.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 17

184. From on or about April 13, 2025, to on or about October 13, 2025, PENA was hired by Victim Company 17, for the benefit of overseas co-conspirators.

185. During the time of his employment, PENA caused to be deposited thirteen payroll checks from Victim Company 17, made payable to PENA for work done by overseas co-conspirators using PENA's identity, in the total amount of \$41,346.57.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 18

186. From on or about April 23, 2025, to on or about May 28, 2025, PENA was hired by Victim Company 18, for the benefit of overseas co-conspirators.

187. During the time of PENA's employment, PENA caused to be deposited two payroll checks from Victim Company 18, made payable to PENA for work done by overseas co-conspirators using PENA's identity, in the total amount of \$3,320.06.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 19

188. From on or about October 1, 2022, to on or about October 23, 2023, Nolte, at the direction of SUN, maintained an online persona using the name and PII of G.I., who Victim Company 19 employed.

189. From on or about October 1, 2022, to on or about October 23, 2023, Nolte, assuming the identity of G.I. repeatedly changed the banking information required for direct deposit and refused to travel to in-person work events held by Victim Company 19.

190. On or about October 23, 2023, as a result of G.I. being terminated, Nolte caused a shipment to be sent to Victim Company 19 containing a laptop owned by Victim Company 19.

191. From on or about October 2022 to October 2023, Nolte managed bank accounts held in the name of G.I., into which Victim Company 19 deposited approximately \$105,000 in pay.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 20

192. From on or about February 5, 2025, to on or about October 22, 2025, PENA was hired by Victim Company 20, for the benefit of overseas co-conspirators.

193. During the time of his employment, PENA caused to be deposited nineteen payroll checks from Victim Company 20, made payable to him for work done by overseas co-conspirators using his identity, in the total amount of \$71,627.62.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 21

194. On or about October 9, 2023, Nolte managed a fictitious persona, "R.R." who was hired by Victim Company 21 based on the fraudulent belief R.R. was a real person.

195. On or about October 7, 2023, Nolte and co-conspirators caused Victim Company 21 to send a laptop to a location in California allegedly maintained by R.R.

196. On or about October 9, 2023, an unknown individual loaded onto the laptop provided by Victim Company 21 Any Desk and software providing a virtual audio tunnel from the laptop to a remote laptop maintained by [REDACTED] using the moniker "[REDACTED]" [REDACTED]

197. Sometime during his period of employment, an individual posing as R.R. conducted an online meeting with Victim Company 21.

198. On or about July 17, 2024, [REDACTED] [REDACTED] sent Nolte a communication to confirm that Nolte received a check in the amount of \$7,508.28, in the name of R.R. dated June 27, 2024. Nolte confirmed the receipt of the check fraudulently obtained using R.R.'s identity.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 22

199. On or about February 15, 2024, GOLDLINE sent Nolte a communication confirming that Nolte received a payroll check from Victim Company 22 in the amount of \$10,560. Nolte confirmed the receipt of the check fraudulently obtained using the persona of J.B.

200. On or about February 24, 2024, Nolte caused Victim Company 22 to mail a package to Nolte, using the persona of J.B.

201. On or about March 13, 2024, Nolte caused Victim Company 22 to mail a package to Nolte, using the persona of J.B.

202. On or about March 13, 2024, Nolte received a payroll check from Victim Company 22 in the amount of \$8,640 and informed SUN via electronic communication.

203. On or about April 15, 2024, Nolte received a payroll check from Victim Company 22 in the amount of \$10,080 and informed SUN via an electronic communication.

204. On or about April 24, 2024, Nolte caused Victim Company 22 to mail a package to Nolte, using the persona of J.B.

205. On or about May 20, 2024, Nolte caused Victim Company 22 to mail a package to Nolte, using the persona of J.B.

206. On or about July 15, 2025, during the search of Nolte's residence, Nolte had a fictitious "authorization for deposit" form bearing the name of R.R. that Nolte used to deposit fraudulently issued checks into his personal account at BANK-1.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 23

207. On or about February 15, 2024, Nolte caused Victim Company 23 to issue a paycheck to the fictitious name of S.I., in the amount of \$4,102.60, mailed to Nolte's address in the Northern District of Ohio.

208. On or about July 8, 2024, Nolte caused Victim Company 23 to issue a paycheck to the fictitious name of S.I., in the amount of \$5,622.11, mailed to Nolte's address in the Northern District of Ohio.

209. On or about July 15, 2025, during the search of Nolte's residence, Nolte possessed a fictitious "authorization for deposit" form bearing the name of S.I. that Nolte used to deposit fraudulently issued checks into his personal account at BANK-1.

Use of Fraudulent Identifications to Gain and Maintain Employment with Company Victim 24

210. From approximately February 2024, to approximately February 2025, Nolte and [REDACTED] using the moniker "[REDACTED] [REDACTED]" used the fictitious name and identity of J.S. to gain employment with Victim Company 24.

211. On or about June 20, 2024, Nolte caused Victim Company 24 to issue a paycheck to the fictitious name of J.S., in the amount of \$4,432.80, with the note "Julio payroll," written on it, mailed to Nolte's address in the Northern District of Ohio.

212. On or about June 28, 2024, Nolte engaged in a chat with [REDACTED] [REDACTED] who confirmed that "J.S." was "sent by us."

213. During his period of employment, J.S. presented to Victim Company 24 a "medical accommodation form," seeking accommodation from using a video camera purportedly signed by his "psychologist S.I."

214. On or about July 15, 2025, during the search of Nolte's residence, Nolte possessed a fictitious "authorization for deposit" form bearing the name of J.S. that Nolte used to deposit fraudulently issued checks into his personal account at BANK-1.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 25

215. On November 1, 2022, Nolte caused Victim Company 25 to send a laptop and electronic devices to S.I., in care of B.B., both fictitious personae maintained by Nolte and used by [REDACTED] using the moniker "[REDACTED] [REDACTED]" an overseas co-conspirator.

216. On or about November 1, 2023, Nolte and [REDACTED] provided Victim Company 25 with a fraudulent passport, in the name of S.I., as verification for employment.

217. On or about April 28, 2023, Nolte caused Victim Company 25 to issue a paycheck to the fictitious name S.I. in the amount of \$4,809.90.

218. On or about May 12, 2023, Nolte engaged in a chat with [REDACTED] and sent [REDACTED] a photograph of the S.I. check issued by Victim Company 25, stating he "needed a signature for S.I."

219. On or about July 15, 2025, during the search of Nolte's residence, Nolte possessed a fictitious "authorization for deposit" form bearing the name of B.B. that Nolte used to deposit fraudulently issued checks into his personal account at BANK-1. Nolte also possessed a notecard with S.I. and B.B.'s names on it, the name of Victim Company 25, and other fraudulent user and employee names used during the criminal scheme.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 26

220. On or about January 29, 2023, in a chat between Nolte and [REDACTED] using the moniker "[REDACTED] [REDACTED]" Nolte provided photographs of a 2022 W-2 for B.B. issued by Victim Company 26, showing gross earnings of \$41,301.40.

221. On or about May 12, 2023, Nolte and [REDACTED] engaged in a chat in which Nolte wrote, "AnyDesk was removed and the laptop shut down," but could be re-installed when needed.

222. During that same conversation, Nolte asked [REDACTED] to sign several checks from Victim Company 26 in the fraudulent name "S.I."

223. On or about September 30, 2024, during a conversation between Nolte and [REDACTED] directed Nolte to load Zoom onto the laptop of Victim Company 26 and leave Zoom on for 24 hours to allow [REDACTED] to remotely access and control the laptop. screen and control sharing

224. On December 30, 2024, Nolte caused Victim Company 26 to issue a paycheck to the fictitious name of B.B. in the amount of \$4,731.21. That day, Nolte deposited the check into an account at BANK-1 he controlled.

225. From on or about January 14, 2025, to on or about January 16, 2025, Nolte sent at least three MTS transfers equaling \$3,184.79 to accounts controlled by overseas co-conspirators.

226. On or about July 15, 2025, Nolte possessed a fictitious "authorization for deposit" form bearing the name of B.B. that Nolte used to deposit fraudulently issued checks into his personal account at BANK-1. Nolte also possessed a notecard with B.B.'s name and other fraudulent user and employee names used during the criminal scheme.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 27

227. From on or about March 15, 2024, to on or about May 14, 2025, Nolte used the fictitious name T.H. to gain employment with Victim Company 27.

228. On or about March 15, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$9,731.76.

229. On or about July 12, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$9,731.76.

230. On or about August 16, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$5,923.68.

231. On or about September 27, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$5,923.68.

232. On or about October 8, 2024, Nolte deposited the check issued by Victim Company 27 on or about September 27, 2024, into an account at BANK-1 that he controlled.

233. On or about October 11, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$8,462.60.

234. On or about October 17, 2024, Nolte deposited the check issued by Victim Company 27 on or about October 11, 2024, into an account at BANK-1 that he controlled.

235. On or about November 13, 2024, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$8,885.53.

236. On or about December 4, 2024, 2024, Nolte deposited the check issued by Victim Company 27 on or about November 13, 2024, into an account at BANK-1 that he controlled.

237. On or about December 13, 2024, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$9,731.76.

238. On or about January 3, 2025, Nolte deposited the check issued by Victim Company 27 on or about December 13, 2024, into an account at BANK-1 that he controlled.

239. On or about May 14, 2025, Nolte caused Victim Company 27 to issue a paycheck to the fictitious name of T.H. in the amount of \$11,847.36. In the memo line of the check was the notation "payroll for 3/16-5/9/2025."

240. On or about July 15, 2025, during the search of Nolte's residence, Nolte had a fictitious "authorization for deposit" form bearing the name of T.H. that Nolte used to deposit fraudulently issued checks into his personal account at BANK-1.

Use of Fraudulent Identifications to Gain and Maintain Employment with Victim Company 28

241. On or about March 22, 2023, Nolte caused Victim Company 28 to issue a paycheck to the fictitious name of B.K. in the amount of \$4,035.62.

242. On or about April 7, 2023, Nolte caused Victim Company 28 to issue a paycheck to the fictitious name of B.K. in the amount of \$4,035.59.

243. On or about April 21, 2023, Nolte caused Victim Company 28 to issue a paycheck to the fictitious name of B.K. in the amount of \$4,035.62.

244. On or about July 15, 2025, Nolte possessed a 2023 W-2 for B.K., issued by Victim Company 28, showing gross earnings of \$41,301.40. Nolte also possessed mail, paystubs and other documents in the name of B.K. from Victim Company 28.

Fraudulent Use of the U.S. Mail

245. On or about the following dates, overseas co-conspirators caused packages containing laptops and other items belonging to U.S. victim companies to be delivered via the U.S. mail and private postal carriers to Nolte's residence in the Northern District of Ohio, all in the names of the following stolen and fraudulently assumed U.S. persons identities:

Sub ¶	Shipping Date	Delivery Date	Recipient Identity	Type of Mailing
246.	05/26/23	05/30/23	A.S.	FedEx
247.	06/01/23	06/02/23	J.B.	FedEx
248.	06/01/23	06/02/23	J.B.	FedEx
249.	07/06/23	07/11/23	M.F.	FedEx
250.	7/7/2023		M.F.	FedEx
251.	7/12/2023		M.F.	FedEx
252.	7/22/2023		Trey Nolte	FedEx

Sub ¶	Shipping Date	Delivery Date	Recipient Identity	Type of Mailing
253.	10/9/2023		Trey Nolte	FedEx
254.	10/10/23	10/12/23	Trey Nolte	FedEx
255.	10/13/2023		Trey Nolte	FedEx
256.	12/01/23	12/04/23	J.B.	FedEx
257.	12/01/23	12/04/23	J.B.	FedEx
258.	1/17/2024		J.B.	FedEx
259.	2/6/2024		M.A.	FedEx
260.	02/14/24	02/15/24	C.B.	FedEx
261.	02/24/24	02/26/24	J.B.	FedEx
262.	03/13/24	03/14/24	J.B.	FedEx
263.	3/30/2024		Trey Nolte	FedEx
264.	3/30/2024		Trey Nolte	FedEx
265.	3/30/2024		Trey Nolte	FedEx
266.	3/30/2024		Trey Nolte	FedEx
267.	04/09/24	04/10/24	B.K.	FedEx
268.	4/15/2024		C.B.	FedEx
269.	04/24/24	04/26/24	J.B.	FedEx
270.	04/29/24	05/01/24	Michael Bostelle	FedEx
271.	05/20/24	05/21/24	J.B.	FedEx
272.	07/10/24	07/12/24	Trey Nolte	FedEx
273.	08/15/24	08/16/24	D.G.	FedEx
274.	09/04/24	09/05/24	D.G.	FedEx
275.	09/10/24	09/11/24	J.B.	FedEx
276.	09/26/24	09/28/24	C.B.	FedEx
277.	9/27/2024		Trey Nolte	FedEx
278.	10/1/2024		Trey Nolte	FedEx
279.	10/15/2024		C.B.	FedEx
280.	11/21/24	11/25/24	Trey Nolte	FedEx
281.	11/27/24	12/03/24	D.G.	FedEx
282.	12/04/24	12/06/24	Trey Nolte	FedEx
283.	12/12/2024		Trey Nolte	FedEx
284.	12/16/24	12/18/24	Trey Nolte	FedEx
285.	12/20/2024		M.A.	FedEx
286.	01/14/25	01/16/25	Trey Nolte	FedEx
287.	5/13/2025		M.A.	FedEx
288.	05/16/25	05/19/25	D.G.	FedEx
289.	5/20/2025		MICHAEL BOSTELLE	FedEx
290.	5/20/2025		MICHAEL BOSTELLE	FedEx
291.	5/20/2025		MICHAEL BOSTELLE	FedEx
292.	5/22/2025		Trey Nolte	FedEx

Sub ¶	Shipping Date	Delivery Date	Recipient Identity	Type of Mailing
293.	06/02/25	06/04/25	S.B.	FedEx
294.	06/03/25	06/04/25	Trey Nolte	FedEx
295.	7/3/2024	07/05/24		DHL

296. On or about February 21, 2022, Nolte sent a package via DHL to PEI LI GUANG containing, among other items, two laptops with chargers obtained from victim companies who hired fictitious employees.

297. On April 18, 2023, Nolte sent a package via DHL to WENG SHOU CHENG containing, among other items, four MacBooks obtained from victim companies who hired fictitious employees based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED] [REDACTED]

298. On April 18, 2023, Nolte sent another package via DHL to WENG SHOU CHENG containing, among other items, an iPhone, a laptop, and a headset obtained from victim companies who hired fictitious employees based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED]
[REDACTED]

299. On April 26, 2023, Nolte sent a package via DHL to WENG SHOU CHENG containing, among other items, a laptop obtained from a victim company who hired a fictitious employee based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED] [REDACTED]

300. On May 3, 2023, Nolte sent a package via DHL to WENG SHOU CHENG containing, among other items, a laptop and iPhone obtained from a victim company who hired fictitious employees based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] and [REDACTED] [REDACTED]

301. On May 16, 2023, Nolte sent a package via DHL to WENG SHOU CHENG containing, among other items, a laptop obtained from a victim company who hired a fictitious employee based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] and [REDACTED]

302. On May 23, 2023, Nolte sent a package via DHL to WENG SHOU CHENG containing, among other items, a laptop obtained from a victim company who hired a fictitious employee based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] and [REDACTED]

303. On June 27, 2023, Nolte sent a package via DHL to WENG SHOU CHENG containing, among other items, a laptop obtained from a victim company who hired a fictitious employee based on the scheme controlled by SUN SHENG MING, PEI LI GUANG, WENG SHOU CHENG, [REDACTED] and [REDACTED]

304. 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 PENA's residence in the Southern District of Texas, in the names of the following stolen and fraudulently assumed U.S. persons identities:

	Shipping Date	Delivery Date	Recipient Identity	Type of Mailing
305	02/27/24	2024-02-28	R.D.	FedEx
306	02/27/24	2024-02-28	R.D.	FedEx
307	02/27/24	2024-02-28	R.D.	FedEx
308	02/28/24	2024-02-29	R.D.	FedEx
309	03/01/24	2024-03-04	K.F.	FedEx

¶	Shipping Date	Delivery Date	Recipient Identity	Type of Mailing
310	08/06/24	2024-08-08	J.L.	FedEx
311	01/23/25	2025-01-24	JUAN PENA	FedEx
312	02/07/25	2025-02-10	JUAN PENA	FedEx
313	02/21/25	2025-02-25	JUAN PENA	FedEx
314	03/28/25	2025-04-01	JUAN PENA	FedEx
315	04/15/25	2025-04-17	JUAN PENA	FedEx
316	04/15/25	2025-04-17	JUAN PENA	FedEx
317	04/16/25	2025-04-18	JUAN PENA	FedEx
318	04/16/25	2025-04-18	JUAN PENA	FedEx
319	04/16/25	2025-04-18	JUAN PENA	FedEx
320	04/16/25	2025-04-18	JUAN PENA	FedEx
321	04/16/25	2025-04-18	JUAN PENA	FedEx
322	04/18/25	2025-04-21	JUAN PENA CARRILLO	FedEx
323	05/13/25	2025-05-14	JUAN PENA CARRILLO	FedEx
324	05/16/25	2025-05-17	Juan Pena	FedEx
325	05/19/25	2025-05-21	JUAN PENA CARRILLO	FedEx
326	01/18/24		R.H.	UPS
327	11/21/23		L.d.l.G.	UPS
328	04/20/23		R.H.	UPS
329	11/03/22		A.M.	UPS
330	10/11/22		F.A.	UPS

¶	Shipping Date	Delivery Date	Recipient Identity	Type of Mailing
331	02/28/23		A.M.	UPS
332	01/04/24		S.R.	UPS
333	03/17/25		JUAN PENA	UPS
334	03/17/25		JUAN PENA	UPS
335	03/17/25		JUAN PENA	UPS
336	04/08/25		JUAN PENA	UPS
337	04/08/25		JUAN PENA	UPS
338	04/09/25		JUAN PENA	UPS
339	04/09/25		JUAN PENA	UPS
340	05/12/25		JUAN PENA	UPS
341	05/12/25		JUAN PENA	UPS
342	09/19/25		JUAN CECILIO PENA	UPS

The Fraudulent Use of Bank and other Financial Accounts

343. On or about December 12, 2021, Nolte and SUN, using the moniker “GOLDLINE,” had a conversation in which SUN directed Nolte to complete tax and citizenship forms in the name of S.R., a fraudulent employee receiving payroll checks in the scheme to defraud. Nolte received these forms from a notary by mail who improperly notarized the signatures. Included in the information Nolte affirmed was a Social Security number, driver’s license number and other information for S.R., provided to him by SUN.

344. On or about September 26, 2022, Nolte and SUN, using the moniker “GOLDLINE,” had a conversation in which Nolte described having to forge signatures of

fraudulent employees, including B.B., in order to deposit their payroll checks into Nolte's account, so that funds could be sent to SUN and other overseas co-conspirators.

345. On or about January 26, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to allow SUN to use Nolte's bank account to receive wire transfers, and then transfer the funds through MTS-1 and MTS-2 to SUN.

346. On or about March 1, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to handle a customer service issue with an existing MTS-3 account in the name of C.B., by using C.B.'s identifiers including a Social Security number, date of birth, email and telephone number.

347. On or about March 9, 2023, Nolte and SUN, using the moniker "GOLDLINE," had a conversation in which SUN directed Nolte to link an existing bank account to an MTS-3 account for use by SUN and directed Nolte to send \$2,000.00 to GOLDENCENTAUR.

348. On or about December 20, 2023, Nolte and LONG, using the moniker "PATRICK BONNER," had a conversation in which LONG directed Nolte to use various MTS, including MTS-1 and MTS-4, or crypto accounts to send to LONG or GOLDLINE (SUN).

349. On or about March 15, 2024, Nolte and [REDACTED] using the moniker "[REDACTED] [REDACTED]" engaged in a chat in which Nolte explained to [REDACTED] that he, Nolte, also works with SUN's team of overseas programmers and further explained to [REDACTED] the fee structure SUN used, and stated that he (Nolte) expected from [REDACTED] a similar fee structure in future dealings.

350. Additionally, on or about January 23, 2025, Nolte and [REDACTED] using the moniker "[REDACTED] [REDACTED]" had a conversation in which [REDACTED] explained that if any bank challenged Nolte's deposits of checks made out to fraudulent employees, Nolte could

direct them to [REDACTED] SUN or [REDACTED] who would pose as authorized representatives for the companies. Additionally, [REDACTED] directed Nolte not to mention Nolte received money for monitoring computers “because some companies don’t like this.”

351. On or about March 15, 2024, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker “[REDACTED] [REDACTED]” instructed Nolte to initiate a money transfer using MTS-1, and then to a virtual currency, using an account opened by [REDACTED] using the moniker “GOLDENCENTAUR55.”

352. On or about July 8, 2024, during a conversation between Nolte and [REDACTED] using the moniker “[REDACTED] [REDACTED]” Nolte explained how he created spreadsheets to manage the transfer of funds between bank accounts and virtual currencies, and then the transfer of those funds to SUN, [REDACTED] and [REDACTED] in a way that maximized the amounts that can be sent in one transaction.

353. On or about September 8, 2024, during a conversation between Nolte and [REDACTED] using the moniker “[REDACTED] [REDACTED] [REDACTED]” directed Nolte to initiate a transfer using MTS-1.

354. On or about January 17, 2025, during a conversation between Nolte and [REDACTED] [REDACTED] using the moniker “[REDACTED] [REDACTED]” directed Nolte to create and send a list of overseas co-conspirators using Nolte’s bank accounts and the activity for those accounts for the past 30 days.

Use of Fraudulent Deposit Permissions with BANK-1

355. On or about July 1, 2024, during a conversation between Nolte and [REDACTED] using the moniker “[REDACTED] [REDACTED]” Nolte expressed to [REDACTED] difficulty managing both [REDACTED] [REDACTED] and GOLDLINE’s personas, along with all of the

accompanying benefits mail for each fraudulent employee and the need to forge “complicated” signatures for every paycheck because he was not a “professional forgery person.” In response, [REDACTED] offered to send some fraudulent signatures.

356. On or about March 15, 2024, Nolte and LONG, using the moniker “PATRICK BONNER,” had a conversation in which LONG provided Nolte with information concerning an incoming payroll check in the name of the fraudulent employee D.G. Nolte expressed concern about depositing a check in another person’s name into his account, but then assured LONG that he would deposit the check.

357. On or about July 3, 2024, during a conversation between Nolte and [REDACTED] using the moniker “[REDACTED] [REDACTED] [REDACTED]” sent Nolte forms he could present to banks that were in the names of fraudulent employees that would give Nolte the ability to deposit fraudulent employee paychecks into Nolte-controlled accounts.

358. On or about September 24, 2024, Nolte and LONG, using the moniker “PATRICK BONNER,” had a conversation in which LONG confirmed that everyone Nolte sends money to overseas using MTS or cryptocurrency transfers works for SUN; LONG also instructed Nolte to continue to find a way to deposit the checks of fraudulent employees into Nolte’s bank account without raising concerns by bank employees.

359. Consistent with these conversations, Nolte presented to BANK-1 twelve “authorizations for deposit, withdrawal and endorsement” in the names of fictitious employee identities, purportedly to allow for Nolte to deposit physical checks sent by employers to fictitious employees.

360. On the occasions identified below, Nolte used the fraudulent permissions to deposit payroll checks sent to him in the name of fictitious employees into his account at BANK-

1:

Fraudulent Employee	Date on Check	Date Deposited	Amount of Check
D.G.	8/30/2024	9/5/2024	\$3,840.89
D.G.	8/30/2024	9/6/2024	\$4,617.49
C.B.	9/20/2024	10/1/2024	\$3,425.73
T.H.	9/27/2024	10/8/2024	\$5,923.68
T.H.	10/11/2024	10/17/2024	\$8,462.40
B.C.	11/19/2024	11/26/2024	\$10,378.71
S.W.	11/7/2024	12/2/2024	\$4,292.10
T.H.	11/13/2024	12/4/2024	\$8,885.52
B.C.	11/19/2024	12/9/2024	\$10,378.71
B.C.	11/29/2024	12/20/2024	\$3,459.57
B.C.	12/13/2024	1/2/2025	\$3,459.57
T.H.	12/13/2024	1/3/2025	\$9,731.76
B.B.	12/18/2024	1/3/2025	\$4,731.21
D.A.	12/10/2024	1/17/2025	\$5,025.38

361. Nolte also deposited thirteen additional payroll checks sent to him for fictitious employees via BANK-1's mobile banking application:

Date Deposited	Amount
8/19/2024	\$4,617.49
8/26/2024	\$6,424.77
9/3/2024	\$1,965.00
9/9/2024	\$736.87
9/30/2024	\$485.00
10/2/2024	\$2,545.00
11/1/2024	\$2,947.50
11/29/2024	\$1,768.50
12/17/2024	\$5,323.20
12/27/2024	\$5,323.18
1/10/2025	\$5,323.74
1/13/2025	\$3,876.70
1/13/2025	\$4,731.21

362. The total amount of deposits of paychecks issued to fictitious employees into BANK-1 by Nolte totaled \$119,673.12.

Transfer of Fraudulent Employee Payroll Deposits Through BANK-4

363. Nolte also maintained an account at BANK-4 in the account name “Dark Falls, LLC,” a company Nolte created. At the time of opening, Nolte provided BANK-4 the following statement of his business for their Know Your Customer requirements: “A remote service company, where people send laptops and they are kept operational and connected.”

364. From on or about September 3, 2024, until on or about November 15, 2024, Nolte deposited a total of \$42,585.55, collected as payroll for fraudulent employee B.K., into his account at BANK-4.

365. From on or about September 4, 2024, until on or about November 15, 2024, BANK-4 identified eight transfers totaling \$41,106.74 from the Dark Falls, LLC bank account to an account at MTS-6 in the name of Nolte and one transfer from BANK-1 in the amount of \$485, for a total of nine transfers totaling \$41,591.74.

Use of MTS-3 to Transfer Money Fraudulently Earned Using Fraudulent Identities

366. On or about February 8, 2023, using an IP address traced back to him, Nolte opened an account with MTS-3 to receive pay from Victim Company #1 and other victim companies in the name of BOSTELLE.

367. From on or about January 3, 2023, to on or about April 15, 2024, Nolte deposited 32 payroll checks from Victim Company 1, made out to fraudulent employees, totaling approximately \$157,271.43.

368. From on or about March 8, 2023, to on or about May 24, 2025, the MTS-3 account controlled by Nolte received \$158,675.54 in deposits from victim company payroll

accounts and transfers from accounts controlled by Nolte at BANKs 2, 3 and 4. During that same time period, Nolte transferred \$132,107.42 to MTS accounts based outside of the United States, including \$131,897.03 to accounts based in China, all controlled by co-conspirators.

369. In total from the above transactions with BANK-2, BANK-4 and BANK-1, Nolte accepted over \$320,000 in bank accounts opened in false or fictitious names and transmitted that money to overseas and domestic bank accounts to further the criminal scheme, avoid reporting requirements and profit personally through fraudulent activity.

PENA's Use of MTS-3 and MTS-4

370. From on or about February 2, 2025, to on or about February 3, 2026, PENA maintained an account with MTS-3.

371. From on or about February 2, 2025, to on or about February 3, 2026, PENA caused to be deposited into MTS-3 approximately \$190,510.39 in fraudulent employee payroll payments from Victim Companies 5, 7, 17, 18 and 20.

372. From on or about February 2, 2025, to on or about February 3, 2026, PENA transferred from MTS-3 to MTS-4 approximately \$155,204.80 for the benefit of overseas co-conspirators.

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

COUNT 2
(Money Laundering Conspiracy, 18 U.S.C. § 1956(h))

The Grand Jury further charges:

373. Paragraphs 1-83 and 87-372 of the Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

374. From on or about February 1, 2019, to on or about January 21, 2026, in the Northern District of Ohio and elsewhere, the defendants, SUN SHENG MING , aka 孙圣明; PEI

LI GUANG; WENG SHOU CHENG; [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬;
WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN; ZHANG WEI PING, aka 张卫平;
ZHANG LI PING; YU YANG, aka 于洋; JIN LONG; [REDACTED] [REDACTED] MICHAEL
JAMES BOSTELLE; and JUAN CECILIO PENA CARRILLO conspired together 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);
- (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);

- (c) to transport, transmit and transfer and attempt to transport, transmit and transfer a monetary instrument and funds involving the proceeds of specified unlawful activity, that is, Wire Fraud, in violation of 18 U.S.C. § 1343; Mail Fraud, in violation of 18 U.S.C. § 1341; Identity Theft, in violation of 18 U.S.C. § 1028; and, Aggravated Identity Theft, in violation of 18 U.S.C § 1028A, from a place in the United States to and through a place outside the United States, knowing that the funds involved in the transportation, transmission and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission and transfer was 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 18 U.S.C. § 1956(a)(2)(B)(i);. and,
- (d) to transport, transmit and transfer and attempt to transport, transmit and transfer a monetary instrument and funds involving the proceeds of specified unlawful activity, that is, Wire Fraud, in violation of 18 U.S.C. § 1343; Mail Fraud, in violation of 18 U.S.C. § 1341; Identity Theft, in violation of 18 U.S.C. § 1028; and, Aggravated Identity Theft, in violation of 18 U.S.C § 1028A, from a place in the United States to and through a place outside the United States, knowing that the funds involved in the transportation, transmission and transfer represented the proceeds of some form of unlawful activity and knowing that the transportation is designed

in whole or part to avoid a transaction reporting requirement under state or federal law, in violation of 18 U.S.C. § 1956(a)(2)(B)(ii).

All in violation of Title 18, United States Code, Section 1956(h).

COUNT 3

(Conspiracy to Commit Identity Theft, 18 U.S.C. §§ 1028(a)(7) and (f) and 2)

The Grand Jury further charges:

379. Paragraphs 1-83 and 87-372 of the Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

380. From on or about February 1, 2019, to on or about January 21, 2026, in the Northern District of Ohio and elsewhere, the defendants SUN SHENG MING, aka 孙圣明; PEI LI GUANG, WENG SHOU CHENG, [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬; WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN, ZHANG WEI PING, aka 张卫平; ZHANG LI PING, YU YANG, aka 于洋; JIN LONG, [REDACTED] [REDACTED] MICHAEL JAMES BOSTELLE, and JUAN CECILIO PENA CARRILLO did knowingly combine, conspire, and agree together and with 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, 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 2.

COUNT 4
(Aggravated Identity Theft, 18 U.S.C. §§ 1028A(a)(1) and 2)

The Grand Jury further charges:

381. Paragraphs 1-83 and 87-372 of the Indictment are hereby re-alleged and incorporated by reference as if fully set forth herein.

382. From on or about December 11, 2023 to on or about September 25, 2025, in the Northern District of Ohio and elsewhere, Defendants SUN SHENG MING, aka 孙圣明; PEI LI GUANG, WENG SHOU CHENG, and JUAN CECILIO PENA CARRILLO did knowingly combine, conspire, and agree together and with 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 name, Social Security number, dates of birth, passport number, and state issued driver's license and identification number, 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 1028A(a)(1) and 2.

FORFEITURE ALLEGATIONS

The Grand Jury further charges:

383. Upon conviction of the offense in violation of Title 18, United States Code, Section 1349, set forth in Count One, the defendants SUN SHENG MING, aka 孙圣明; PEI LI GUANG; WENG SHOU CHENG; [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬; WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN; ZHANG WEI PING, aka 张卫平;

ZHANG LI PING; YU YANG, aka 于洋; JIN LONG; [REDACTED] [REDACTED] MICHAEL JAMES BOSTELLE; and JUAN CECILIO PENA CARRILLO 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.

384. Upon conviction of the offense in violation of Title 18, United States Code, Section 1956(h), set forth in Count Two, the defendants SUN SHENG MING , aka 孙圣明; PEI LI GUANG; WENG SHOU CHENG; [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬; WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN; ZHANG WEI PING, aka 张卫平; ZHANG LI PING; YU YANG, aka 于洋; JIN LONG; [REDACTED] [REDACTED]; MICHAEL JAMES BOSTELLE; and JUAN CECILIO PENA CARRILLO 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.

385. Upon conviction of the offense in violation of Title 18, United States Code, Section 1028(a)(7), (f) and 2, set forth in Count Three, the defendants SUN SHENG MING , aka 孙圣明; PEI LI GUANG; WENG SHOU CHENG; [REDACTED] [REDACTED] HAN GUO BIN, aka 韩国彬; WANG JIAN JUN, aka 王建钧; SHENG ZHANG KUN; ZHANG WEI PING, aka 张卫平; ZHANG LI PING; YU YANG, aka 于洋; JIN LONG; [REDACTED] [REDACTED] MICHAEL JAMES BOSTELLE; and JUAN CECILIO PENA CARRILLO 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.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.

United States v. Sun Sheng Ming, aka 孙圣明, et al.

A TRUE BILL.

FOREPERSON

DAVID M. TOEPFER
United States Attorney

By:

Daniel J. Riedl, Chief
National Security Unit