U.S. Department of
JUSTICE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

25-CR-20021-GAYLES/GOODMAN

Case No. _____

18 U.S.C. § 371
18 U.S.C. § 1349
18 U.S.C. § 1956(h)
18 U.S.C. § 1028(a)(2), (f)
50 U.S.C. § 1705(a), (c)
18 U.S.C. § 981(a)(1)(C)
18 U.S.C. § 982(a)(1)
18 U.S.C. § 982(a)(2)(B)
18 U.S.C. § 982(b)
18 U.S.C. § 1028(b)(5)
18 U.S.C. § 1030(i)

UNITED STATES OF AMERICA

vs.

JIN SUNG-IL,
a/k/a "진성일,"
a/k/a "Jin Song-Il,"
a/k/a "Pedro Alonso,"
a/k/a "Richard Stewart,"
a/k/a "Stewart Conn,"
a/k/a "Kelsey Bane,"
PEDRO ERNESTO ALONSO DE LOS REYES,
ERICK NTEKEREZE PRINCE,
a/k/a "Eric Prince",
PAK JIN-SONG,
a/k/a "박진성,"
a/k/a "Glaus Li,"
and
EMANUEL ASHTOR,
a/k/a "Ndagijimana Emmanuel,"

Defendants.
_____/

INDICTMENT

The Grand Jury charges that:

GENERAL ALLEGATIONS

At all times relevant to this Indictment, unless alleged otherwise:

Background on North Korean IT Workers

1. The United States maintained comprehensive trade and economic sanctions against the Democratic People's Republic of Korea (the "DPRK" or "North Korea"), due to the national security threats posed by North Korea, including its nuclear weapons program. The sanctions had the effect of cutting off North Korea from the U.S. marketplace and financial system, restricting the ability of U.S. persons and companies from doing business and otherwise transacting with North Korea. As a result, North Korea sponsored various schemes to evade U.S. sanctions to generate funds for the regime.

2. According to a May 2022 advisory by the Department of State, the Department of the Treasury, and the Federal Bureau of Investigation ("FBI"), North Korea dispatched thousands of highly skilled information technology ("IT") workers around the world to generate revenue that contributed to North Korea's weapons programs in violation of U.S. and United Nations sanctions. These North Korean IT workers posed as non-North Korean foreign and U.S.-based remote workers and surreptitiously obtained contracts for remote IT work from companies around the world, including in the United States. According to the same advisory, North Korean IT workers could individually earn more than $300,000 a year in some cases, and teams of IT workers could collectively earn more than $3 million annually. The North Korean government withheld up to 90 percent of wages of overseas workers, which generated an annual revenue to the North Korean government of hundreds of millions of dollars.

3. North Korean IT workers commonly obtained these remote IT work contracts through online platforms that allowed companies to advertise contracts for IT projects on which freelance IT workers could bid. North Korean IT workers provided prospective employers with counterfeit, altered, or falsified documents, including identification documents, to hide their true identities. To obtain these documents, North Korean IT workers commonly paid individuals and websites for document forgery services or altered authentic identity documents by combining a photo of the North Korean IT worker with the personally identifiable information, such as names, social security numbers, dates of birth, among other information ("PII") of another person, including U.S. persons.

4. DPRK IT workers used remote desktop software to access U.S.-based computers so that it appeared they were performing their work from U.S.-based locations. Remote desktop software applications allowed a computer to remotely run another computer's desktop environment. The remote connection between devices was established and maintained through the Internet.

5. North Korean IT workers further obfuscated their identities, locations, and nationality by using virtual private networks ("VPNs") and virtual private servers ("VPSs"). A VPN was a network of dedicated servers, run by a VPN service, that encrypted a user's Internet traffic; that is, the information sent from the user's computer across the Internet. VPN services maintained servers in different locations worldwide, enabling their users to mask their true geolocation by accessing the Internet through a VPN that is in a different location.

6. DPRK IT workers were aided in this fraud by both U.S. and foreign facilitators. According to a May 2024 advisory by the FBI, North Korean IT workers obfuscated their identities

by leveraging U.S.-based individuals, both witting and unwitting, to gain fraudulent employment and access to U.S. company networks. These U.S.-based enablers provided a U.S. address for victim companies to send laptop computers and other devices, enabling the North Korean IT workers to circumvent controls companies had in place to prevent hiring illicit, overseas workers and prevent unauthorized access or damage to company networks. After receiving a device, the U.S. enablers used credentials provided by either the North Korean IT worker or the victim company to log in to the device and install remote access software without authorization. Sometimes enablers allowed the North Korean IT workers to apply for remote IT positions using their names and identity documents. Enablers performed these activities in exchange for a fee, which was typically paid to them through online money transfer and digital payment services. DPRK IT workers' favored payment platforms that specialized in facilitating cross-border business-to-business payments, cross-border wire transfers, online payments, and refillable debit card services.

The International Emergency Economic Powers Act

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

8. Pursuant to IEEPA, the President and the Executive Branch issued Executive Orders and regulations, respectively, governing and prohibiting certain transactions involving North Korea. Specifically, on June 26, 2008, the President issued Executive Order 13466, finding that that "the existence and risk of the proliferation of weapons-usable fissile material on the Korean Peninsula constituted an unusual and extraordinary threat to the national security and foreign policy of the United States" and declared a "national emergency to deal with that threat." The President imposed additional sanctions with respect to North Korea. *See* Executive Orders 13551 (Aug. 30, 2010), 13570 (Apr. 18, 2011), 13722 (Mar. 15, 2016), and 13810 (Sept. 20, 2017). To implement those Executive Orders, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued the North Korean Sanctions Regulations (the "NKSR"). 31 C.F.R. Part 510.

9. On March 15, 2016, the President took additional steps with respect to the national emergency described in Executive Order 13466 and issued Executive Order 13722 to address the Government of North Korea's continuing pursuit of its nuclear and missile programs. Pursuant to Executive Order 13722, OFAC had the authority to block all property and interests in property of the Government of North Korea and the Workers' Party of Korea. As a result, U.S. persons, including U.S. financial institutions and companies, were generally prohibited from transacting with North Korea.

10. On March 5, 2018, OFAC amended and reissued the NKSR in their entirety to implement Executive Order 13722, among others. 83 Fed. Reg. 9182 (Mar. 5, 2018). Absent a license from OFAC, the NKSR prohibited, among other things, the exportation or re-exportation, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods,

services, or technology to North Korea. 31 C.F.R. § 510.206(a); *see also* Executive Order 13722 § 3. This prohibition applied to services, including financial services, performed on behalf of a person in North Korea or the Government of North Korea or where the benefit of such services was otherwise received in North Korea. 31 C.F.R. § 510.405. Additionally, the benefit of services performed anywhere in the world on behalf of the North Korean government was presumed to be received in North Korea. *Id.* The NKSR also prohibited any transaction that evaded or avoided, had the purpose of evading or avoiding, caused a violation of, attempted to violate, or any conspiracy formed to violate any of the prohibitions set forth in the NKSR. 31 C.F.R. § 510.212; *see also* Executive Order 13722 § 7.

The Defendants

11. Defendant **JIN SUNG-IL**, a/k/a **Jin Song-Il**, a/k/a 진성일, was a North Korean IT worker residing in Liaoning Province, China.

12. Defendant **PEDRO ERNESTO ALONSO DE LOS REYES** was a Mexican citizen residing in Sweden.

13. Defendant **ERICK NTEKEREZE PRINCE**, a/k/a **Erick Ntekereze**, was a United States citizen residing in New York and the owner of Taggcar Inc.

14. Defendant **PAK JIN-SONG**, a/k/a 박진성, was a North Korean IT worker residing in Liaoning Province, China.

15. Defendant **EMANUEL ASHTOR**, a/k/a **Ndagijimana Emmanuel**, was a United States citizen residing in New York and, later, North Carolina, and one of the owners of Vali Tech Inc.

Relevant Entities and Victims

16. Taggcar Inc. was a Delaware company that acted as a staffing agency to provide other companies with remote contract IT workers in the United States.

17. Vali Tech Inc. was a Florida company that acted as a staffing agency to provide other companies with remote contract IT workers in the United States.

18. Company A was a multinational retail corporation headquartered in the United States.

19. Company B was a U.S. financial institution headquartered in Stamford, Connecticut.

20. Company C was an international cruise line headquartered in Miami, Florida.

21. Company D was a U.S. technology company headquartered in San Francisco, California.

22. U.S. Staffing Company 1 was a staffing and recruiting firm located in Deer Park, Illinois.

23. U.S. Staffing Company 2 was a staffing and recruiting firm headquartered in Santa Clara, California.

24. U.S. Staffing Company 3 was a staffing and recruiting firm headquartered in Fort Lauderdale, Florida.

25. U.S. IT Company 1 was an IT company headquartered in Palo Alto, California.

26. U.S. IT Company 2 was an IT company headquartered in Milpitas, California.

27. Online Payment Platform 1 was an online payment company headquartered in New York, New York.

28. Online Payment Platform 2 was an online payment company headquartered in the United Kingdom.

29. Anydesk Software GmbH was a software company that provided a remote desktop application called Anydesk, which allowed users to access and control a computer located in a different location, and is headquartered in Stuttgart, Germany.

30. TeamViewer Germany GmbH was a software company that provided a remote desktop application called TeamViewer, which allowed users to access and control a computer located in a different location, and is headquartered in Goeppingen, Germany.

31. U.S. Victim 1 was a U.S. citizen whose identity the co-conspirators stole and used to fraudulently obtain remote IT work.

COUNT 1
Conspiracy to Damage a Protected Computer
(18 U.S.C. § 371)

1. The General Allegations section of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

2. From as early as in or around April 2018, the exact date being unknown to the Grand Jury, and continuing through in or around August 2024, in Miami-Dade and Broward Counties, in the Southern District of Florida, and elsewhere, the defendants,

JIN SUNG-IL,
a/k/a "진성일,"
a/k/a "Jin Song-Il,"
a/k/a "Pedro Alonso,"
a/k/a "Richard Stewart,"
a/k/a "Stewart Conn,"
a/k/a "Kelsey Bane,"
PEDRO ERNESTO ALONSO DE LOS REYES,
ERICK NTEKEREZE PRINCE,

a/k/a "Eric Prince,"
PAK JIN-SONG,
a/k/a "박진성,"
a/k/a "Glaus Li,"
and
EMANUEL ASHTOR,
a/k/a "Ndagijimana Emmanuel,"

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

OBJECT AND PURPOSE OF THE CONSPIRACY

3. It was the object and purpose of the conspiracy for **JIN SUNG-IL, PEDRO ERNESTO ALONSO DE LOS REYES, ERICK NTEKEREZE PRINCE, PAK JIN-SONG, EMANUEL ASHTOR,** and their co-conspirators (collectively, the "co-conspirators") to unlawfully enrich themselves and raise revenue for the North Korean regime by: (a) obtaining employment at U.S. companies for remote IT work under false and fraudulent pretenses, representations, promises, and by making material omissions; (b) causing the unauthorized transmission of a program, information, code, or command, on U.S. companies' protected computers; (c) performing remote IT work to fraudulently earn salary payments from victim U.S.

companies; (d) making false statements and engaging in other fraudulent activities designed to conceal the commission of the offense; and (e) laundering the fraudulently obtained salary payments by conducting financial transactions designed to promote the carrying on of unlawful activity and to conceal or disguise the nature or source of the proceeds of unlawful activity.

MANNER AND MEANS OF THE CONSPIRACY

The manner and means by which the co-conspirators sought to accomplish the object and purpose of the conspiracy included, among others, the following:

4. **JIN SUN-IL, PEDRO ERNESTO ALONSO DE LOS REYES, ERICK NTEKEREZE PRINCE, PAK JIN-SONG, EMANUEL ASHTOR**, and their co-conspirators registered U.S. companies, including Taggcar Inc. and Vali Tech Inc., to obtain corporation-to-corporation employment contracts (*i.e.*, an agreement between two (or more) businesses for services, rather than an agreement between a business and an employee (or contractor) for services).

5. As part of the conspiracy, the co-conspirators identified U.S. companies seeking remote IT workers and successfully applied for remote IT work positions at the victim companies, including Company A, Company B, Company C, and Company D. To conceal the true identities of the North Korean IT workers, including **JIN SUNG-IL** and **PAK JIN-SONG**, and obtain employment, the co-conspirators provided the victim companies with forged identity documents and other false information, including U.S. passports containing the pictures of North Korean IT workers and the PII of U.S. persons, including U.S. Victim 1.

6. As part of their fraudulently obtained employment with U.S. based companies, the co-conspirators received U.S. victim company-provided laptops ("victim laptops") at **ERICK**

NTEKEREZE PRINCE's and **EMANUEL ASHTOR's** residences. **PRINCE** and **ASHTOR** then accessed, without authorization, victim laptops and mobile devices in order to download, without authorization, remote desktop applications, which enabled the co-conspirators, including **JIN SUNG-IL** and **PAK JIN-SONG**, to remotely access victim laptops by turning them on, logging in, installing software, and executing other commands on such devices without authorization.

7. As part of the conspiracy and in furtherance of the scheme to defraud, members of the conspiracy created accounts with U.S. banks and online payment platforms, including Online Payment Platform 1, to receive salary payments from the U.S. companies in exchange for the fraudulently obtained remote IT work. In some instances, members of the conspiracy, through their fraudulent scheme, caused U.S. victim companies to send the salary payments to U.S. bank accounts associated with Taggcar Inc. and Vali Tech Inc. The co-conspirators, in turn, transferred large portions of those funds (minus funds retained by **ERICK NTEKEREZE PRINCE** and **EMANUEL ASHTOR**) to online payment platform accounts registered to identified individuals claiming to live in, among other places, Dandong, China. In other instances, members of the conspiracy caused U.S. Victim companies to send payments directly to members of the conspiracy via online payment platforms.

8. During the course of the conspiracy, the co-conspirators fraudulently obtained remote IT work from at least 64 U.S. companies, with payments from ten U.S. companies, including Company A, Company B, and Company D, totaling approximately $866,255, some of which was laundered through Online Payment Platform 1 accounts. During the course of the

conspiracy, an Online Payment Platform 1 account belonging to one of the China-based financial facilitators deposited at least $677,440 into a Chinese bank account.

9. During the course of the conspiracy, the co-conspirators caused damage and loss to victim companies, with the value of such harms exceeding a total of $1 million for Company B, Company D, and U.S. IT Company 1. The loss resulting from the co-conspirators' conduct included the costs borne by the victim companies for legal fees and to remediate computer networks and devices.

10. During the course of the conspiracy and as a direct result of his participation in the conspiracy, **ERICK NTEKEREZE PRINCE** was paid more than $89,000, through Taggcar Inc., representing funds obtained or otherwise derived from specified unlawful activity.

11. During the course of the conspiracy and as a direct result of his participation in the conspiracy, **EMANUEL ASHTOR** was paid more than $40,000, through Vali Tech Inc. and other means, representing funds obtained or otherwise derived from specified unlawful activity.

OVERT ACTS

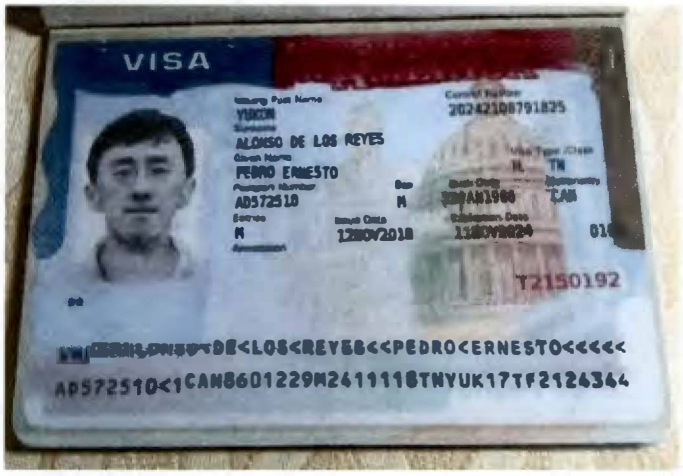
In furtherance of this conspiracy, and to accomplish its purpose and objects, at least one of the co-conspirators committed or caused to be committed, in the Southern District of Florida, and elsewhere, at least one of the following overt acts, among others:

Fraudulent Employment with Company A

1. Between in or around June 2021, through in or around March 2022, **JIN SUNG-IL**, **ERICK NTEKEREZE PRINCE**, and **PEDRO ERNESTO ALONSO DE LOS REYES**, used **ALONSO's** identity to fraudulently obtain and maintain remote IT employment with

Company A as a developer for cellphone applications, to earn income from such fraudulent employment, and to launder such funds in furtherance of the conspiracy.

2. On or about June 2021, **JIN SUNG-IL** applied for a position with U.S. IT Company 1, for which **JIN** would ultimately perform work on Company A's mobile platform, utilizing **PEDRO ERNESTO ALONSO DE LOS REYES'** identity with **ALONSO's** consent, one of **ERICK NTEKEREZE PRINCE's** New York addresses, and the fake non-immigrant United States-Mexico-Canada Agreement ("USMCA") Professional (TN) visa, pictured below:



3. In or around June 2021, **JIN SUNG-IL** signed the following documents utilizing **PEDRO ERNESTO ALONSO DE LOS REYES'** identity: (1) a job offer for employment with U.S. Staffing Company 1 as a mobile application developer; (2) a confidentiality agreement for U.S. IT Company 1; and (3) a U.S. IT Company 1 agreement to care for and return a U.S. IT Company-provided laptop.

4. On or about June 24, 2021, **JIN SUNG-IL** informed **ERICK NTEKEREZE** that he had secured employment with Company A for an expected salary of $120,000.00 per year.

5. On or about June 28, 2021, **JIN SUNG-IL** caused U.S. IT Company 1 to ship a laptop to one of **ERICK NTEKEREZE PRINCE's** New York addresses, which was received by **NTEKEREZE** on or about June 29, 2021.

6. Between in or around August 2021 and continuing through in or around March 2022, **ERICK NTEKEREZE PRINCE** used his company, Taggcar Inc., to invoice U.S. Staffing Company 1 approximately eight times, totaling approximately $75,709.00, for IT work performed by **JIN SUNG-IL**, who was posing as **PEDRO ERNESTO ALONSO DE LOS REYES**. Shortly after receiving the funds, **NTEKEREZE** transferred a portion of the payments to an Online Payment Platform 1 account in the name of **ALONSO**, which was accessible by both **JIN** and **ALONSO**.

7. On or about March 23, 2022, **PAK JIN-SONG** and **ERICK NTEKEREZE PRINCE**, with assistance from **JIN SUNG-IL**, used the fake persona "Glaus Li" to fraudulently obtain a second remote job with Company A in furtherance of the conspiracy.

8. On or about March 23, 2022, **PAK JIN-SONG** was hired for a position as a mobile application developer for services ultimately rendered by Company A utilizing the "Glaus Li" persona and a Maryland address.

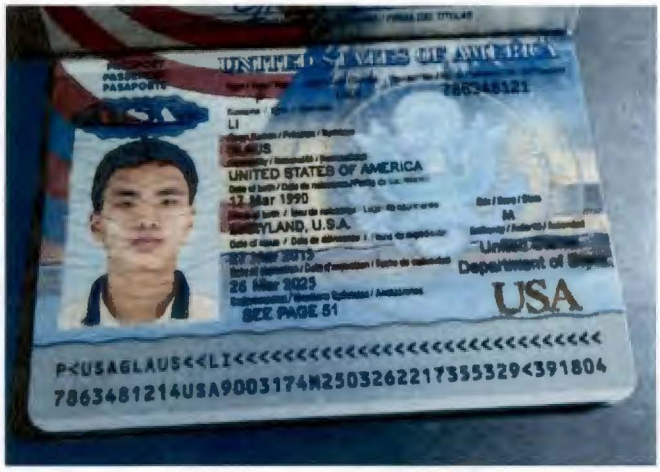
9. On or about April 21, 2022, **ERICK NTEKEREZE PRINCE** received a laptop sent by Company A and addressed to "Glaus Li" at one of **NTEKEREZE's** New York addresses.

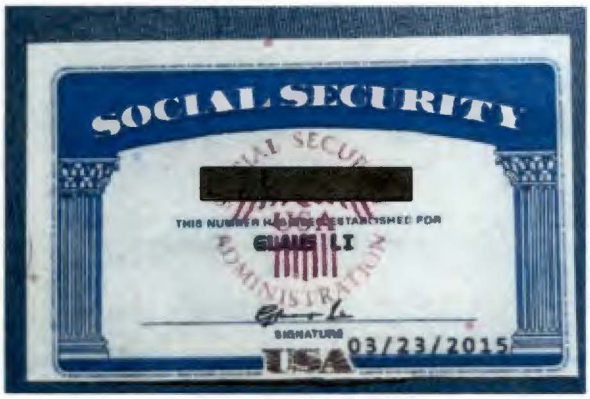
10. On or about April 22, 2022, **JIN SUNG-IL** provided **ERICK NTEKEREZE PRINCE** with login credentials for the Company A laptop, specifically a username and password, and asked **NTEKEREZE** to install Anydesk. Without authorization, **NTEKEREZE** downloaded

and installed Anydesk on the Company A laptop, enabling **PAK JIN-SONG**, to perform remote IT work using the "Glaus Li" persona.

Fraudulent Employment with Company B

11. On or about March 16, 2022, **PAK JIN-SONG**, utilizing the "Glaus Li" persona, applied for a specialist engineer position with U.S. Staffing Firm 2 to fill a mobile application developer position with Company B. **PAK** applied for this position utilizing the "Glaus Li" persona, one of **ERICK NTEKEREZE PRINCE's** New York addresses, and the fake U.S. passport and social security card, pictured below:





12. On or about April 22, 2022, **ERICK NTEKEREZE PRINCE** received a laptop sent by Company B and addressed to "Glaus Li" at one of **NTEKEREZE's** New York addresses.

13. On or about June 27, 2022, **JIN SUNG-IL** provided **ERICK NTEKEREZE PRINCE** with login credentials for the Company B laptop, specifically a username and password.

14. On or about April 29, 2022, **JIN SUNG-IL** directed **ERICK NTEKEREZE PRINCE** to ship the Company B laptop to an address in Dalian, China, claiming that this was the true address of "Glaus Li". **NTEKEREZE** shipped the Company B laptop to that address.

15. From on or about November 7, 2022, to in or around March 2023, co-conspirators accessed, without authorization, the Company B laptop from China and accessed, without authorization, Company B's internal corporate network from the Company B laptop through VPNs.

Attempted Fraudulent Employment with Company C

16. On October 12, 2022, **PAK JIN-SONG**, utilizing the "Glaus Li" persona, applied for a position as a mobile application developer with Company C, which is headquartered in the Southern District of Florida.

17. On or about October 12, 2022, **PAK JIN-SONG** caused U.S. Staffing Company 3, a recruiting firm, to attempt to fill a position for Company C, and U.S. Staffing Company 3 subsequently assigned a recruiter in its Doral, Florida office to manage the hiring process.

18. On October 12, 2022, in response to an inquiry from a U.S. Staffing Company 3 recruiter, **PAK JIN-SONG** used email address glausli1990@outlook.com to provide U.S. Staffing Company 3 a copy of the "Glaus Li" persona's resume.

19. On or about October 20, 2022, **PAK JIN-SONG**, posing as "Glaus Li," interviewed with U.S. Staffing Company 3 for the Company C Android app developer position. Company C did not ultimately hire **PAK** for the position.

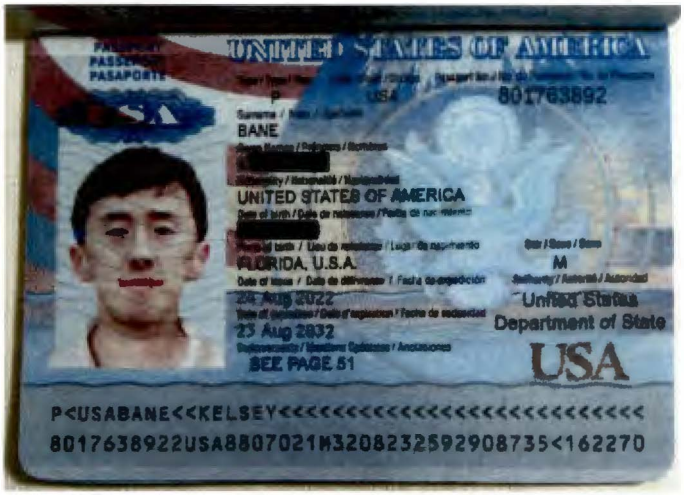
Fraudulent Employment with Company D

20. On or about July 20, 2022, **EMANUEL ASHTOR** registered the company Vali Tech Inc. with the Florida Department of State, listing three officers: **ASHTOR**, S.B. (whose identity is known to the Grand Jury), and U.S. Victim 1. **ASHTOR** did not have lawful authority to transfer, possess, and use a means of identification of U.S. Victim 1 to register Vali Tech Inc.

21. On or about August 26, 2022, **JIN SUNG-IL** obtained a remote IT work position with U.S. IT Company 2 using the name and other means of identification belonging to U.S. Victim 1.

22. On or about August 26, 2022, **JIN SUNG-IL** told U.S. IT Company 2 he had changed his family—that is, his last name—to "Bane" and was issued a new passport.

23. On or about October 11, 2022, **JIN SUNG-IL** obtained a remote IT developer position at Company D, through a corporation-to-corporation contract between **EMANUEL ASHTOR's** company Vali Tech Inc and U.S. IT Company 2. **JIN** applied to the position using one of **ASHTOR's** New York addresses, and the fake U.S. passport, pictured below:



24. On or about October 11, 2022, **JIN SUNG-IL**, using the "K. Bane" persona, was hired by Company D.

25. On or about October 11, 2022, **EMANUEL ASHTOR** received a laptop sent by Company D, and addressed to "K. Bane," to one of **ASHTOR's** New York addresses.

26. On or about October 11, 2022, **EMANUEL ASHTOR**, without authorization, connected the Company D laptop to Company D's network and then knowingly downloaded and installed AnyDesk on the Company D laptop.

27. On October 20, 2022, **EMANUEL ASHTOR**, on behalf his company Vali Tech Inc., sent Company D a completed Form I-9 for "K. Bane," certifying that **ASHTOR** had examined the U.S. passport ending in -3892 for "K. Bane" and determined it was legitimate, despite knowing that it was fraudulent.

28. On or about January 10, 2024, **EMANUEL ASHTOR** received a second laptop sent by Company D, and addressed to "K. Bane," at one of **ASHTOR**'s New York addresses.

29. On or about February 14, 2024, **EMANUEL ASHTOR**, without authorization, connected the second Company D laptop to Company D's network and then knowingly downloaded and installed TeamViewer on the second Company D laptop.

30. From on or about February 26, 2024, and continuing through on or about March 19, 2024, **EMANUEL ASHTOR**, without authorization, logged into the Company D laptop computer provided to "K. Bane" and connected the Company D laptop to Wi-Fi networks associated with **ASHTOR's** North Carolina residential address. Doing so allowed **JIN SUNG-IL** to perform remote IT work for Company D as "K. Bane".

31. Between in or around January 2023 and May 2024, **EMANUEL ASHTOR** used his company, Vali Tech Inc., to invoice U.S. IT Company 2 at least 10 times for IT work performed by **JIN SUNG-IL**, posing as K. Bane at Company D. U.S. IT Company 2 paid **JIN**, through Vali Tech Inc, $206,080. In at least some instances, **ASHTOR** transferred a portion of these payments

to an Online Payment Platform 2 account in the name of **PEDRO ERNESTO ALONSO DE LOS REYES**, which was accessible by both **JIN** and **ALONSO**.

All in violation of Title 18, United States Code, Section 371.

COUNT 2
Conspiracy to Commit Wire Fraud and Mail Fraud
(18 U.S.C. § 1349)

1. The General Allegations section of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

2. From as early as in or around April 2018, the exact date being unknown to the Grand Jury, and continuing through in or around August 2024, in Miami-Dade and Broward Counties, in the Southern District of Florida, and elsewhere, the defendants,

JIN SUNG-IL,
a/k/a "진성일,"
a/k/a "Jin Song-Il,"
a/k/a "Pedro Alonso,"
a/k/a "Richard Stewart,"
a/k/a "Stewart Conn,"
a/k/a "Kelsey Bane,"
PEDRO ERNESTO ALONSO DE LOS REYES,
ERICK NTEKEREZE PRINCE,
a/k/a "Eric Prince,"
PAK JIN-SONG,
a/k/a "박진성,"
a/k/a "Glaus Li,"
and
EMANUEL ASHTOR,
a/k/a "Ndagijimana Emmanuel,"

did knowingly and willfully combine, conspire, confederate and agree with each other, and with others known and unknown to the Grand Jury, to commit certain offenses against the United States, namely:

a. to knowingly and with the intent to defraud, devise and intend 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, knowing the pretenses, representations, and promises were false and fraudulent when made, and for the purpose of executing the scheme and artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate commerce, certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343; and

b. to knowingly, and with the intent to defraud, devise, and intend 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, knowing that the pretenses, representations, and promises were false and fraudulent when made, and, for the purpose of executing the scheme and artifice, did knowingly cause to be delivered certain mail matter, via United States mail and private and commercial interstate carrier, according to the directions thereon, in violation of Title 18, United States Code, Section 1341.

PURPOSE OF THE CONSPIRACY

3. The Object and Purpose of the Conspiracy section from Count 1 of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

MANNER AND MEANS OF THE CONSPIRACY

The Manner and Means of the Conspiracy section from Count 1 of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

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

COUNT 3
Conspiracy to Commit Money Laundering
(18 U.S.C. § 1956(h))

1. The General Allegations section of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

2. From as early as in or around April 2018, the exact date being unknown to the Grand Jury, and continuing through in or around August 2024, in Miami-Dade and Broward Counties, in the Southern District of Florida, and elsewhere, the defendants,

JIN SUNG-IL,
a/k/a "진성일,"
a/k/a "Jin Song-Il,"
a/k/a "Pedro Alonso,"
a/k/a "Richard Stewart,"
a/k/a "Stewart Conn,"
a/k/a "Kelsey Bane,"
PEDRO ERNESTO ALONSO DE LOS REYES,
ERICK NTEKEREZE PRINCE,
a/k/a "Eric Prince,"
PAK JIN-SONG,
a/k/a "박진성,"
a/k/a "Glaus Li,"
and
EMANUEL ASHTOR,
a/k/a "Ndagijimana Emmanuel,"

did knowingly and voluntarily combine, conspire, confederate, and agree with each other, and with others known and unknown to the Grand Jury, to commit offenses defined in Title 18, United States Code, Section 1956(h), namely:

a. To knowingly conduct and cause others to conduct, and attempt to conduct, financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, knowing that the property

involved in the financial transactions represented the proceeds of some form of unlawful activity, with the intent to promote the carrying on of specified unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and

b. To knowingly conduct, and aid, abet, and cause others to conduct, and attempt to conduct, financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, and that the financial transactions were designed in whole and in part, to conceal and disguise the nature, the location, the source, the ownership, and control of the proceeds of said specified unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

It is further alleged that the specified unlawful activity is damaging a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), wire fraud, in violation of Title 18, United States Code, Section 1343, and mail fraud, in violation of Title 18, United States Code, Section 1341.

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

COUNT 4
Conspiracy to Transfer False Identification Documents
(18 U.S.C. § 1028(a)(2) and (f))

1. The General Allegations section of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

2. From as early as in or around April 2018, the exact date being unknown to the Grand Jury, and continuing through in or around August 2024, in Miami-Dade and Broward Counties, in the Southern District of Florida, and elsewhere, the defendants,

JIN SUNG-IL,
a/k/a "진성일,"
a/k/a "Jin Song-Il,"
a/k/a "Pedro Alonso,"
a/k/a "Richard Stewart,"
a/k/a "Stewart Conn,"
a/k/a "Kelsey Bane,"
PEDRO ERNESTO ALONSO DE LOS REYES,
ERICK NTEKEREZE PRINCE,
a/k/a "Eric Prince,"
PAK JIN-SONG,
a/k/a "박진성,"
a/k/a "Glaus Li,"
and
EMANUEL ASHTOR,
a/k/a "Ndagijimana Emmanuel,"

did knowingly combine, conspire, confederate, and agree with each other, and with others known and unknown to the Grand Jury, to knowingly transfer false identification documents, that is, false U.S. passports, visas, social security cards, and driver licenses, knowing such documents were produced without lawful authority, which possession occurred in and affecting interstate commerce, in violation of Title 18, United States Code, Section 1028(a)(2); all in violation of Title 18, United States Code, Section 1028(f).

COUNT 5
Conspiracy to Violate the International Emergency Economic Powers Act (50 U.S.C. § 1705(a) and (c))

1. The General Allegations section of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

2. From as early as in or around April 2018, the exact date being unknown to the Grand Jury, and continuing through in or around August 2024, in Miami-Dade and Broward Counties, in the Southern District of Florida, and elsewhere, and begun and committed outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, the defendants,

JIN SUNG-IL,
a/k/a "진성일,"
a/k/a "Jin Song-Il,"
a/k/a "Pedro Alonso,"
a/k/a "Richard Stewart,"
a/k/a "Stewart Conn,"
a/k/a "Kelsey Bane,"
and
PAK JIN-SONG,
a/k/a "박진성,"
a/k/a "Glaus Li,"

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

All in violation of Title 50 U.S.C. § 1705(a) and (c), Executive Order 13722, and 31 C.F.R. §§ 510.206 and 510.212.

FORFEITURE ALLEGATIONS

1. The allegations of this Indictment are hereby re-alleged and by this reference fully incorporated herein for the purpose of alleging forfeiture to the United States of certain property in which the defendants, **JIN SUNG-IL**, **PEDRO ERNESTO ALONSO DE LOS REYES**, **ERICK NTEKEREZE PRINCE**, **PAK JIN-SONG**, and **EMANUEL ASHTOR**, have an interest.

2. Upon conviction of a violation of Title 18, United States Code, Section 1349, specifically to a conspiracy to violate Title 18, United States Code, Sections 1341 and 1343, as alleged in this Indictment, the defendants shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offense, pursuant to Title 18, United States Code, Section 981(a)(1)(C).

3. Upon conviction of a violation of Title 18, United States Code, Section 371, specifically a conspiracy to violate Title 18, United States Code, Section 1030, as alleged in this Indictment, the defendants shall forfeit to the United States:

i. any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i); and

ii. any personal property that was used or intended to be used to commit or to facilitate the commission of such offense, pursuant to Title 18, United States Code, Section 1030(i).

4. Upon conviction of a violation of, or a conspiracy to violate, Title 18, United States Code, Section 1956, as alleged in this Indictment, the defendants shall forfeit to the United States

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

5. Upon conviction of a violation of, or a conspiracy to violate, Title 18, United States Code, Section 1028, as alleged in this Indictment, the defendants shall forfeit to the United States: (a) any property constituting, or derived from, proceeds obtained, directly or indirectly, as the result of such offense, pursuant to Title 18, United States Code, Section 982(a)(2)(B); and (b) any personal property used or intended to be used to commit the offense, pursuant to Title 18, United States Code, Section 1028(b)(5).

6. Upon conviction of a violation of, or a conspiracy to violate, Title 50, United States Code, Section 1705, as alleged in this Indictment, the defendant shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offense, pursuant to Title 18, United States Code, Section 981(a)(1)(C).

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 982(b), 1028(b)(5), and 1030(i), and the procedures set forth at Title 21, United States Code, Section 853, as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1028(g), and Title 28, United States Code, Section 2461(c).

A TRUE BILL

[redacted]

FOREPERSON

MICHAEL S. DAVIS
ACTING UNITED STATES ATTORNEY

JONATHAN D. STRATTON
ASSISTANT UNITED STATES ATTORNEY

SEAN CRONIN
ASSISTANT UNITED STATES ATTORNEY

GREGORY NICOSIA
TRIAL ATTORNEY
NATIONAL SECURITY DIVISION