AFM/NJM:ADR/BW/RMS
F. #2024R00105

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

CHEN ZHI,
also known as "Vincent,"

Defendant.

----------X

I N D I C T M E N T

Cr. No. 25-CR-312
(T. 18, U.S.C., §§ 981(a)(1)(C), 982(a)(1), 982(b)(1), 1956(h), 1349 and 3551 *et seq.*; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

Judge Rachel P. Kovner
Magistrate Judge Cheryl L. Pollak

THE GRAND JURY CHARGES:

INTRODUCTION

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

I. Overview

1. Since approximately 2015, the defendant CHEN ZHI, also known as "Vincent," served as Chairman of Prince Holding Group ("Prince Group"), a Cambodian corporate conglomerate he founded that operated dozens of business entities in more than thirty countries. Ostensibly, Prince Group was focused on real estate development, financial services and consumer services. However, in secret, CHEN and his top executives grew Prince Group into one of the largest transnational criminal organizations in Asia. Under CHEN's direction, Prince Group made enormous profits for CHEN and his associates by operating forced-labor scam compounds across Cambodia that engaged in cryptocurrency investment fraud schemes and other fraudulent schemes and used its vast network of business enterprises to launder its

criminal proceeds. The schemes resulted in billions of dollars in losses incurred by victims in the United States and around the world.

II. Background

A. The Defendant, Co-Conspirators and Relevant Entities

2. The defendant CHEN ZHI was a citizen of China, Cambodia, Vanuatu, St. Lucia and Cyprus and resided in Cambodia, Singapore, Taiwan and the United Kingdom.

3. Co-Conspirator-1, an individual whose identity is known to the Grand Jury, was a citizen of Cambodia, Vanuatu, Cyprus and St. Kitts and resided in Cambodia, Singapore and the United Kingdom.

4. Co-Conspirator-2, an individual whose identity is known to the Grand Jury, was a citizen of Cambodia and Cyprus and resided in Singapore and the United States.

5. Co-Conspirator-3, an individual whose identity is known to the Grand Jury, was a citizen of China and Cambodia and resided in the United States and elsewhere.

6. Co-Conspirator-4, an individual whose identity is known to the Grand Jury, was a citizen and resident of Cambodia.

7. Co-Conspirator-5, an individual whose identity is known to the Grand Jury, was a citizen and resident of Hong Kong.

8. Co-Conspirator-6, an individual whose identity is known to the Grand Jury, was a citizen and resident of Hong Kong.

9. Co-Conspirator-7, an individual whose identity is known to the Grand Jury, was a citizen and resident of Singapore.

10. Exchange-1, an entity the identity of which is known to the Grand Jury, was a cryptocurrency exchange platform based in China.

11. Exchange-2, an entity the identity of which is known to the Grand Jury, was a cryptocurrency exchange platform based in the Seychelles.

12. Trading Platform-1, an entity the identity of which is known to the Grand Jury, was an online trading platform.

13. Prince Group was a Cambodian-registered corporate holding company that operated more than 100 business entities in over thirty countries. The defendant CHEN ZHI was the founder and Chairman of Prince Group.

14. Yun Ki Estate Intermediary Co., Ltd. ("Yun Ki") was a Prince Group subsidiary that was engaged in the real estate development business. In or about and between 2020 and the present, Co-Conspirator-1 was the Chairman of Yun Ki.

15. Awesome Global Investment Group ("Awesome Global") was a Prince Group subsidiary that was engaged in the entertainment, hospitality and real estate development businesses. In or about and between 2017 and 2022, Co-Conspirator-2 served as the Chairman of Awesome Global.

16. Prince Real Estate Group and Prince Huan Yu Real Estate Group were Prince Group subsidiaries that were engaged in the real estate development business. In or about and between 2018 and at least 2024, Co-Conspirator-3 served as the Chairman of Prince Huan Yu Real Estate Group.

17. Prince Bank was a Prince Group subsidiary that was engaged in the financial services business. In or about and between 2015 and at least 2023, Co-Conspirator-4 served as Vice-Chairman of Prince Bank.

B. Relevant Terms and Definitions

18. "Pig-butchering" (or "*sha zhu pan*") scams were cyber-enabled investment fraud schemes in which malicious actors contacted unwitting victims through messaging or social media applications and convinced them to transfer cryptocurrency or other funds to specified accounts based on false promises that the funds would be invested and generate profits. In reality, the funds were misappropriated from the victims and laundered for the benefit of the perpetrators. Pig-butchering scams often relied on social engineering to earn victims' trust to induce the fraudulent investments.

19. Pig-butchering scams typically involved four stages. First, a perpetrator would use a fictious identity and cold contact a victim on a messaging or social media application. Often, the perpetrator would pretend to have contacted the wrong number but would continue communicating with the victim. Second, the perpetrator would establish a relationship and build trust with the victim by continuing to message the victim over days, weeks or months. Third, the perpetrator would devise a narrative to induce the victim to send a series of payments in the form of virtual currency. Common narratives included lucrative investment opportunities, emergencies necessitating funds and romance scams. Many perpetrators would convince victims to use fraudulent websites or applications, controlled by scammers, to invest in virtual currency. Perpetrators coached victims through the investment process, showed them fake profits and encouraged them to invest more. Fourth, the perpetrator would disengage the victim once the victim's funds were stolen, generally cutting off all contact.

20. "*Jingliao*," or "scripted chat," was a term commonly associated with cryptocurrency investment fraud schemes and related schemes.

21. "Virtual currencies" were digital representations of value that, like traditional coin and paper currency, functioned as a medium of exchange (*i.e.*, they could be digitally traded or transferred, and could be used for payment or investment purposes). Virtual currencies were a type of digital asset separate and distinct from digital representations of traditional currencies, securities and other traditional financial assets. The exchange value of a particular virtual currency generally was based on agreement or trust among its community of users. Some virtual currencies had equivalent values in real currency or could act as substitutes for real currency, while others were specific to particular virtual domains and generally could not be exchanged for real currency.

22. "Cryptocurrencies," like bitcoin ("BTC") and ether ("ETH"), were types of virtual currencies, which relied on cryptography for security. Cryptocurrencies typically lacked a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies used algorithms, a distributed ledger known as a "blockchain" and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

23. "Stablecoins" were a type of virtual currency with a valuation tied to the price of a commodity, such as gold, or to a conventional (or "fiat") currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT (or "tether"), and USDC were stablecoins tied to the U.S. dollar. Stablecoins achieved their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

24. "Mining" was the process by which certain types of virtual currency transactions, including bitcoin transactions, were verified and added to the public ledger (in the case of bitcoin, the Bitcoin blockchain), and also the means through which new units of those

virtual currencies were generated and released. Transactions were verified and assembled into "blocks" through the creation of codes, or "hashes," that fulfilled certain requirements, which were then appended to the blockchain. Those that carried out the task of verifying "blocks" of legitimate transactions, often referred to as "miners," were rewarded with an amount of that cryptocurrency. A "mining pool" was a group of cryptocurrency miners who combined their computational resources over a network to strengthen the probability of successfully mining cryptocurrency.

25. A "virtual currency address" was an alphanumeric string that designated the virtual location on a blockchain where virtual currency could be sent and received. A virtual currency address was associated with a virtual currency wallet.

26. A "virtual currency wallet" was an application that allowed users to store and retrieve virtual currency, including cryptocurrency, as well as other digital assets. Each wallet contained one or more unique cryptographic address. When a user acquired cryptocurrency, whether by purchasing it in a currency exchange, receiving it as a gift, or as revenue from mining, it was deposited into an address contained in a wallet. Wallets could be maintained or "hosted" by a third-party service, such as a virtual currency exchange, or held directly by individuals (referred to as an "unhosted" wallet). While transactions involving particular addresses could generally be traced on the blockchain ledger of the respective cryptocurrency, there was no user identification available for wallets beyond the unique cryptographic addresses associated with them. This ability to namelessly conduct transactions using wallets on decentralized ledgers allowed cryptocurrencies to be used to obscure the source of criminal proceeds and mask the audit trail from criminal activity.

27. A "virtual currency exchange," also called a "cryptocurrency exchange," was a platform that allowed customers to buy, sell and trade virtual currencies for other assets, such as fiat currency or other virtual currencies. A cryptocurrency exchange could typically send cryptocurrency to a user's personal cryptocurrency wallet. Exchanges accepted credit card payments, wire transfers or other forms of payment in exchange for virtual currencies or other digital assets. Many exchanges also stored their customers' virtual currency addresses in hosted wallets. Cryptocurrency exchanges could be centralized (*i.e.*, an entity or organization that facilitated virtual currency trading between parties on a large scale and often resembled traditional asset exchanges like the exchange of stocks) or decentralized (*i.e.*, a peer-to-peer marketplace where transactions occurred directly between parties).

III. The Criminal Schemes

28. From approximately 2015 to the present, the defendant CHEN ZHI and top executives at Prince Group engaged in schemes to defraud victims around the world through cryptocurrency investment scams and other fraudulent schemes that resulted in the misappropriation of billions of dollars. To effectuate the schemes, CHEN and his co-conspirators caused Prince Group to build and operate forced-labor scam compounds across Cambodia in which workers were made to execute the scams at high volumes. CHEN and his co-conspirators used their political influence in multiple countries to protect their criminal enterprise and paid bribes to foreign public officials to avoid disruption by law enforcement. They subsequently laundered the proceeds of the fraudulent schemes through professional money laundering operations and through Prince Group's own network of ostensibly legal business enterprises, including its online gambling and cryptocurrency mining operations.

A. The Fraud Schemes

29. The defendant CHEN ZHI was the founder and Chairman of Prince Group. According to its website, Prince Group's "key business units" in Cambodia included "Prince Real Estate Group, Prince Huan Yu Real Estate Group, Prince Bank, as well as Awesome Global Investment Group." Together, those and other Prince Group units operated in a range of publicly disclosed business sectors, including "real estate development, banking, finance, tourism, logistics, technology, food and beverages, and lifestyle." However, in secret, Prince Group generated enormous profits for CHEN from its illicit and fraudulent activities, coordinated by CHEN and facilitated by a close network of CHEN's top executives and associates, including Co-Conspirator-1 through Co-Conspirator-7, among others.

1. The Scam Compounds

30. In particular, Prince Group came to dominate the rapidly growing online scam industry. As part of that illicit industry, thousands of migrant workers traveled to Cambodia and elsewhere seeking job opportunities but instead were trafficked and forced to work in scam compounds executing cryptocurrency investment fraud and other fraudulent schemes, often under the threat of violence. The scam compounds housed vast dormitories surrounded by high walls and barbed wire, and functioned as forced labor camps.

31. At the defendant CHEN ZHI's direction, Prince Group built and operated at least ten scam compounds throughout Cambodia that perpetrated cryptocurrency investment scams and other fraudulent schemes, including, among others: (i) a compound associated with Prince Group's Jinbei Hotel and Casino in Sihanoukville, Cambodia, known as the "Jinbei Compound"; (ii) a compound in Chrey Thom, Cambodia, known as the "Golden Fortune Science

and Technology Park" (also known as the "Jinyun Compound"); and (iii) a compound in Kampong Speu Province, Cambodia, known as "Mango Park" (also known as "Jinhong Park").

32. The defendant CHEN ZHI was directly involved in managing the scam compounds and maintained records associated with each one, including records tracking profits from the scams that explicitly referenced "*sha zhu*," or pig-butchering. One ledger saved by CHEN tracked the various fraud schemes run from Prince Group's Jinhong Park, as well as which buildings and floors at the park were responsible for each. The listed schemes included "Vietnamese order fraud," "Russian order fraud," "European and American *jingliao*" (a reference to investment scams), "Vietnamese," "Chinese" and "Taiwanese" "*jingliao*," and "Chinese brush order," as pictured below.

金鸿园区团队业务	
A2001	越南刷单
B2001	欧美商城
B2002	中国精聊
B2003	欧美精聊
B2004	台湾精聊
B2005	越南贷款
B2008	中国股票
B3004	俄罗斯刷单
B3005	中国刷单
B3007	欧美精聊
C1001	越南刷单
C1005	越南精聊
C1006	中国精聊
C1007	台湾精聊
C1014	欧美精聊
C1022	中国刷单

Original

Jinhong Park Team Business	
A2001	Vietnamese order fraud
B2001	European and American market
B2002	Chinese *jingliao*
B2003	European and American *jingliao*
B2004	Taiwanese *jingliao*
B2005	Vietnamese loans
B2008	Chinese stocks
B3004	Russian order fraud
B3005	Chinese brush order
B3007	European and American *jingliao*
C1001	Vietnamese order fraud
C1005	Vietnamese *jingliao*
C1006	Chinese *jingliao*
C1007	Taiwanese *jingliao*
C1014	European and American *jingliao*
C1022	Chinese brush order

Translation

33. The defendant CHEN ZHI and his co-conspirators designed the compounds to maximize profits and personally ensured that they had the necessary infrastructure to reach as many victims as possible. For example, in or about 2018, Co-Conspirator-1 was involved in procuring millions of mobile telephone numbers and account passwords from an illicit online marketplace. In or about 2019, Co-Conspirator-3 helped oversee construction of the Golden Fortune compound. CHEN himself maintained documents describing and depicting "phone farms," automated call centers used to facilitate cryptocurrency investment fraud and other cybercrimes, including the below image:

The documents detailed the completion of two particular facilities staffed with 1,250 mobile phones that controlled 76,000 accounts on a popular social media platform.

34. Additional internal Prince Group documents included instructions on building rapport with victims and guidance on how to register social media accounts in bulk, including a direction to use profile photos of women who were not "too beautiful," so that the accounts would appear genuine.

35. In the summer of 2022, Co-Conspirator-2 boasted that, in 2018, Prince Group was earning over $30 million a day from fraudulent *sha zhu pan* schemes and related illicit activities.

2. Use of Bribes and Violence in Furtherance of the Schemes

36. The defendant CHEN ZHI and his co-conspirators used their political influence to protect the scam operations from law enforcement in multiple countries, including from the Chinese Ministry of Public Security ("MPS") and Ministry of State Security ("MSS"). Among other things, Prince Group executives bribed public officials for information in advance of law enforcement raids of Prince Group scam compounds. Additionally, CHEN enlisted Co-Conspirator-2 to preside over Prince Group's "risk control" function to monitor investigations and engage in corrupt bargaining with foreign law enforcement officials to advance Prince Group's interests.

37. For example, in or about May 2023, Co-Conspirator-2 engaged in communications with an MPS official who stated that he could get Prince Group associates "off the hook." In return, Co-Conspirator-2 offered to "take care of" the official's son. As another example, in or about July 2023, Co-Conspirator-2 directed a Chinese law enforcement official to have local police extort businesses on behalf of Prince Group, stating, "Tell the police to rob [] places, and then go to talk to them about protection, in my company's and my name. Rob them first and then protect them." In the same conversation, Co-Conspirator-2 boasted that whenever

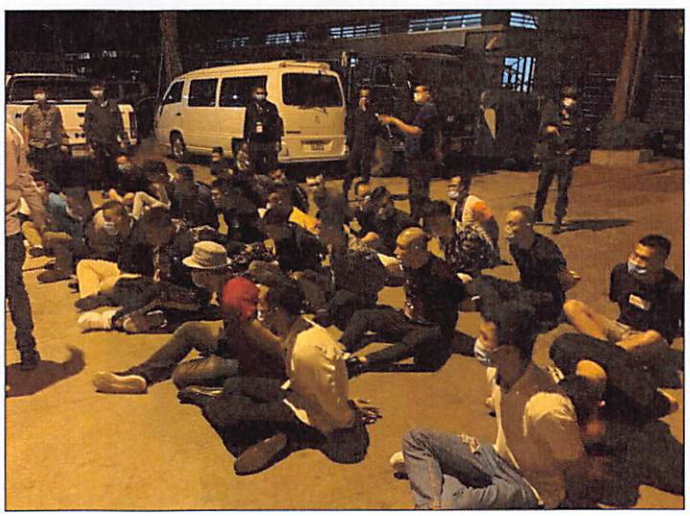
there were law enforcement crackdowns at the scam compounds, nothing happened to "us," referring to Prince Group. Co-Conspirator-2 and the defendant CHEN ZHI communicated at length about "risk control" issues and which officials from the MPS Co-Conspirator-2 was in touch with. CHEN also boasted to others of his arrangements with the MSS to be informed of law enforcement actions in exchange for bribe payments.

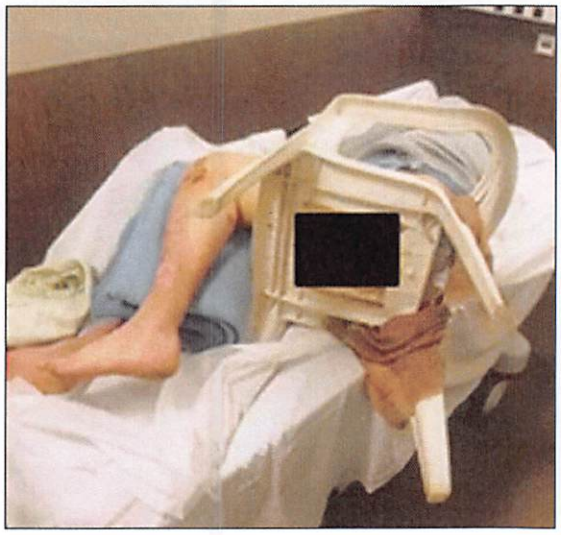
38. The defendant CHEN ZHI maintained ledgers of bribes to public officials, including a ledger that tracked hundreds of millions of dollars in reimbursements to Prince Group associates for bribes and luxury purchases. The ledger indicated, for example, that in 2019, Co-Conspirator-2 purchased a yacht for a senior official of a foreign government worth more than $3 million. CHEN also purchased luxury watches worth millions of dollars for another senior foreign government official (the "Official"). In 2020, the Official helped CHEN obtain a diplomatic passport that CHEN used to travel to the United States in April 2023.

39. As part of his "risk control" duties, Co-Conspirator-2 served as a Prince Group enforcer and used corrupt and violent means to maintain Prince Group's dominance among scam operators. For example, in or about July 2024, Co-Conspirator-3 reached out to the defendant CHEN ZHI to discuss the theft of illicit Prince Group profits by a Prince Group associate. Co-Conspirator-3 informed CHEN that "one finance personnel" had "fled with [funds]" and "tried to hide." Co-Conspirator-3 informed CHEN of efforts to reclaim the stolen funds, and promised him that, "no matter how, we will make sure no stone is unturned. I don't know if the boss [referring to CHEN] and the Group [referring to Prince Group] has any suggestions or approaches that can be shared. . . . [B]oth the mafia and government are ready to be mobilized, and can set an example for others. Boss, does the Group have experience and resources on this?" CHEN later responded, "For this specific situation, you talk to

[Co-Conspirator-2] first. Get all the information before deciding how to do it. Find out where this person is now."

40. Prince Group associates, at the defendant CHEN ZHI's direction, frequently used violence and coercion to achieve business outcomes and further their criminal schemes. In one such instance, a Prince Group associate discussed with CHEN beating an individual who had "caused trouble" at a compound. CHEN approved of the beating and instructed that the individual not be "beaten to death." He added: "we must keep an eye on them and not let them run away." In another instance, CHEN communicated with Co-Conspirator-4 about two individuals who had been reported missing and were found by police at the Golden Fortune compound. Co-Conspirator-4 assured CHEN that he would handle the situation, but suggested that CHEN use his police connections. CHEN possessed images illustrating Prince Group's violent methods, including those below:





3. The Brooklyn Network

41. Prince Group's investment fraud schemes targeted victims around the world, including in the United States, with assistance from local networks working on Prince Group's behalf. One such network operated in the Eastern District of New York (the "Brooklyn Network"). The Brooklyn Network facilitated an investment fraud scheme perpetrated by scammers at Prince Group's Jinbei Compound in which victims were contacted on various messaging applications by individuals unknown to them (the "Introducers") who claimed to have made money investing in various investment markets, such as cryptocurrency markets and foreign exchange markets. The Introducers convinced the victims to invest and introduced them to purported account managers (the "Account Managers") who would process their transactions. The Account Managers subsequently provided the victims with instructions regarding the bank accounts to which they should wire their investments and created fraudulent profiles and investment portfolios for them at mobile online trading platforms, including Trading Platform-1 and others.

42. However, in reality, the bank accounts provided by the Account Managers to the victims were not investment accounts but rather bank accounts controlled by the Brooklyn Network in the names of Brooklyn- and Queens-based shell companies at financial institutions in Brooklyn, Queens and throughout New York. The victims' funds were not invested, as they had been promised, but were misappropriated and laundered through these accounts and additional accounts.

43. Meanwhile, the trading profiles created by the Account Managers for the victims were manipulated to appear to reflect growing investments when in reality they did not. Initially, the purported value of the victims' investment portfolios would appear to increase, giving the victims the impression that they were profiting on their investments and enabling the perpetrators to convince the victims to continue to invest. Additionally, when victims made initial requests to withdraw small amounts of their investments, the Account Managers facilitated their requests. However, when the victims contacted the Account Managers to withdraw larger amounts of their funds from the trading platforms, they were met with a series of obstacles. For example, the Account Managers told the victims that they had to pay transaction fees, taxes or legal fees to withdraw their investment funds. Over time, the Account Managers and the Introducers ceased communicating with and responding to the victims, who were unable to withdraw the bulk of the funds they had transferred at the Account Mangers' direction.

44. Ultimately, the Brooklyn Network sent the funds through a series of accounts back to Prince Group scammers at the Jinbei Compound and elsewhere, where they were further laundered before returning to Prince Group and its top executives. Between approximately May 2021 and August 2022, the Brooklyn Network facilitated the fraudulent

transfer and laundering of more than $18 million on behalf of Prince Group from over 250 victims in the Eastern District of New York and throughout the United States.

B. The Money Laundering Schemes

45. The defendant CHEN ZHI and his co-conspirators laundered Prince Group's illicit profits through a variety of complex money laundering networks, including by enlisting the help of professional money laundering operations and by using Prince Group's own businesses, including online gambling and cryptocurrency mining, to launder proceeds. They subsequently used the funds for luxury travel and entertainment and to make expensive purchases such as watches, yachts, private jets, vacation homes, high-end collectables and rare artwork, including a Picasso painting purchased through an auction house in New York City.

46. Professional laundering operations, sometimes referred to as "laundering houses," "money houses" or "water houses," received fraudulent proceeds misappropriated from victims of Prince Group's scam operations and then funneled them back to Prince Group. One common method was to collect scam proceeds in the form of bitcoin or stablecoins such as USDT or USDC and then off-ramp them into fiat currencies. The launderers then used that cash to purchase clean bitcoin or other cryptocurrencies. The defendant CHEN ZHI was directly involved in coordinating these laundering efforts and spoke with co-conspirators about his use of "illegal money shops" and "underground money houses." CHEN maintained documents that explicitly discussed "BTC washing" and "BTC money laundering people."

47. The defendant CHEN ZHI and his co-conspirators also laundered fraudulent proceeds through shell companies that served little purpose other than to launder funds, including companies controlled by CHEN, Co-Conspirators 1, 5, 6 and 7, and other Prince Group associates. Some of these companies maintained bank accounts at financial institutions

based in the United States that were opened on fraudulent pretenses. For example, one such company falsely stated in account opening documents that it was engaged in "[p]roprietary trading and investing" of "[p]ersonal wealth" and understated its anticipated deposit and withdrawal activity by more than 1,000%. An account associated with another such company was used to make payments to the spouse of an Awesome Global executive and to purchase millions of dollars' worth of luxury items, including a Rolex watch.

48. The defendant CHEN ZHI and his co-conspirators also laundered illicit proceeds through functional Prince Group business units, including Prince Group's expansive online gambling business, which operated in multiple countries even following Cambodia's ban on online gambling in approximately 2020. To avoid law enforcement disruption, Prince Group ran its gambling operations through mirror websites, which replicated websites across different domains and servers. CHEN had direct oversight over Prince Group's online gambling operations and communicated with others about laundering fraudulent cryptocurrency proceeds through those operations. Co-Conspirator-1 was involved in managing the payrolls of Prince Group's online gambling operations and maintained ledgers with dates ranging from approximately 2018 through 2024 containing employee payroll data related to the operations. The ledgers included the warning, "Employee wages – Please use clean money to pay."

49. Additionally, the defendant CHEN ZHI and his co-conspirators laundered illicit proceeds by using the proceeds to fund large-scale cryptocurrency mining operations, including a Laos-based company called Warp Data and its Texas-based subsidiary, and a China-based company called Lubian, all of which produced large sums of clean bitcoin dissociated from criminal proceeds. For some of the time it was active, the Lubian mining operation was the sixth largest bitcoin mining operation in the world. CHEN boasted to others of Prince

Group's mining businesses that "the profit is considerable because there is no cost"—that is, the operating capital for the businesses comprised money stolen from Prince Group's many victims.

50. The defendant CHEN ZHI and his co-conspirators also systematically combined illicit funds with newly mined cryptocurrency to obscure the origins of those funds. For example, addresses associated with the Lubian mining operation received large sums of cryptocurrency from sources unrelated to new mining. In another example, newly mined bitcoin was deposited into a particular unhosted wallet while unrelated funds originating from Exchange-2 were deposited into that same wallet in the same approximate amounts and intervals, making it appear as though all of the funds in that wallet originated from bitcoin mining.

51. The defendant CHEN ZHI and his co-conspirators often employed multiple layers of laundering techniques to further obscure the illicit sources of CHEN's and Prince Group's profits. At CHEN's direction, Co-Conspirator-5, a Prince Group associate who worked as CHEN's personal wealth manager, and Co-Conspirator-6, another Prince Group associate, among others, used sophisticated cryptocurrency laundering techniques to obscure the source of fraudulent Prince Group profits, including "spraying" and "funneling" techniques in which large volumes of cryptocurrency were repeatedly disaggregated across scores of wallets and then re-consolidated into fewer wallets, to obscure the source of the funds, consistent with known money laundering typologies. CHEN personally directed and monitored the flow of funds and maintained diagrams tracing the movements.

52. Some of these proceeds were ultimately held in wallets at cryptocurrency exchanges such as Exchange-1 and Exchange-2, or off-ramped into fiat currency and stored in traditional bank accounts. Other proceeds, including those that had been laundered through

Prince Group's mining operations as described above, were stored in unhosted cryptocurrency wallets controlled by the defendant CHEN ZHI.

53. By approximately 2020, the defendant CHEN ZHI had amassed a staggering sum of laundered proceeds that included approximately 127,271 bitcoin across unhosted cryptocurrency wallets whose private keys he personally held. CHEN maintained diagrams recording the process by which some of his cryptocurrency was laundered.

COUNT ONE
(Wire Fraud Conspiracy)

54. The allegations contained in paragraphs one through 53 are realleged and incorporated as if fully set forth in this paragraph.

55. In or about and between January 2014 and October 2025, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant CHEN ZHI, also known as "Vincent," together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud others by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications and money transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 *et seq.*)

COUNT TWO
(Money Laundering Conspiracy)

56. The allegations contained in paragraphs one through 53 are realleged and incorporated as if fully set forth in this paragraph.

57. In or about and between January 2014 and October 2025, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant CHEN ZHI, also known as "Vincent," together with others, did knowingly and intentionally conspire:

(a) to conduct one or more financial transactions in and affecting interstate and foreign commerce, which transactions in fact involved the proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that the property involved in such financial transactions represented the proceeds of some form of unlawful activity, and knowing that such 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, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i); and

(b) to transport, transmit, and transfer monetary instruments and funds from one or more places in the United States to one or more places outside the United States, and from one or more places outside the United States to and through one or more places in the United States, knowing that the monetary instruments and 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 one or

more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i).

(Title 18, United States Code, Sections 1956(h) and 3551 *et seq.*)

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT ONE

58. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count One, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offense to forfeit any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, including but not limited to approximately 127,271 bitcoin previously stored at the following virtual currency addresses:

	Address	**Currency Amount**
(a)	3Pja5FPK1wFB9LkWWJai8XYL1qjbqqT9Ye	20,452.85228 BTC
(b)	3FrM1He2ZDbsSKmYpEZQNGjFTLMgCZZkaf	14,111.92546835 BTC
(c)	3B1u4PsuFzww1P8if5jYmitXxpMs2EMSqt	2,999.09118947 BTC
(d)	3JJ8b7voMPSPChHazdHkrZMqxC7Cb4vNk2	1,000.08105870 BTC
(e)	3PWNGS2357TnjRX7FpewqR3e3qsWwpFrJH	0.00736862 BTC
(f)	34Jpa4Eu3ApoPVUKNTN2WeuXVVq1jzxgPi	14,139.260 BTC
(g)	338uPVW8drux5gSemDS4gFLSGrSfAiEvpX	9,099.01146835 BTC
(h)	3J4sTPyD1g6KvNUSJxjwLs4iaPeDPqxUZr	499.90936500 BTC
(i)	33uEsaGLcF9H46Dvzx1kMnuMCQ13ndkAjV	3,000.09125022 BTC
(j)	3KabDvdetZXDHNm9HXowLc9SppiSXKn7UU	9,500.99220072 BTC
(k)	38Md7BghVmV7XUUT1Vt9CvVcc5ssMD6ojt	15,033.29416267 BTC
(l)	3GaB3nRWA1PLc3XQkkbpVtFwYYZEuMxD4i	0.02415042 BTC
(m)	32i6n2vXhjvJg1vniURFy7A5VK6eG6oDgg	3,000.09118974 BTC
(n)	3HuUiXmKN3beQSoM97kWjK1fesWWJvKvaZ	4,500.00841044 BTC
(o)	34MFtk9iMxYcUPZWXHfiGfqz4o7X3kpJbV	0.5084661 BTC
(p)	3LjTXe31gepN8nW3AZyKpyD2QwbtmfjNwm	156.04996844 BTC

	Address	Currency Amount
(q)	3MHa8JJ3bu8j3x3iQHhqsrZvk1EjBQmC78	2,700.44863780 BTC
(r)	3AWpzKtkHfWsiv9RGXKA3Z8951LefsUGXQ	10,500.04293955 BTC
(s)	34KYo7VdVr5CJ7m4hYhH9RpwqXhbsTrw4T	4,500.00941044 BTC
(t)	3DdFSGcXaP2rZ9CaL3tjnqRARvQ5K3VW4a	251.6000482 BTC
(u)	39B6oSa58qNpFMGpuowtRHAYp3fM4ghXRq	212.5930613 BTC
(v)	3NmHmQte2rP8pS54U3B8LPYQKkpG1pFF69	8,611.07446862 BTC
(w)	3BA3PEF4BMoy9y3kdMRUdMhL8Gp24vikhF	2.16989588 BTC
(x)	389JrNcn8trYgYi2EtHi4X7bTCqtVbep86	1,500.01255361 BTC
(y)	339khCuymVi4FKbW9hCHkH3CQwdopXiTvA	1,500.00 BTC

and all proceeds traceable thereto.

59. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT TWO

60. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Two, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offense to forfeit any property, real or personal, involved in such offense, or any property traceable to such property, including but not limited to approximately 127,271 bitcoin previously stored at the following virtual currency addresses:

	Address	**Currency Amount**
(a)	3Pja5FPK1wFB9LkWWJai8XYL1qjbqqT9Ye	20,452.85228 BTC
(b)	3FrM1He2ZDbsSKmYpEZQNGjFTLMgCZZkaf	14,111.92546835 BTC
(c)	3B1u4PsuFzww1P8if5jYmitXxpMs2EMSqt	2,999.09118947 BTC
(d)	3JJ8b7voMPSPChHazdHkrZMqxC7Cb4vNk2	1,000.08105870 BTC
(e)	3PWNGS2357TnjRX7FpewqR3e3qsWwpFrJH	0.00736862 BTC
(f)	34Jpa4Eu3ApoPVUKNTN2WeuXVVq1jzxgPi	14,139.260 BTC
(g)	338uPVW8drux5gSemDS4gFLSGrSfAiEvpX	9,099.01146835 BTC
(h)	3J4sTPyD1g6KvNUSJxjwLs4iaPeDPqxUZr	499.90936500 BTC
(i)	33uEsaGLcF9H46Dvzx1kMnuMCQ13ndkAjV	3,000.09125022 BTC
(j)	3KabDvdetZXDHNm9HXowLc9SppiSXKn7UU	9,500.99220072 BTC
(k)	38Md7BghVmV7XUUT1Vt9CvVcc5ssMD6ojt	15,033.29416267 BTC
(l)	3GaB3nRWA1PLc3XQkkbpVtFwYYZEuMxD4i	0.02415042 BTC
(m)	32i6n2vXhjvJg1vniURFy7A5VK6eG6oDgg	3,000.09118974 BTC
(n)	3HuUiXmKN3beQSoM97kWjK1fesWWJvKvaZ	4,500.00841044 BTC
(o)	34MFtk9iMxYcUPZWXHfiGfqz4o7X3kpJbV	0.5084661 BTC
(p)	3LjTXe31gepN8nW3AZyKpyD2QwbtmfjNwm	156.04996844 BTC
(q)	3MHa8JJ3bu8j3x3iQHhqsrZvk1EjBQmC78	2,700.44863780 BTC
(r)	3AWpzKtkHfWsiv9RGXKA3Z8951LefsUGXQ	10,500.04293955 BTC
(s)	34KYo7VdVr5CJ7m4hYhH9RpwqXhbsTrw4T	4,500.00941044 BTC
(t)	3DdFSGcXaP2rZ9CaL3tjnqRARvQ5K3VW4a	251.6000482 BTC
(u)	39B6oSa58qNpFMGpuowtRHAYp3fM4ghXRq	212.5930613 BTC
(v)	3NmHmQte2rP8pS54U3B8LPYQKkpG1pFF69	8,611.07446862 BTC

	Address	Currency Amount
(w)	3BA3PEF4BMoy9y3kdMRUdMhL8Gp24vikhF	2.16989588 BTC
(x)	389JrNcn8trYgYi2EtHi4X7bTCqtVbep86	1,500.01255361 BTC
(y)	339khCuymVi4FKbW9hCHkH3CQwdopXiTvA	1,500.00 BTC

and all proceeds traceable thereto.

61. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

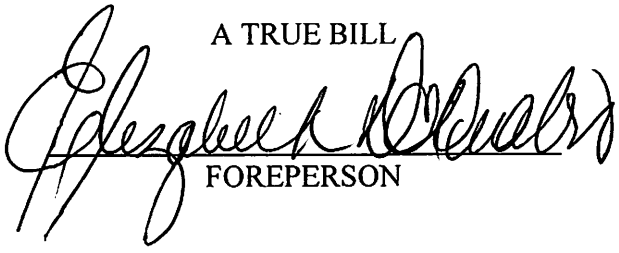
(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other

property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

A TRUE BILL



FOREPERSON

by Alexandra Smith, Assistant U.S. Attorney

JOSEPH NOCELLA, JR.
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK