AFM/NJM/BGK:ADR/BW/RMS/TRP
F. #2025V02069

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
– X

UNITED STATES OF AMERICA,

Plaintiff,

-against-

APPROXIMATELY 127,271 BITCOIN ("BTC") PREVIOUSLY STORED AT THE VIRTUAL CURRENCY ADDRESSES LISTED IN ATTACHMENT A, AND ALL PROCEEDS TRACEABLE THERETO,

Defendants *In Rem*.

– X

VERIFIED COMPLAINT IN REM

Civil Action No.

1:25-cv-05745(Cogan)

Plaintiff, United States of America, by its attorney, Joseph Nocella, Jr., United States Attorney for the Eastern District of New York, alleges upon information and belief as follows:

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit and condemn to the use and benefit of the United States the above-captioned defendant property and all proceeds traceable thereto (collectively, the "Defendants *In Rem*").

2. The Defendants *In Rem* are subject to forfeiture pursuant to: (a) 18 U.S.C. § 981(a)(1)(C), as property, real or personal, which constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343, or a conspiracy to commit such offense, in violation of 18 U.S.C. § 1349; and/or (b) 18 U.S.C. § 981(a)(1)(A), as property, real or personal, involved

in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property traceable to such property, or a conspiracy to commit such offense.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action commenced by the United States, pursuant to 28 U.S.C. § 1345, and over an action for forfeiture, pursuant to 28 U.S.C. § 1355.

4. Venue lies in the Eastern District of New York pursuant to 28 U.S.C. §§ 1355 and 1395 in that acts and omissions giving rise to the forfeiture accrued in the Eastern District of New York.

THE DEFENDANTS IN REM

5. The Defendants *In Rem* consist of the following:

(a) Approximately 127,271 bitcoin ("BTC") previously stored at the virtual currency addresses listed in Attachment A, and all proceeds traceable thereto (the "Defendant Cryptocurrency").

6. The Defendant Cryptocurrency is currently in the custody of the United States at virtual currency addresses known to the government.

RELEVANT STATUTES AND REGULATIONS

A. Wire Fraud

7. Pursuant to 18 U.S.C. § 1343, it is illegal to knowingly and intentionally devise a scheme or artifice to defraud others by means of one or more materially false or fraudulent pretenses, representations or promises, and for the purpose of executing such scheme or artifice, to transmit or cause to be transmitted by means of wire communication in interstate or foreign commerce, writings, signs, signals, pictures or sounds.

8. Pursuant to 18 U.S.C. § 1349, it is unlawful for any person to attempt or conspire to commit wire fraud contrary to 18 U.S.C. § 1343.

B. Money Laundering

9. Pursuant to 18 U.S.C. § 1956(a)(1)(B)(i), it is unlawful for anyone to conduct one or more financial transactions in and affecting interstate or foreign commerce, which transactions in fact involved the proceeds of one or more specified unlawful activities, 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 or in part to conceal and disguise the nature, location, source, ownership or control of the proceeds of specified unlawful activity.

10. Pursuant to 18 U.S.C. § 1956(a)(2)(B)(i), it is unlawful for anyone to transport, transmit, or transfer, or attempt to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States, knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of one or more specified unlawful activities.

11. Pursuant to 18 U.S.C. § 1956(h), it is unlawful for any person to conspire to commit any offense defined in 18 U.S.C. § 1956.

12. Pursuant to 18 U.S.C. § 1961(1)(B), as incorporated by 18 U.S.C. § 1956(c)(7)(A), the term "specified unlawful activity" includes violations of 18 U.S.C. §§ 1343 (wire fraud) and 1956 (money laundering).

C. Forfeiture Statutes

13. Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343, or any offense constituting specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7)), or a conspiracy to commit any such offenses, is subject to forfeiture to the United States.

14. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to forfeiture to the United States.

FACTS

A. Introduction

15. Since approximately 2015, Chen Zhi, also known as "Vincent," served as Chairman of Prince Holding Group ("Prince Group"), a Cambodian corporate conglomerate 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 seemingly legitimate 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.

B. Relevant Individuals and Entities

16. During the time period alleged herein, the following individuals and entities are described as follows:

a. Chen Zhi was a citizen of China, Cambodia, Vanuatu, St. Lucia and Cyprus and resided in Cambodia, Singapore, Taiwan and the United Kingdom.

b. Co-Conspirator-1 was a citizen of Cambodia, Vanuatu, Cyprus and St. Kitts and resided in Cambodia, Singapore and the United Kingdom.

c. Co-Conspirator-2 was a citizen of Cambodia and Cyprus and resided in Singapore and the United States.

d. Co-Conspirator-3 was a citizen of China and Cambodia and resided in the United States and elsewhere.

e. Co-Conspirator-4 was a citizen and resident of Cambodia.

f. Co-Conspirator-5 was a citizen and resident of Hong Kong.

g. Co-Conspirator-6 was a citizen and resident of Hong Kong.

h. Co-Conspirator-7 was a citizen and resident of Singapore.

i. Exchange-1 was a cryptocurrency exchange platform based in China.

j. Exchange-2 was a cryptocurrency exchange platform based in the Seychelles.

k. Exchange-3 was a cryptocurrency exchange platform based in the United States.

l. Exchange-4 was a cryptocurrency exchange platform based in the United States.

m. Trading Platform-1 was an online trading platform.

n. Financial Institution-1 was a financial institution based in the United States, the deposits of which were insured by the Federal Deposit Insurance Corporation ("FDIC").

o. Prince Group was a Cambodian-registered corporate holding company that operated more than 100 business entities in over thirty countries. Chen Zhi was the founder and Chairman of Prince Group.

p. 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.

q. 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.

r. 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.

s. 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.

t. Warp Data Technology Lao Sole Co., Ltd. ("Warp Data") was an entity registered in Laos that operated bitcoin mining facilities.

u. Lubian was a Chinese bitcoin mining operation that maintained bitcoin mining facilities across Asia, including in China and Iran.

v. Future Technology Investment ("FTI") was an entity incorporated in the Cayman Islands. Co-Conspirator-6 was the Director of FTI and was a signatory on its bank accounts.

w. Amber Hill Ventures Limited ("Amber Hill") was an entity incorporated in the British Virgin Islands. Co-Conspirator-6 was the Director of Amber Hill and was a signatory on its bank accounts.

x. Lateral Bridge Global Limited ("LBG") was an entity incorporated in the British Virgin Islands. Co-Conspirator-7, who was also affiliated with FTI and Amber Hill, was the Director of LBG.

y. Hing Seng Limited ("Hing Seng") was an entity incorporated in Hong Kong.

C. Relevant Terms and Definitions

17. During the time period alleged herein, the following terms had the following definitions:

a. "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.

b. Pig-butchering scams typically involved four stages. First, a perpetrator would use a fictitious 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.

c. "*Jingliao*," or "scripted chat," was a term commonly associated with pig-butchering scams.

d. "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.

e. "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.

f. "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.

g. "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.

h. 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.

i. 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 addresses. 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.

j. 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).

k. Each virtual currency address was controlled through the use of a unique corresponding "private key," a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key could authorize a transfer of virtual currency from that address to another address.

l. A "seed phrase" was a mnemonic passphrase made up of a series of apparently random words. A person in possession of a seed phrase could use it to reconstitute a private key, and thus to access the value stored at a cryptocurrency address.

D. The Criminal Schemes

i. Background

18. The rapidly growing scam industry across southeast Asia has caused billions of dollars in damages around the world. Over the past decade, extensive reporting in the news media and research by international human rights groups has detailed the trafficking of thousands of individuals across Asia into countries such as Cambodia, Laos and Myanmar, where they are forced to work for criminal syndicates executing mass cyberfraud schemes under the threat of physical violence. The most widely used technique among these operations is pig-butchering scams.

19. As a recent report observed, "transnational organized cybercrime is now the world's fastest growing and most dangerous illegal industry. Criminal syndicates are luring unsuspecting job seekers from over 70 countries and forcing them—alongside willing criminals—to perpetrate sophisticated fraud schemes targeting virtually every global jurisdiction, at scale."[1] In Cambodia, Laos and Myanmar alone, the cybercriminal labor force is believed to consist of

[1] Sims, J. (May 2025). *Policies and Patterns: State-Abetted Transnational Crime in Cambodia as a Global Security Threat*. Humanity Research Consultancy.

more than 350,000 people, with some estimates putting annual revenue generated by scam syndicates somewhere between $50 and $75 billion. As the report states, "this makes transnational fraud perhaps the most dominant economic activity in the entire Mekong sub-region [of Southeast Asia]—equivalent to nearly half of total GDP in the primary host countries." Cambodia's scam industry in particular is enormously profitable, with estimates ranging from $12.5 to $19 billion in illicit revenue annually.

20. From approximately 2015 to the present, Chen Zhi and top executives at Prince Group engaged in schemes to defraud victims around the world through fraudulent 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.

ii. <u>The Fraud Schemes</u>

21. 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 business sectors, including "real estate development, banking, finance, tourism, logistics, technology, food and beverages, and

lifestyle." However, Prince Group's largest profits came 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.

a. The Scam Compounds

22. In particular, Prince Group came to dominate the online scam industry discussed above, in which 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 violent forced labor camps.

23. At Chen'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").

24. Chen 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 fraudulent chats),

"Vietnamese," "Chinese" and "Taiwanese" "*jingliao*," and "Chinese brush order" (a reference to online retail fraud).

25. Chen 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. 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. 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.

26. 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.

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

27. Chen 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.

28. 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 Chen communicated at length about "risk control" issues and whom 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.

29. Chen 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.

30. 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 Chen 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."

31. Prince Group associates, at Chen'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.

a. The Brooklyn Network

32. 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 profiles and investment portfolios for them at mobile online trading platforms, including Trading Platform-1 and others.

33. 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.

34. Meanwhile, the trading profiles created by the Account Managers for the victims were manipulated to appear to reflect growing investments when in reality they were not increasing. 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.

35. 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. Among other methods, fraudulent victim proceeds were moved through shell company bank accounts, converted to USDT and then transferred to and through complex networks of unhosted virtual currency addresses. Other funds were withdrawn as cash to disrupt the audit trail. The cash was used to purchase cryptocurrency that was subsequently transferred in the same manner.

36. 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.

37. Chen also personally monitored activity in virtual currency addresses that received fraudulent proceeds, including from U.S.-based victims. For example, Chen maintained records describing a transfer of 100,000 USDT into a virtual currency address beginning with 0x77 (the "0x77 Address") in or about June 2021. That same address received funds directly traceable to a scam victim residing in California ("Victim-1") that same summer.[2]

[2] In particular, on or about and between July and August 2021, Victim-1 transferred more than $400,000 in cryptocurrency from Victim-1's account at a popular virtual currency exchange to an address beginning with 0x1e (the "0x1e Address"). The funds were subsequently transferred through an address beginning with 0x83 (the "0x83 Address") to an address beginning with 0x34 (the "0x34 Address"). On or about and between July and September 2021, the 0x34 Address sent more than $350,000 in USDT to the 0x77 Address that Chen was monitoring.

iii. The Money Laundering Schemes

38. Chen and his co-conspirators laundered Prince Group's illicit profits, including the Defendant Cryptocurrency, 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 extravagant 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.

39. 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 provided 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. Chen 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."

40. Chen 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. These companies included FTI, Amber Hill and LBG, among dozens of others. FTI was used to launder illicit funds, including through Warp Data, a Prince Group mining operation discussed further

below. In account opening records from January 2019 for an account controlled by FTI at Financial Institution-1, Co-Conspirator-6 described FTI's business activities as including "[m]ining, buying and selling digital assets of our of [sic] own capital," but falsely listed FTI's source of income as "[p]ersonal wealth." Co-Conspirator-6 also grossly understated FTI's monthly transaction activity in the same account opening documents, listing its anticipated deposit and withdrawal activity as approximately $2 million each. According to account statements, in February 2019, FTI's account at Financial Institution-1 instead had approximately $28 million in deposits and $27 million in withdrawals. Amber Hill was similarly used to launder illicit proceeds. As with FTI, Amber Hill had a banking relationship with Financial Institution-1. In March 2019 account opening records, Co-Conspirator-6 stated that Amber Hill's business activities consisted of "[p]roprietary trading and investing," and falsely listed Amber Hill's source of income as "[p]ersonal wealth." As with FTI, Co-Conspirator-6 significantly understated Amber Hill's monthly transaction activity in its account opening documents, similarly listing its anticipated deposit and withdrawal activity as approximately $2 million each. According to account statements, in February 2020, Amber Hill's account at Financial Institution-1 had approximately $22.5 million in deposits and $21.8 million in withdrawals.[3]

41. Chen and his co-conspirators also laundered illicit proceeds through functional Prince Group business units, and in particular its sprawling online gambling business,

[3] In or about 2023, Financial Institution-1 announced that it would cease banking operations and surrender its bank charter. In 2024, Financial Institution-1 announced settlements with the Board of Governors of the Federal Reserve System, the California Department of Financial Protection and Innovation, and the Securities and Exchange Commission in connection with alleged violations of its transaction monitoring obligations under the Bank Secrecy Act and other anti-money laundering regulations, particularly with respect to its cryptocurrency customers.

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."[4]

42. Additionally, Chen and his co-conspirators laundered illicit proceeds by using the proceeds to fund large-scale cryptocurrency mining operations, including the Laos-based Warp Data and its Texas-based subsidiary, and the China-based 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, "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. As one example, in or about and between November 2022 and March 2023 Warp Data received over $60 million from Hing Seng, a shell company that was also used to make

[4] According to the Humanity Research Consultancy report discussed above, "International observers consistently noted the vital role of gambling and money laundering infrastructure in the scale and intractability of scam compounds, among others in Cambodia. One key explanation offered by interviewees for these persistent gambling-criminal linkages is the gambling industry's secondary banking system which facilitates casino operations and frequently serves as a 'mixer'—co-mingling funds from different sources and making them difficult to track."

payments to the spouse of an Awesome Global executive and to purchase millions of dollars' worth of luxury items, including a Rolex watch and the Picasso painting referenced above. Chen and his co-conspirators also systematically combined illicit funds with newly mined cryptocurrency in wallets associated with mining operations to obscure the origins of those funds.

43. Chen 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, with no business purpose other than to obscure the source of the funds, as illustrated below. 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.[5] Other proceeds, including proceeds that had been laundered through Prince Group's mining operations, were stored in unhosted cryptocurrency wallets personally controlled by Chen.

[5] Because Exchange-1 does not respond to legal process from United States law enforcement, it is a favored exchange among overseas criminals, particularly in Asia, to launder illicit proceeds without detection by U.S. authorities. In this case, Prince Group executives were aware of, and discussed, the lack of cooperation between United States and Chinese law enforcement and were therefore aware of the lack of visibility United States authorities would have into transactions on Exchange-1.

E. The Defendants *In Rem*

44. By approximately 2020, Chen had amassed a vast sum of fraud proceeds packaged as heavily laundered cryptocurrency, including the Defendant Cryptocurrency, which was stored across 25 cryptocurrency addresses in unhosted wallets controlled and personally tracked by Chen (the "Chen Wallets"),[6] as listed below:[7]

The Chen Wallets

Address	Currency Amount
3Pja5FPK1wFB9LkWWJai8XYL1qjbqqT9Ye	20,452.85228 BTC
3FrM1He2ZDbsSKmYpEZQNGjFTLMgCZZkaf	14,111.92546835 BTC
3B1u4PsuFzww1P8if5jYmitXxpMs2EMSqt	2,999.09118947 BTC
3JJ8b7voMPSPChHazdHkrZMqxC7Cb4vNk2	1,000.08105870 BTC
3PWNGS2357TnjRX7FpewqR3e3qsWwpFrJH	0.00736862 BTC
34Jpa4Eu3ApoPVUKNTN2WeuXVVq1jzxgPi	14,139.260 BTC
338uPVW8drux5gSemDS4gFLSGrSfAiEvpX	9,099.01146835 BTC
3J4sTPyD1g6KvNUSJxjwLs4iaPeDPqxUZr	499.90936500 BTC
33uEsaGLcF9H46Dvzx1kMnuMCQ13ndkAjV	3,000.09125022 BTC
3KabDvdetZXDHNm9HXowLc9SppiSXKn7UU	9,500.99220072 BTC
38Md7BghVmV7XUUT1Vt9CvVcc5ssMD6ojt	15,033.29416267 BTC

[6] Chen personally maintained records of the wallet addresses and seed phrases associated with the private keys for each.

[7] This table identifies the addresses at which the Defendant Cryptocurrency was stored as of December 2020. The addresses contained the Defendant Cryptocurrency and no other funds. As discussed below, the Defendant Cryptocurrency is now stored at addresses controlled by the government.

Address	Currency Amount
3GaB3nRWA1PLc3XQkkbpVtFwYYZEuMxD4i	0.02415042 BTC
32i6n2vXhjvJg1vniURFy7A5VK6eG6oDgg	3,000.09118974 BTC
3HuUiXmKN3beQSoM97kWjK1fesWWJvKvaZ	4,500.00841044 BTC
34MFtk9iMxYcUPZWXHfiGfqz4o7X3kpJbV	0.5084661 BTC
3LjTXe31gepN8nW3AZyKpyD2Qwbtmfj Nwm	156.04996844 BTC
3MHa8JJ3bu8j3x3iQHhqsrZvk1EjBQmC78	2,700.44863780 BTC
3AWpzKtkHfWsiv9RGXKA3Z8951LefsUGXQ	10,500.04293955 BTC
34KYo7VdVr5CJ7m4hYhH9RpwqXhbsTrw4T	4,500.00941044 BTC
3DdFSGcXaP2rZ9CaL3tjnqRARvQ5K3VW4a	251.6000482 BTC
39B6oSa58qNpFMGpuowtRHAYp3fM4ghXRq	212.5930613 BTC
3NmHmQte2rP8pS54U3B8LPYQKkpG1pFF69	8,611.07446862 BTC
3BA3PEF4BMoy9y3kdMRUdMhL8Gp24vikhF	2.16989588 BTC
389JrNcn8trYgYi2EtHi4X7bTCqtVbep86	1,500.01255361 BTC
339khCuymVi4FKbW9hCHkH3CQwdopXiTvA	1,500.00 BTC

45. Personnel from the Federal Bureau of Investigation ("FBI") have conducted extensive blockchain tracing to analyze the movements of the Defendant Cryptocurrency, as described below. That tracing has determined that the above addresses were primarily funded by two categories of sources: (1) cryptocurrency mining, including addresses associated with Lubian and Warp Data; and (2) indirect transfers from wallets at centralized cryptocurrency exchanges,

including wallets at Exchange-1 and Exchange-2, and wallets at additional exchanges controlled by FTI, Amber Hill, LBG and other shell companies.[8]

46. FBI cryptocurrency analysts have determined that the addresses composing the Chen Wallets can be grouped into thirteen clusters of one or more addresses ("Cluster Index-1" through "Cluster Index-13"), as identified below, with addresses within the same cluster exhibiting similar funding patterns.

Cluster Index	Address
1	3Pja5FPK1wFB9LkWWJai8XYL1qjbqqT9Ye
2	3FrM1He2ZDbsSKmYpEZQNGjFTLMgCZZkaf
3	3JJ8b7voMPSPChHazdHkrZMqxC7Cb4vNk2 3B1u4PsuFzww1P8if5jYmitXxpMs2EMSqt
4	3J4sTPyD1g6KvNUSJxjwLs4iaPeDPqxUZr 34Jpa4Eu3ApoPVUKNTN2WeuXVVq1jzxgPi 338uPVW8drux5gSemDS4gFLSGrSfAiEvpX 3PWNGS2357TnjRX7FpewqR3e3qsWwpFrJH
5	33uEsaGLcF9H46Dvzx1kMnuMCQ13ndkAjV 32i6n2vXhjvJg1vniURFy7A5VK6eG6oDgg 3KabDvdetZXDHNm9HXowLc9SppiSXKn7UU 38Md7BghVmV7XUUT1Vt9CvVcc5ssMD6ojt 3HuUiXmKN3beQSoM97kWjK1fesWWJvKvaZ 3GaB3nRWA1PLc3XQkkbpVtFwYYZEuMxD4i

[8] In this paragraph and the paragraphs that follow, "indirect transfers" means transfers in which the funds passed through unhosted intermediary wallets before arriving in the referenced destinations.

Cluster Index	Address
6	34MFtk9iMxYcUPZWXHfiGfqz4o7X3kpJbV
7	3MHa8JJ3bu8j3x3iQHhqsrZvk1EjBQmC78 3LjTXe31gepN8nW3AZyKpyD2QwbtmfjNwm 34KYo7VdVr5CJ7m4hYhH9RpwqXhbsTrw4T 3AWpzKtkHfWsiv9RGXKA3Z8951LefsUGXQ
8	3DdFSGcXaP2rZ9CaL3tjnqRARvQ5K3VW4a
9	39B6oSa58qNpFMGpuowtRHAYp3fM4ghXRq
10	3NmHmQte2rP8pS54U3B8LPYQKkpG1pFF69
11	3BA3PEF4BMoy9y3kdMRUdMhL8Gp24vikhF
12	389JrNcn8trYgYi2EtHi4X7bTCqtVbep86
13	339khCuymVi4FKbW9hCHkH3CQwdopXiTvA

47. In particular, the clusters exhibited the following funding patterns:

a. Cluster Index-1 contained approximately 20,675.83 BTC and was funded primarily by bitcoin mining proceeds, indirect transfers from wallets at Exchange-1, and indirect transfers from other hosted wallets controlled by FTI, Amber Hill and LBG.

b. Cluster Index-2 contained approximately 14,000.02 BTC and was funded primarily by bitcoin mining proceeds, indirect transfers from wallets at Exchange-1, and indirect transfers from other hosted wallets controlled by FTI and Amber Hill.

c. Cluster Index-3 contained approximately 3,999.09 BTC and was funded primarily by indirect transfers from wallets at Exchange-1.

d. Cluster Index-4 contained approximately 23,738.17 BTC and was funded primarily by bitcoin mining proceeds and indirect transfers from wallets at Exchange-1 and Exchange-2, including wallets at Exchange-2 controlled by LBG.[9]

e. Cluster Index-5 contained approximately 35,034.43 BTC and was funded primarily by indirect transfers from wallets at Exchange-1 and indirect transfers from other hosted wallets controlled by FTI and LBG.

f. Cluster Index-6 contained approximately 0.5084661 BTC and was funded primarily by indirect transfers from wallets at Exchange-1.

g. Cluster Index-7 contained approximately 17,855.74 BTC and was funded primarily by indirect transfers from wallets at Exchange-1 and Exchange-2, as well as by bitcoin mining proceeds.

h. Cluster Index-8 contained approximately 251.51 BTC and was funded primarily by indirect transfers from wallets at Exchange-1 and Exchange-2, and transfers from "unnamed services," which are address clusters that exhibit exchange-like behavior but that cannot be traced to any known cryptocurrency service.

i. Cluster Index-9 contained approximately 212.50 BTC and was funded primarily by transfers from unnamed services.

[9] Tracing determined that all four addresses in Cluster Index-4 were associated with Lubian (in particular, one address showed a "Lubian.com" notation on the blockchain and the remaining three co-spent with that address, demonstrating shared ownership). However, unlike most addresses associated with mining operations, these addresses received large sums of cryptocurrency from sources unrelated to new mining. In fact, while addresses associated with most mining operations are funded almost entirely by newly mined cryptocurrency (generally more than 80-90%), Lubian's addresses were only 30% funded by newly mined cryptocurrency, which is highly unusual and suggests the commingling of funds for the purpose of laundering.

j. Cluster Index-10 contained approximately 8,500.00 BTC and was funded primarily by transfers from unnamed services.

k. Cluster Index-11 contained approximately 2.17 BTC and was funded primarily by bitcoin mining proceeds.

l. Cluster Index-12 contained approximately 1,500.01 BTC and was funded primarily by indirect transfers from wallets at Exchange-1.

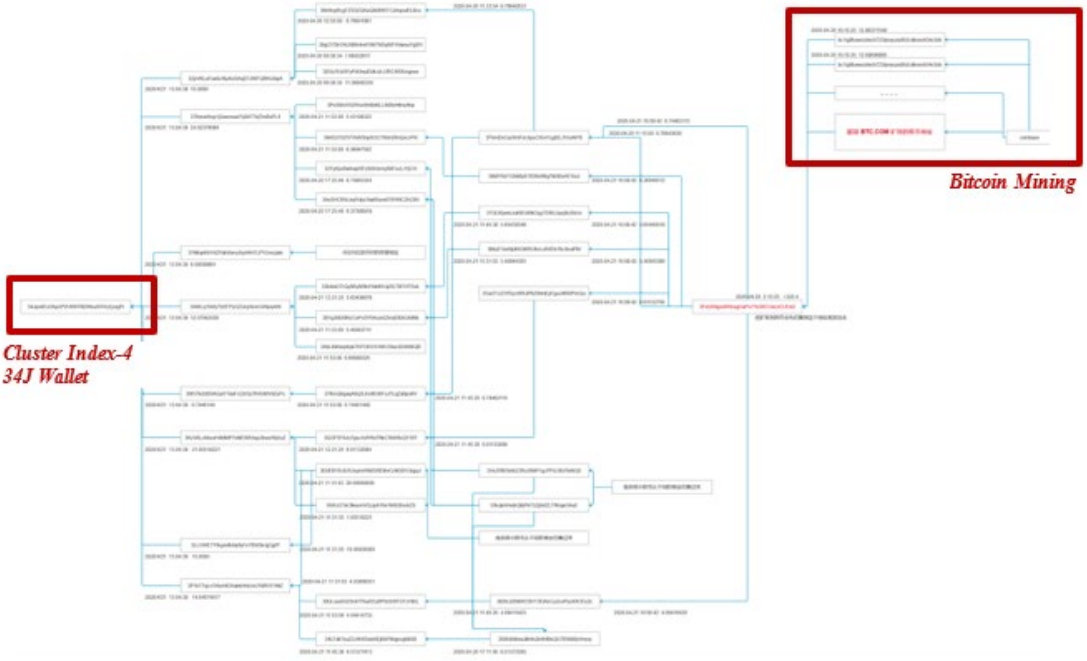
m. Cluster Index-13 contained approximately 1,499.99 BTC and was funded primarily by indirect transfers from wallets at Exchange-1.

48. The Defendant Cryptocurrency was moved across a complex network of hosted and unhosted cryptocurrency wallets affiliated with various shell companies and individuals through a process of high-volume disaggregation and funneling before it ultimately converged into the Chen Wallets. These patterns were consistent with known money laundering typologies and were apparently designed to disassociate funds from their illicit sources, complicate the audit trail and hide the illicit origins of the funds.

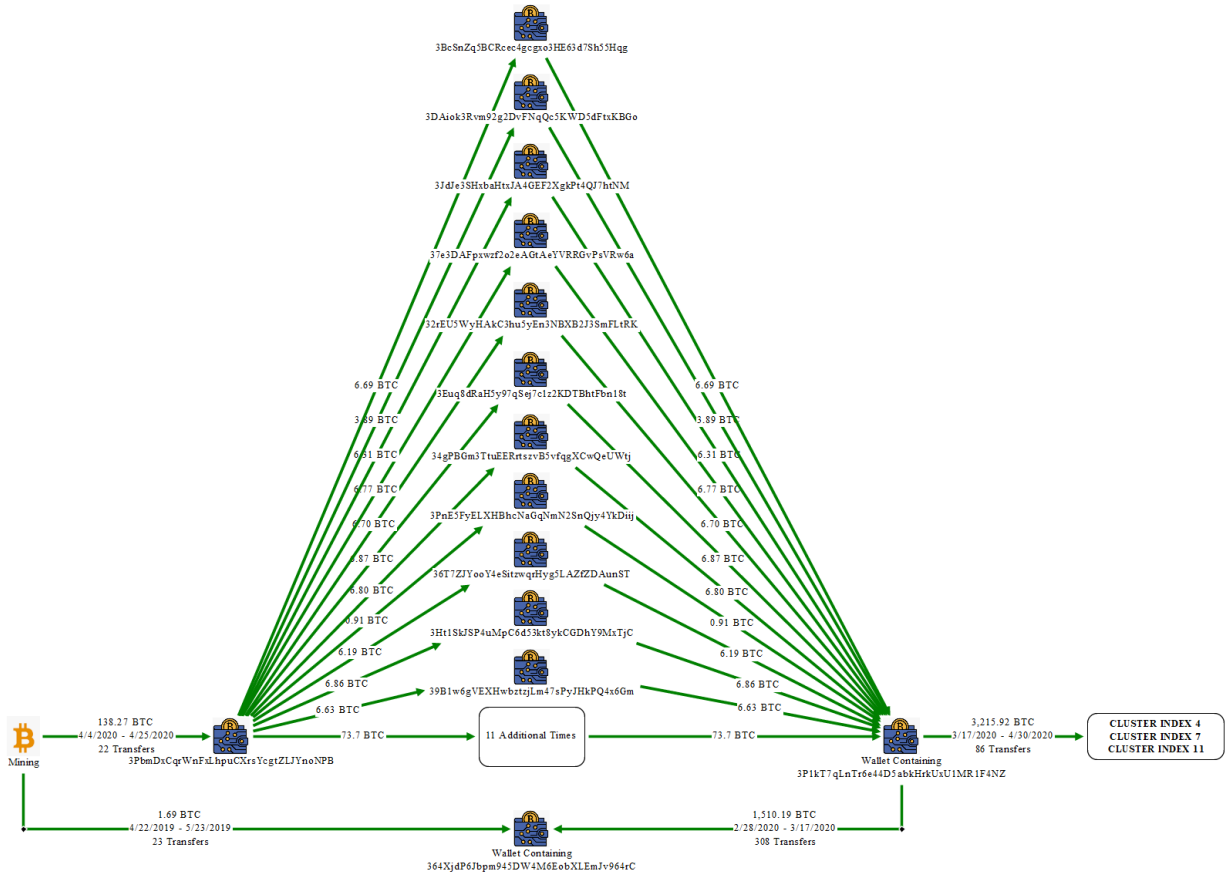
49. For example, approximately 61,230.03 BTC, nearly half of the Defendant Cryptocurrency, was transferred to the Chen Wallets through three sets of transactions, described below.

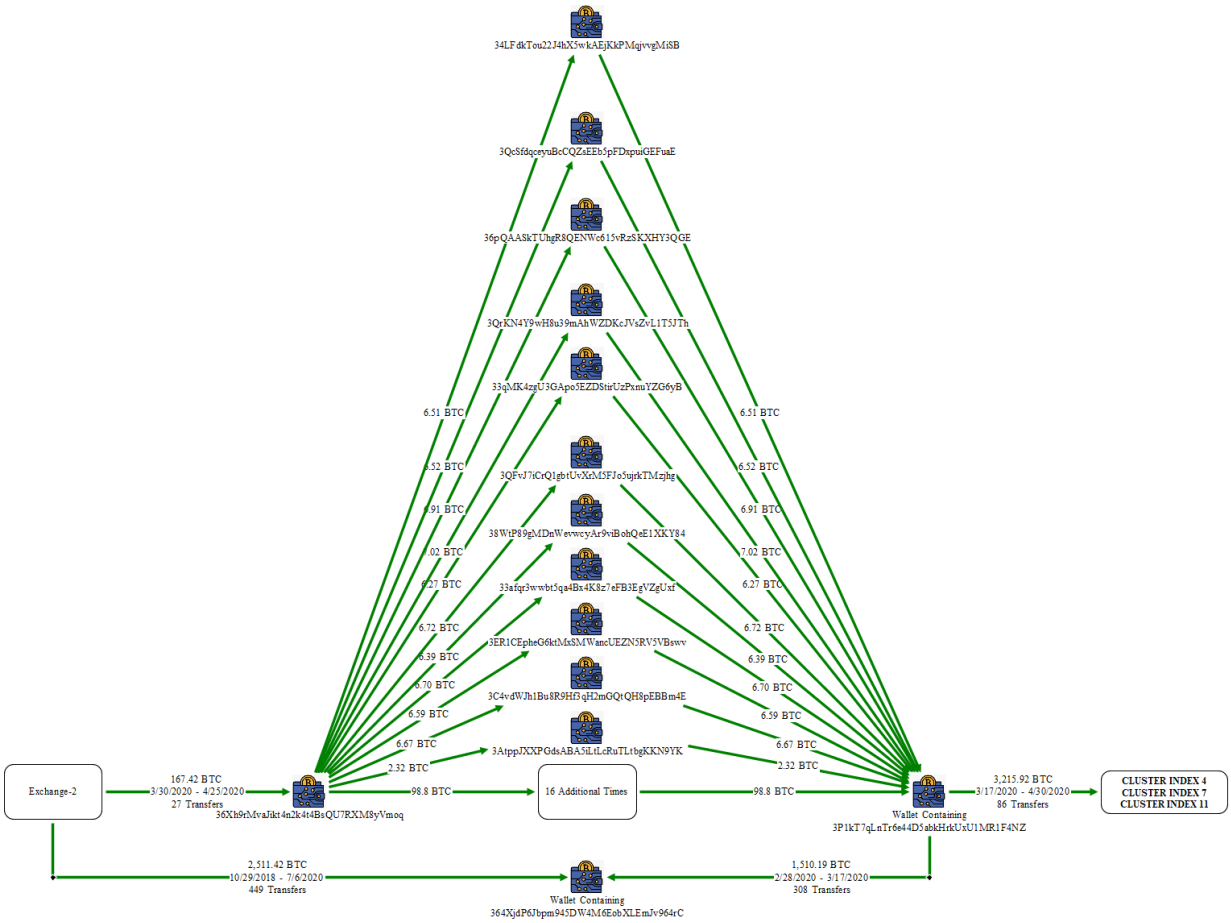
50. *Transaction Set 1*. On or about and between April 24, 2020 and December 28, 2020, approximately 11,115.83 newly mined bitcoin were sent directly to Cluster Index-4 address 34Jpa4Eu3ApoPVUKNTN2WeuXVVq1jzxgPi (the "34J Wallet") in approximately 1,477 separate transactions, as depicted below.

51. Cluster Index-4 also received mining proceeds indirectly after extensive disaggregating and funneling of the funds to obscure their source. For example, the below chart, kept by Chen, traces funds (from right to left) from a bitcoin mining operation through a convoluted series of steps in which the funds were dispersed across multiple addresses and subsequently funneled back into one single address, the 34J Wallet in Cluster Index-4 described above.



52. Blockchain tracing identified several additional examples involving wallets in the above image in which funds were split into dozens of addresses, only to be funneled into one address, and then passed along to the Chen Wallets. The first diagram below, created by the FBI, depicts funds from a bitcoin mining pool that were divided across 22 separate addresses, recombined into one address (the "Funneling Address"), and transferred to Chen Wallet addresses in Cluster Indices 4, 7 and 11. The second diagram below, also created by the FBI, depicts funds from Exchange-2 divided into 27 separate addresses, recombined into that same Funneling Address, and then transferred to Chen Wallet addresses in Cluster Index-4. This pattern repeated itself multiple times and functioned to make tracing the funds more difficult. In each case, funds were also sent from the Funneling Address to an unhosted wallet containing address 364XjdP6Jbpm945DW4M6EobXLEmJv964rC (the "364 Wallet"), which funded multiple Cluster Indices, as described further below.


3BcSnZq5BCRcec4gcgxo3HE63d7Sh55Hqg
3DAiok3Rvm92g2DvFNqQc5KWD5dFtxKBGo
3JdJe3SHxbaHtxJA4GEF2XgkPt4QJ7htNM
37e3DAFpxwzf2e2eAGtAeYVRRGvPsVRw6a
32rEU5WyHAkC3hu5yEn3NBXB2J3SmFLtRK
3Euq8dRaH5y97qSej7c1z2KDTBhtFbn18t
34gPBGm3TtuEERrtszvB5vfqgXCwQeUWtj
3PnE3FyELXHBhcNaGqNmN2SnQjy4YkDitj
36T7ZJYooY4eSitzwqtHyg5LAZfZDAunST
3Ht1SkJSP4uMpC6d5kt8ykCGDhY9MxTjC
39B1w6gVEXHwbztzjLm47sPyJHkPQ4x6Gm
6.69 BTC
3.89 BTC
6.31 BTC
6.77 BTC
6.70 BTC
6.87 BTC
6.80 BTC
0.91 BTC
6.19 BTC
6.86 BTC
6.63 BTC
Mining
138.27 BTC
4/4/2020 - 4/25/2020
22 Transfers
3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPB
73.7 BTC
11 Additional Times
73.7 BTC
Wallet Containing
3P1kT7qLnTr6e44D5abkHrkUxU1MR1F4NZ
3,215.92 BTC
3/17/2020 - 4/30/2020
86 Transfers
CLUSTER INDEX 4
CLUSTER INDEX 7
CLUSTER INDEX 11
1.69 BTC
4/22/2019 - 5/23/2019
23 Transfers
Wallet Containing
364XjdP6Jbpm945DW4M6EobXLEmJv964rC
1,510.19 BTC
2/28/2020 - 3/17/2020
308 Transfers



53. Further investigation of the Funneling Address indicated that the timing and amounts of the funds originating from Exchange-2 very closely mirrored the timing and amounts of the funds originating from the bitcoin mining pool, as illustrated in the selected transactions below:

Origination	Asset	Date (UTC)	Destination Address	Amount (BTC)
Mining Pool	BTC	4/4/2020 2:57	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	3.893368
Exchange-2	BTC	4/4/2020 11:04	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.912689
Mining Pool	BTC	4/5/2020 2:30	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.830337
Exchange-2	BTC	4/5/2020 10:38	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.715072
Mining Pool	BTC	4/6/2020 2:39	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.723102
Exchange-2	BTC	4/6/2020 7:10	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.670902
Mining Pool	BTC	4/7/2020 3:21	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.770778
Exchange-2	BTC	4/7/2020 8:56	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.732440
Mining Pool	BTC	4/8/2020 3:09	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	7.019560
Exchange-2	BTC	4/8/2020 9:51	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.705535
Mining Pool	BTC	4/9/2020 3:44	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.861649
Exchange-2	BTC	4/9/2020 10:13	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.518136
Mining Pool	BTC	4/10/2020 2:42	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.685891
Exchange-2	BTC	4/10/2020 11:09	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.390689
Mining Pool	BTC	4/11/2020 3:03	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.698781
Exchange-2	BTC	4/11/2020 8:20	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.427371
Mining Pool	BTC	4/12/2020 1:52	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.462614
Exchange-2	BTC	4/12/2020 9:42	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.261473
Mining Pool	BTC	4/13/2020 2:15	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.550203
Exchange-2	BTC	4/13/2020 8:19	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.271436
Mining Pool	BTC	4/14/2020 3:13	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.670280
Exchange-2	BTC	4/14/2020 9:01	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.542837
Mining Pool	BTC	4/15/2020 2:19	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.631315
Exchange-2	BTC	4/15/2020 8:34	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.595241
Mining Pool	BTC	4/16/2020 2:44	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.655603
Exchange-2	BTC	4/16/2020 8:59	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.480370
Mining Pool	BTC	4/17/2020 3:24	3PbmDxCqrWnFxLhpuCXrsYcgtZLJYnoNPE	6.768991
Exchange-2	BTC	4/17/2020 9:31	36Xh9rMvaJikt4n2k4t4BsQU7RXM8yVmoq	6.548593

54. The extensive spraying and funneling activity, together with the common transfer timing and amounts, indicates that the bitcoin sourced from Exchange-2 was deliberately moved in a manner that would mimic the patterns of funds originating from the mining pool. This had the effect of commingling bitcoin from Exchange-2 with mining proceeds and obfuscating the true origin of the Exchange-2 funds.

55. *Transaction Set 2*. On or about and between May 31, 2019 and May 9, 2020, over 20,000 newly mined bitcoin were sent through hosted wallets controlled by FTI and

Amber Hill, in accounts created by Co-Conspirator-6, and ultimately funneled to the 364 Wallet discussed above. Additional mining proceeds were sent directly to the 364 Wallet. Following the above transfers, approximately 26,115.2 BTC was transferred from the 364 Wallet to the Chen Wallet address in Cluster Index-1. In particular:

a. On or about and between May 31, 2019 and March 29, 2020, approximately 13,469 newly minted BTC were sent to address 3QLeXx1J9Tp3TBnQyHrhVxne9KqkAS9JSR (the "3QL Wallet"). Those proceeds passed to the 364 Wallet both directly and circuitously before ultimately settling in the Chen Wallet address in Cluster Index-1.

b. In particular, on or about and between July 18, 2019 and September 30, 2019, the 3QL Wallet sent approximately 2,138.4 BTC to the 364 Wallet.

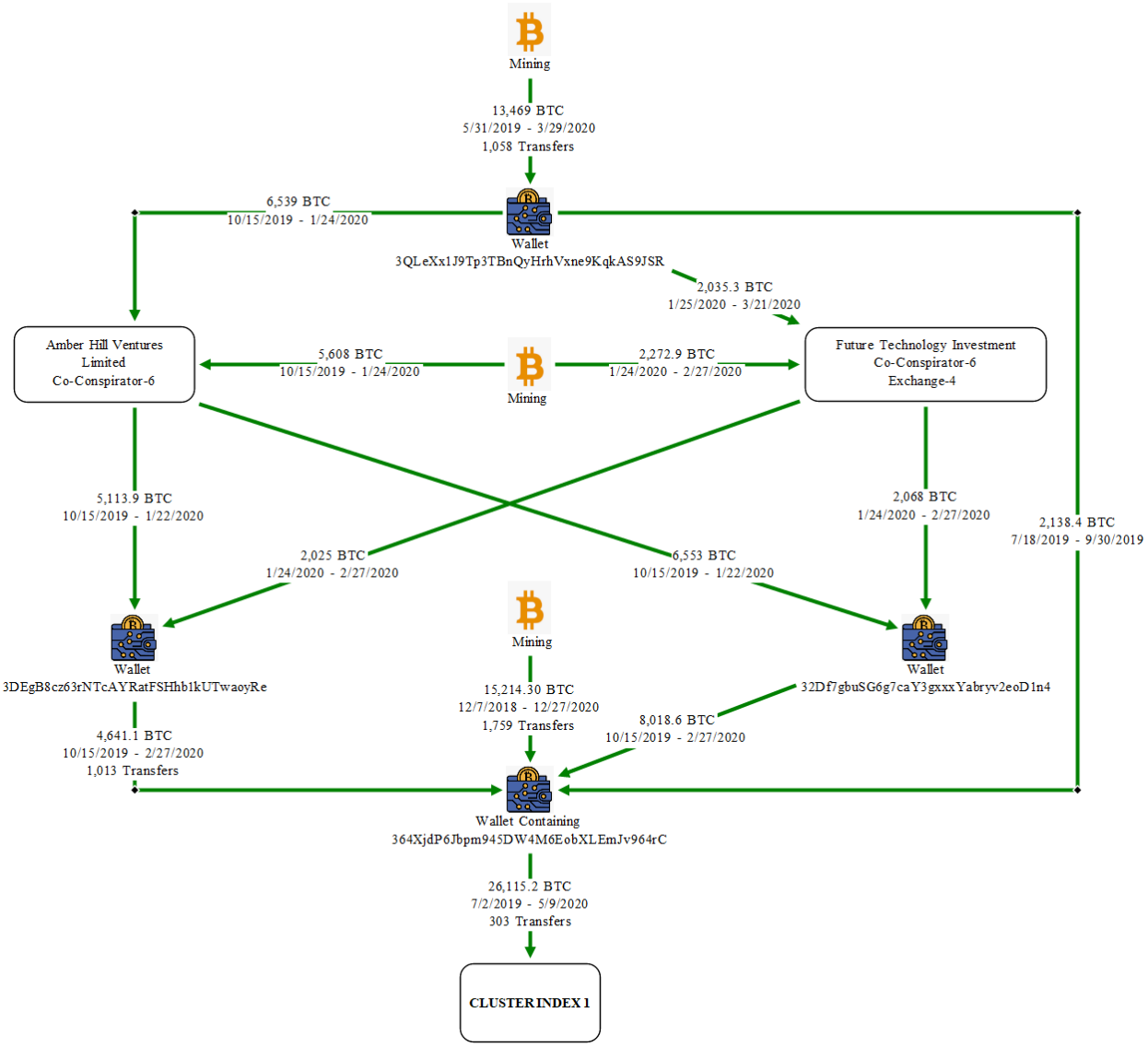
c. On or about and between October 15, 2019 and January 24, 2020, the 3QL Wallet sent approximately 6,539 BTC to a wallet at Exchange-3 controlled by Amber Hill (which also received approximately 5,608 BTC from bitcoin mining during that same approximate timeframe). Also during that same approximate timeframe, Amber Hill's wallet at Exchange-3 sent approximately 6,553 BTC to address 32Df7gbuSG6g7caY3gxxxYabryv2eoD1n4 (the "32D Wallet") and approximately 5,113.9 BTC to address 3DEgB8cz63rNTcAYRatFSHhb1kUTwaoyRe (the "3DE Wallet").

d. On or about and between January 25, 2020 and March 21, 2020, the 3QL Wallet sent approximately 2,035.3 BTC to a wallet at Exchange-4 controlled by FTI (which also received approximately 2,272.9 BTC from bitcoin mining during that same approximate timeframe). Also during that same approximate timeframe, FTI's wallet at Exchange-4 sent approximately 2,068 BTC to the 32D Wallet and approximately 2,025 BTC to the 3DE Wallet.

e. On or about and between October 15, 2019 and February 27, 2020, the 32D Wallet sent approximately 8,018.6 BTC to the 364 Wallet and the 3DE Wallet sent approximately 4,641.1 BTC to the 364 Wallet.

f. On or about and between December 7, 2018 and December 27, 2020, approximately 15,214.30 newly mined BTC were transferred directly to the 364 Wallet.

g. On or about and between July 2, 2019 and May 9, 2020, approximately 26,115.2 BTC was transferred from the 364 Wallet to the sole address in Cluster Index-1. Transaction Set 2 is depicted below.



56. *Transaction Set 3.* On or about and between April 7, 2018 and July 29, 2018, approximately 41,793.2 BTC was transferred from wallets at Exchange-1 to four addresses associated with the same wallet: 1FaUfrUhv37aqFAZ9ij595587wtnGWBFKS; 13vGS7YsuHv166D5pGqJD1X8xS9ib2TrA1; 18Uh5uHapoWqCJiZxoDnfGvPpzkDDeZgXo; and 19Pm9qTzQ3APKXnJLqdswd4HxpmqtPV3sy. That wallet made five transfers on or about

April 5, 2019 to Chen Wallet addresses in Cluster Indices 1, 3 and 5, totaling 23,999 BTC, as depicted below.

57. The patterns described above with respect to the Defendant Cryptocurrency are strongly indicative of money laundering. They are also consistent with other financial data maintained by Chen and his associates and analyzed by the FBI during the course of its investigation. For example, internal Prince Group documents maintained by Chen and others suggest that as of January 2024, total annual revenue from legitimate business operations across Prince Group's holdings likely did not exceed several hundred million dollars. Indeed, some key Prince Group entities were struggling and maintained negative cash flows. By contrast, for example, Co-Conspirator-2 stated that Prince Group was earning over $30 million a day in 2018 from fraudulent *sha zhu pan* schemes and related illicit activities, an amount which annualizes to approximately $11 billion.

58. The Defendant Cryptocurrency was subsequently transferred in its entirety to multiple additional addresses. It is currently in the custody of the United States.

F. Criminal and Regulatory Actions

59. On or about October 8, 2025, a grand jury sitting in the Eastern District of New York returned an indictment charging Chen with wire fraud conspiracy and money laundering conspiracy for directing and overseeing Prince Group's scam compound operations and other illicit

activities. A copy of the indictment is attached hereto as Attachment B and is incorporated by reference. The indictment was unsealed on October 14, 2025. That same day, on or about October 14, 2025, the United States Department of Treasury's Office of Foreign Assets Control ("OFAC") designated the Prince Group Transnational Criminal Organization ("Prince Group TCO") and placed Prince Holding Group and many of its affiliates, which included more than 100 corporate entities, and more than one dozen employees and officers of entities owned or controlled by Prince Group TCO or its members, including Chen and several of his co-conspirators, on the Specially Designated Nationals and Blocked Persons List (the "SDN List"). As a result of OFAC's designation, a block was placed on all property of the SDN List designees subject to United States jurisdiction, and all United States persons or persons within the United States were prohibited from transacting business with the SDN List designees without a license from OFAC. The OFAC designation also caused financial institutions to freeze bank accounts held by Prince Group, Chen and others.

FIRST CLAIM FOR RELIEF
(Proceeds Traceable to Wire Fraud)

60. Plaintiff repeats and realleges each and every allegation contained in paragraphs 1 through 59 as if fully set forth herein.

61. The Defendant Cryptocurrency represents property, real or personal, which constitutes or is derived from proceeds traceable to an offense constituting a "specified unlawful activity," which includes wire fraud, in violation of 18 U.S.C. § 1343, or a conspiracy to commit such offenses, in violation of 18 U.S.C. § 1349.

62. As a result, the Defendant Cryptocurrency is liable to condemnation and forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

SECOND CLAIM FOR RELIEF
(Property Involved in Money Laundering)

63. Plaintiff repeats and realleges each and every allegation contained in paragraphs 1 through 59 as if fully set forth herein.

64. The Defendant Cryptocurrency represents property involved in or traceable to property involved in a transaction or attempted transaction of money laundering, or a conspiracy to commit such offenses, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i) and 1956(h).

65. As a result, the Defendant Cryptocurrency is liable to condemnation and forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

WHEREFORE, plaintiff the United States of America requests that: warrants be issued by the Clerk of Court for the arrest of the Defendant Cryptocurrency; due process issue to enforce the forfeiture of the Defendant Cryptocurrency; that due notice of these proceedings be given to all interested persons to appear and show cause why forfeiture should not decreed; that this Court decree that the Defendant Cryptocurrency be forfeited and condemned to the use of the United States for disposition according to law; that the Plaintiff be awarded its costs and

disbursements in this action, and for such other and further relief as the Court may deem just and proper.

Dated: Brooklyn, New York
October 14, 2025

JOSEPH NOCELLA, JR.
United States Attorney
Attorney for Plaintiff
Eastern District Of New York
271-A Cadman Plaza East
Brooklyn, New York 11201

BY: */s/ Tanisha R. Payne*
Alexander F. Mindlin
Andrew D. Reich
Benjamin Weintraub
Rebecca M. Schuman
Tanisha R. Payne
Assistant United States Attorneys
(718) 254-7000

JOHN A. EISENBERG
Assistant Attorney General
Attorney for Plaintiff
National Security Division
United States Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

BY: */s/ Christopher B. Brown*
Christopher B. Brown
Deputy Chief
National Security Cyber Section
(202) 353-0018

VERIFICATION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and, as such, have knowledge of the facts underlying this action.

2. I have read the within Verified Complaint *In Rem* and know the contents thereof.

3. The matters contained in the within Verified Complaint *In Rem* are true and accurate to the best of my knowledge, information and belief.

4. The source of my information and the grounds for my belief are my personal knowledge and information provided by other law enforcement officers, FBI personnel, witnesses and financial institutions.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief.

Dated: October 9, 2025

Charles Lee
Special Agent
Federal Bureau of Investigation

Attachment A

Address
3Pja5FPK1wFB9LkWWJai8XYL1qjbqqT9Ye
3FrM1He2ZDbsSKmYpEZQNGjFTLMgCZZkaf
3B1u4PsuFzww1P8if5jYmitXxpMs2EMSqt
3JJ8b7voMPSPChHazdHkrZMqxC7Cb4vNk2
3PWNGS2357TnjRX7FpewqR3e3qsWwpFrJH
34Jpa4Eu3ApoPVUKNTN2WeuXVVq1jzxgPi
338uPVW8drux5gSemDS4gFLSGrSfAiEvpX
3J4sTPyD1g6KvNUSJxjwLs4iaPeDPqxUZr
33uEsaGLcF9H46Dvzx1kMnuMCQ13ndkAjV
3KabDvdetZXDHNm9HXowLc9SppiSXKn7UU
38Md7BghVmV7XUUT1Vt9CvVcc5ssMD6ojt
3GaB3nRWA1PLc3XQkkbpVtFwYYZEuMxD4i
32i6n2vXhjvJg1vniURFy7A5VK6eG6oDgg
3HuUiXmKN3beQSoM97kWjK1fesWWJvKvaZ
34MFtk9iMxYcUPZWXHfiGfqz4o7X3kpJbV
3LjTXe31gepN8nW3AZyKpyD2QwbtmfjNwm
3MHa8JJ3bu8j3x3iQHhqsrZvk1EjBQmC78
3AWpzKtkHfWsiv9RGXKA3Z8951LefsUGXQ
34KYo7VdVr5CJ7m4hYhH9RpwqXhbsTrw4T
3DdFSGcXaP2rZ9CaL3tjnqRARvQ5K3VW4a
39B6oSa58qNpFMGpuowtRHAYp3fM4ghXRq
3NmHmQte2rP8pS54U3B8LPYQKkpG1pFF69
3BA3PEF4BMoy9y3kdMRUdMhL8Gp24vikhF
389JrNcn8trYgYi2EtHi4X7bTCqtVbep86
339khCuymVi4FKbW9hCHkH3CQwdopXiTvA

Attachment B

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

INDICTMENT

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

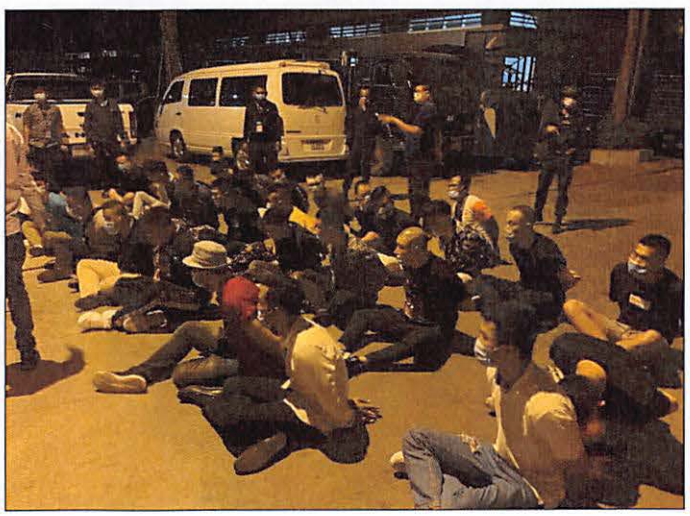
there were law enforcement crackdowns at the scam compounds, nothing happened to "us," referring to Prince Group. Co-Conspirator-2 and the defendant CHEN ZHI communicated at length about "risk control" issues and which officials from the MPS Co-Conspirator-2 was in touch with. CHEN also boasted to others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

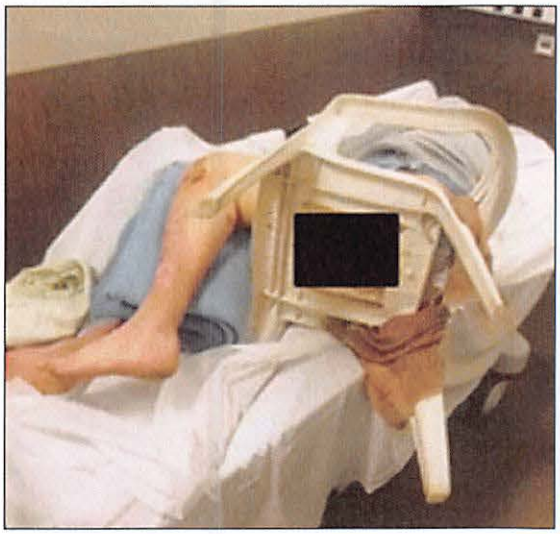
38. The defendant CHEN ZHI maintained ledgers of bribes to public officials, including a ledger that tracked hundreds of millions of dollars in reimbursements to Prince Group associates for bribes and luxury purchases. The ledger indicated, for example, that in 2019, Co-Conspirator-2 purchased a yacht 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

s/

FOREPERSON

by Alixandra Smith, Assistant U.S. Attorney

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