UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	**Civil Action No. 24-cv-2063**
2,546,415.01 USDT SEIZED FROM TWO BINANCE ACCOUNTS WITH USER IDS ENDING IN 9186 AND 5164,	)	
	)	
Defendant.	)	
	)	

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

Plaintiff, the United States of America, through the U.S. Attorney for the District of Columbia, brings this verified complaint for forfeiture in a civil action *in rem* against 2,546,415.01 in Tether cryptocurrency, hereinafter Defendant Property, and alleges as follows:

JURISDICTION AND VENUE

1. This Court has original jurisdiction of this civil action by virtue of 28 U.S.C. § 1345 because it has been commenced by the United States and by virtue of 28 U.S.C. § 1355(a) because it is an action for the recovery and enforcement of a forfeiture under an Act of Congress.

2. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b).

3. Venue is proper in this judicial district under 18 U.S.C. § 3238 and 28 U.S.C. §§ 1355(b) and 1395(a), (b), and (c).

NATURE OF THE ACTION AND STATURY BASIS FOR FORFEITURE

4. The United States files this *in rem* forfeiture action to seek forfeiture of Defendant Property as constituting proceeds of wire fraud and wire fraud conspiracy offenses, committed in

violation of 18 U.S.C. §§ 1343, 1349, 2, and 3, and as involved in money laundering and money laundering offenses, committed in violation of 18 U.S.C. 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 2, and 3.

5. Procedures for this action are mandated by Rule G of the supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981 and 983 and the Federal Rules of Civil Procedure.

6. 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957 or 1960, or any property traceable to such property.

7. 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, or any offense constituting "specified unlawful activity" as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offense. A violation of 18 U.S.C. § 1343, or a conspiracy to commit that offense, constitutes specified unlawful activity under 18 U.S.C. § 1956(c)(7)(A) as an offense listed in 18 U.S.C. § 1961(1)(B).

8. Title 18 U.S.C. § 1343 provides that whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, commits the violation of wire fraud.

9. Title 18 U.S.C. § 1349 provides that whoever attempts or conspires to commit a violation of 18 U.S.C. § 1343 shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

10. Title 18 U.S.C. § 1956(a)(1)(B)(i) provides in relevant part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity— . . . knowing that the transaction 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 specified unlawful activity" is guilty concealment money laundering.

11. Title 18 U.S.C. § 1956(a)(2)(B)(i) provides that whoever transports, transmits, or transfers, or attempts 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 specified unlawful activity, commits international money laundering.

12. Title 18 U.S.C. § 1956(h) provides that any person who conspires to commit any offense of 1956 or 1957 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

PROPERTY INFORMATION

13. The Defendant Funds were seized from two Binance accounts: 2,343,115.54 USDT from an account with User ID Number ending in 9186 ("Subject Account 1") held in the name of [Subject 1] ("Subject 1"), and 203,299.47 USDT from an account with User ID Number ending in 1564 ("Subject Account 2") held in the name of [Subject 2] ("Subject 2").

14. Tether is a digital currency backed by the U.S. Dollar (*i.e.*, a stablecoin). Stablecoins are digital assets that may be pegged to a currency like the U.S. dollar or to a commodity's price, such as gold. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

15. The Defendant Funds are currently in FBI custody and will be transferred to the United States Marshals Service in the District of Columbia.

STATEMENT OF FACTS

16. The Federal Bureau of Investigation ("FBI") seized the Defendant Property from criminals abroad involved in "pig-butchering" scams—some of whom may be victims of forced labor themselves. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities; to promote and enhance cooperation among federal and foreign law enforcement agencies; and most importantly, to recover assets that may be used to compensate victims.[1]

I. Background on cryptocurrency

17. **Virtual currency:** Virtual currencies are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any

[1] *See* United States Asset Forfeiture Program, *Our Mission*, https://www.justice.gov/afp.

government or bank like traditional fiat currencies, such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin (BTC) and Ether (ETH) are currently the most well-known virtual currencies in use.

18. **Stablecoins:** Stablecoins are a type of virtual currency designed to maintain a stable value relative to another asset, typically a unit of currency or commodity or basket of assets. USDT, commonly referred to as a stablecoin, is pegged to the value of the U.S. dollar, and one USDT is intended to be valued at $1. Tether Limited is the token manager (the owner of the smart contract) and the entity responsible for keeping funds in reserve that back USDT. Tether Limited Inc. is owned by iFinex Inc., a company registered in the British Virgin Islands and reportedly headquartered in Hong Kong.

19. **Virtual currency address:** Virtual currency addresses are the specific virtual locations to or from which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

20. **Private key:** Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder(s) of an address's private key can authorize a transfer of virtual currency from that address to another address.

21. **Virtual currency wallet:** There are various types of virtual currency wallets, including software wallets, hardware wallets, paper wallets. A software wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

22. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

23. **Blockchain:** The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers and using that blockchain's technology, containing an immutable and historical record of every transaction. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

24. **Blockchain explorers** are online tools that operate as a blockchain search engine. Blockchain explorers enable users to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

25. **USDT**, also known as Tether, is a crypto currency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar. Thus, one unit of USDT is represented to be backed by one U.S. dollar in Tether's reserves, making it what is known s a "stablecoin." USDT is issued by Tether Ltd. USDT is hosted on the Ethereum and Tron blockchains, among others.

26. **Ethereum (ETH)** is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

27. **Virtual currency exchanges (VCEs)** are trading and/or storage platforms for virtual currencies such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, "know your customer" or "KYC" checks) and to have anti-money laundering programs in place.

28. **Blockchain analysis:** It is virtually impossible to look at a single transaction on a blockchain and immediately ascertain the identity of the individual behind the transaction. That is because blockchain data generally consist only of alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To analyze blockchain data, law enforcement can use blockchain explorers as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v.*

Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

II. Overview of the pig-butchering scheme and related wire fraud and money laundering

A. Pig-butchering defined

29. Investment-fraud schemes like the one described in this Complaint are commonly referred to as "pig-butchering." That term is derived from the foreign-language word used to describe such schemes. Pig-butchering schemes begin by criminals contacting potential victims through seemingly misdirected text messages, dating applications, or professional meetup groups. Next, using various means of manipulation, the criminal gains the victim's trust and affection. Criminals refer to victims as "pigs" at this stage because they concoct elaborate stories to "fatten up" their victims.

30. Once that trust is established, the criminal recommends cryptocurrency investment by touting their own, or an associate's, success in the field. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake investment platform hosted on a website. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The criminal assists the victim with opening a cryptocurrency account, often on an exchange such as Binance or Coinbase, then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. On its surface, the platform shows lucrative returns, encouraging further investment; underneath, all deposited funds are routed to a cryptocurrency wallet address controlled completely by the criminals—the "butchering" phase of the scheme.

31. Pig-butchering perpetrators frequently allow victims to withdraw some of their "profits" early in the scheme to engender trust and help convince victims of the legitimacy of the platform. As the scheme continues, victims are unable to withdraw their funds are provided various excuses as to why. For example, the criminals will often levy a fake "tax" requirement, by stating that taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by the criminals to elicit more money from victims. The criminals then typically lock the victims out of their "accounts" on the platforms and the victims lose access to their funds. The criminals then move the victim funds beyond reach of law enforcement, typically by using non-custodial or "private" wallets that law enforcement cannot attribute using legal process or blockchain analysis alone; by transferring victim funds through multiple wallets before those funds reach a consolidation wallet; and by commingling victim funds with other funds in a consolidation wallet and sometimes then further transferring the funds to additional "downstream" wallets. Criminals frequently liquidate their cryptocurrency fraud proceeds by using "brokers" who agree to buy the cryptocurrency in exchange for other currency, including fiat currency.[2]

32. Based on data submitted to the FBI's Internet Crime Complaint Center (https://www.ic3.gov), in 2022 alone, pig-butchering schemes targeted tens of thousands of victims in the United States and resulted in more than $2 billion in fraud proceeds being transferred overseas.

[2] Financial Crimes Enforcement Network, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (Sept. 8, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.

B. The first victim and identification of CHOLUMNUAY

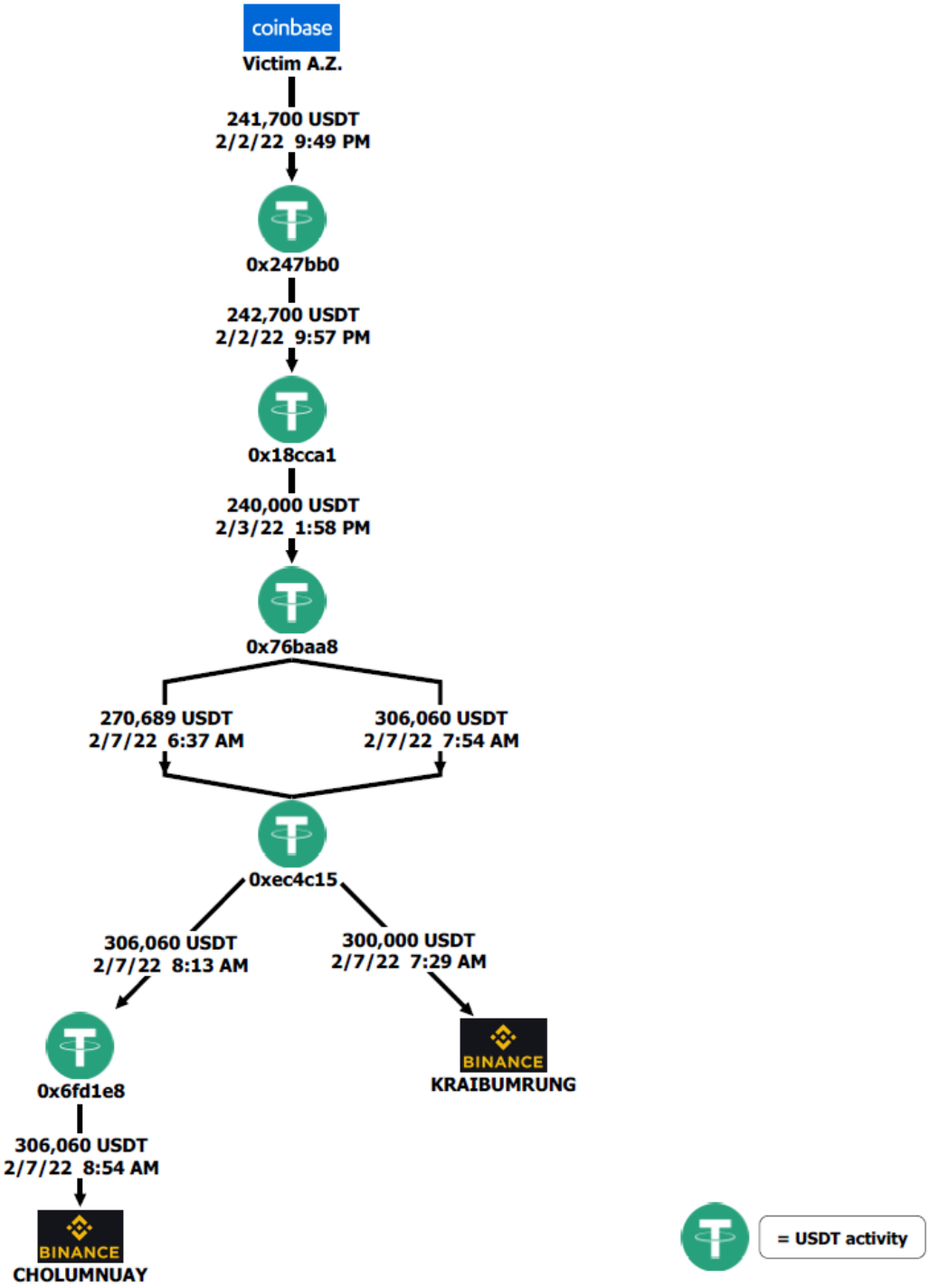
33. In about February 2022, the FBI's Boston field office learned of a pig-butchering victim, A.Z., who lost $782,000. A.Z. belonged to a real estate investment group on WeChat, a messaging application. A.Z. received a private message from a member named "Kevin" who, over time, gained A.Z.'s trust and discussed investing in cryptocurrency. Kevin walked A.Z. through the process and provided A.Z. a link to mybinet.com, a fake investment platform. Between January 21, 2022, and February 2, 2022, through six transactions in both BTC and USDT, A.Z. deposited approximately $823,120 worth of funds to mybinet.com via Coinbase. To facilitate the process, A.Z. received quick-response code ("QR code") prompts from mybinet.com, simplifying the process of depositing cryptocurrency to the website.

34. Like other pig-butchering victims, A.Z. was able to withdraw a small portion of their funds (approximately $30,000). A.Z. attempted a second withdrawal, they were unable to do so. A.Z. was told to pay "fees" and "percentages." A.Z. was unable to recover the remainder of their funds and lost roughly $782,000.

35. FBI forensic accountants traced a portion of A.Z.'s funds using blockchain analysis tools. Within five days, the perpetrators funneled A.Z.'s largest transaction[3] through several intermediary wallets and a consolidation wallet,[4] where it was commingled with other funds controlled by perpetrators. A.Z.'s then-commingled funds were then deposited into Binance accounts opened in the names of WASIT CHOLUMNUAY ("CHOLUMNUAY") and CHATCHAL KRAIBUMRUNG ("KRAIBUMRUNG"). The flow of A.Z.'s funds is

[3] Processing fees reduced A.Z.'s transaction to 241,700 USDT.
[4] Consolidation wallets have much larger numbers of deposits than withdrawals as compared to other wallets in the chain.

illustrated below (the cryptocurrency addresses here and elsewhere in this document are truncated for ease of reference):



36. This flow of funds is indicative of money laundering through cryptocurrency. At each stage of above, various methods were used by criminals to thwart law enforcement's ability to trace, and ultimately recover, any illicit proceeds. Those methods include:

- **The Use of Unattributable "0 Level" Deposit Addresses (0x247bb0).** Deposit addresses known as "0 Level" addresses are the initial addresses into which victims deposit funds on the blockchain. The criminals provide these addresses to victims. Criminals usually provide 0 Level addresses corresponding to noncustodial, or "private," wallets that are difficult to attribute—rather than wallets hosted by exchanges or other third-party intermediaries—to evade identification. Such is the case here with 0x247bb0.
- **High Velocity Flow of Funds to Consolidation Wallet (0x76baa8).** After duping victims into depositing their investment funds into the 0 Level Address, criminals typically rapidly transfer those fraudulently obtained funds through multiple wallets to a consolidation wallet, where the criminals then commingle the fraud proceeds with other funds. A.Z.'s funds followed exactly such a path: after being deposited into the 0 Level wallet at 9:57 PM, only 10 minutes later, the fraud proceeds were transferred to a different wallet, and approximately 16 hours after that, the fraud proceeds were transferred yet again, this time to a "consolidation" wallet, 0x76baa8, where the fraud proceeds remained for just over four days.
- **Use of Consolidation Wallet to Commingle Funds (0x76baa8 and 0xec4c15).** As a part of a "layering" stage of the money-laundering process, criminals commingle fraud proceeds in consolidation wallets with other funds

to conceal the nature, source, ownership, location, and/or control of the fraud proceed—and, in that process, to make it harder for investigators to trace the disposition of the fraud proceeds. The criminals commingled the fraud proceeds that they had obtained from A.Z. at almost every step in the flow of those fraud proceeds—and, ultimately, the criminals commingled those fraud proceeds in two large transactions totaling USDT 306,060 and 300,000.

37. There is no reason, economic or otherwise, for legitimate businesses or individuals to conduct cryptocurrency transfers in the above fashion. Whether transferring BTC or, in this case, USDT, each individual cryptocurrency transfer costs money. For USDT, that cost is paid via "gas" fees levied by operation of Ethereum blockchain.[5] It is reasonable to assume that businesses and individuals who simply sought to transfer legitimate funds from one address to another would strive to minimize those fees by conducting transfers with as few transactions, or "hops," as possible. Such seemingly unnecessary intermediate cryptocurrency transactions also delay the process of disposing of cryptocurrency funds—and thus tend to defeat any advantage that cryptocurrency might offer as a quick means of exchange. Most businesses and individuals engaging in legitimate cryptocurrency transactions—who are thus unconcerned with obfuscating the source and destination of their funds—seek to minimize their crypt transaction costs by using "retail" exchanges. Retail exchanges, like Coinbase or Binance, can consolidate crypto transactions and thereby lower crypto transaction fees for customers. Criminals laundering through cryptocurrency, however, often avoid these retail exchanges as much as possible because transactions conducted through retail exchanges can

[5] Fees are a cornerstone of blockchain technology, as they are the rewards provided to those providing the computing power to operate the blockchain itself.

more readily by attributed using blockchain analysis tools and because retail exchanges are often responsive to legal process.

38. In March 2022, FBI Boston notified FBI Bangkok that the victim funds traced into Binance accounts in the names of CHOLUMNUAY and KRAIBUMRUNG. During initial deconfliction discussions, the Royal Thai Police—the national police force of Thailand—reported that CHOLUMNUAY was a suspected money launderer. In November 2022 and again in December 2022, FBI Bangkok interviewed CHOLUMNUAY. In those interviews, CHOLUMNUAY stated that he operated a cryptocurrency business and sold large quantities of various virtual currencies in exchange for Thai Baht. CHOLUMNUAY confirmed that KRAIBUMRUNG was a business partner. CHOLUMNUAY remarked that his Binance account had been frozen on multiple occasions and speculated that it could be due to the volume of transactions through his account. To circumvent daily transaction limits of 2 million Baht, CHOLUMNUAY would transfer some of his deposits to accounts of his "friends."

39. During the interviews, CHOLUMNUAY also reported that on February 7, 2023, he purchased 606,060 USDT from an individual later identified by law enforcement as YIN HONGZHI. Of that, CHOLUMNUAY transferred 306,060 USDT first to his Bitkub account—a Thailand-based cryptocurrency exchange—and then to his Binance account. To avoid payment of fees, CHOLUMNUAY stated that he had instructed HONGZHI to send the remaining 300,000 USDT directly to KRAIBUMRUNG. Based on CHOLUMNUAY's recollection, it is reasonable to assume that 0xEC4C15 belongs to HONGZHI. CHOLUMNUAY stated that after the 306,060 USDT posted to his Binance account, he distributed portions of the 306,060 USDT to friends, who, for a small fee paid by CHOLUMNUAY, would sell the USDT for Thai Baht on CHOLUMNUAY's behalf.

40. Based on the investigation to date, CHOLUMNUAY made no attempts to verify the source or legitimacy of the fraud proceeds he laundered. Furthermore, CHOLUMNUAY told Thai law enforcement that he knowingly employed methods to circumvent rules on transaction limits, such as distributing proceeds to associates for a fee. Notably, CHOLUMNUAY could have avoided paying those fees simply by applying for a larger daily transaction limit account on the Thai exchange Bitkub. To do so, CHOLUMNUAY only would have needed to provide a three-month bank statement and proof of address. CHOLUMNUAY's lack of due diligence, use of intermediaries to circumvent rules on transaction limits, and movement of funds through multiple exchanges (Bitkub and Binance) show that CHOLUMNUAY not only took measures to obscure the nature of his business activities to Thai authorities but that he took active steps to conceal the nature, source, ownership, location, and control of the funds that he transacted and conspired to transact. The unnecessary complexity and costs entailed in these transactions also indicate that CHOLUMNUAY and his coconspirators knew that they funds that were involved in these transactions included proceeds of some form of unlawful activity.

41. As described below, further evidence shows that other victim funds flowed into accounts controlled by CHOLUMNUAY. The evidence thus indicates that CHOLUMNUAY and other coconspirators (known and unknown) schemed to launder such victim funds.

42. CHOLUMNUAY thereby conspired with others to knowingly engage in concealment money laundering transactions for the purpose of laundering criminal proceeds—criminal proceeds that in fact included proceeds of the above-described pig-butchering fraud scheme—all in violation of Title 18, United States Code, Section 1956(h).

43. As a part of that money laundering conspiracy, CHOLUMNUAY conspired with others to engage in financial transactions that CHOLUMNUAY and his coconspirators knew involved proceeds of some form of unlawful activity and that, in fact, involved proceeds of the pig-butchering wire fraud scheme committed in violation of Title 18, United States Code, Section 1343, a specified unlawful activity under Title 18, United States Code, Section 1956(c)(7). CHOLUMNUAY and his coconspirators engaged in those financial transactions for the purpose of concealing the nature, source, ownership, location, and control of criminal proceeds.

44. Each of those transactions was a substantive concealment money laundering transaction in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and (a)(2)(B)(i).

45. All property "involved in" a money laundering offense are subject to civil forfeiture under Title 18, United States Code, Section 981(a)(1)(A).

46. Property subject to forfeiture as involved in concealment money laundering conduct includes both the proceeds of specified unlawful activity that were laundered as well as other untraced funds that were used to facilitate the concealment money laundering transactions by helping to conceal the nature, source, ownership, location, or control of the criminal proceeds.

47. The Defendant Funds in the Subject Accounts are thus subject to forfeiture, at least in part as traceable to proceeds of fraud, and in whole as property involved in money-laundering offenses.

C. Royal Thai Police search warrant and identification of additional victims

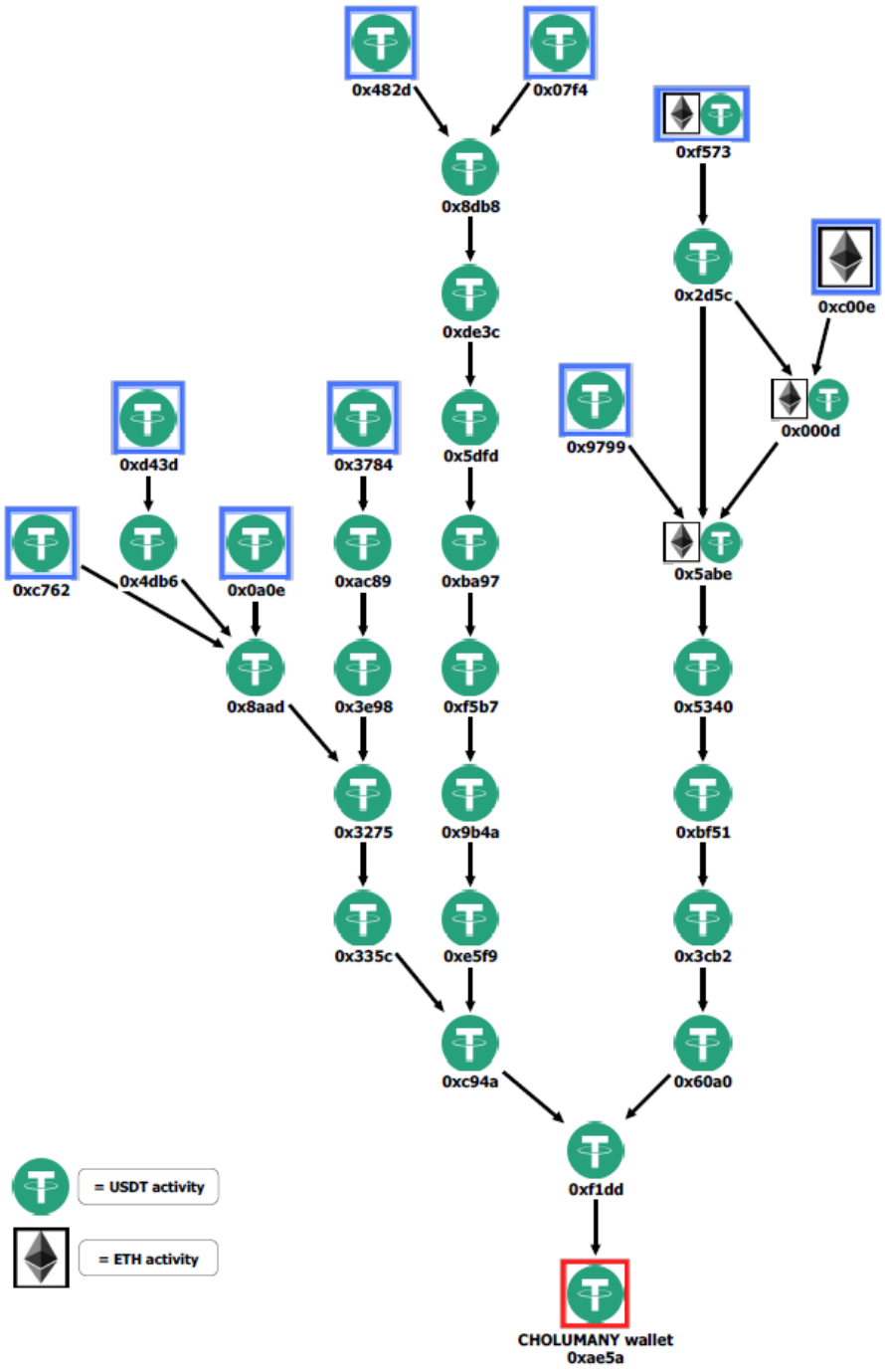
48. On April 19, 2023, the Royal Thai Police executed a warrant issued by a Thai judge at CHOLUMNUAY's residence, under which they seized and searched CHOLUMNUAY's digital devices. Investigators found several private wallets stored on CHOLUMNUAY's digital devices. The Royal Thai Police shared with the FBI evidence collected from the search, including screenshots of CHOLUMNUAY's private wallet addresses. FBI forensic accountants performed blockchain analysis on those addresses:

FIGURE 2: CHOLUMNUAY's PRIVATE WALLETS

Address	Asset	Balance
0xae5a72bfab545976dc7a9f1dd354f196d6b20ee1	USDT	388,100.00
0x4c69c08190db5229525c04d53e593b127e218cc8	USDT	31,815
TKPw9BZ5MiJXDUo4Cq5ZECV3XyEfaqwfax	USDT	311,327
TT6VckqGDX1dZHYcEpXNEiGG5HQDumEMdq	USDT	
	TOTAL	**731,242**

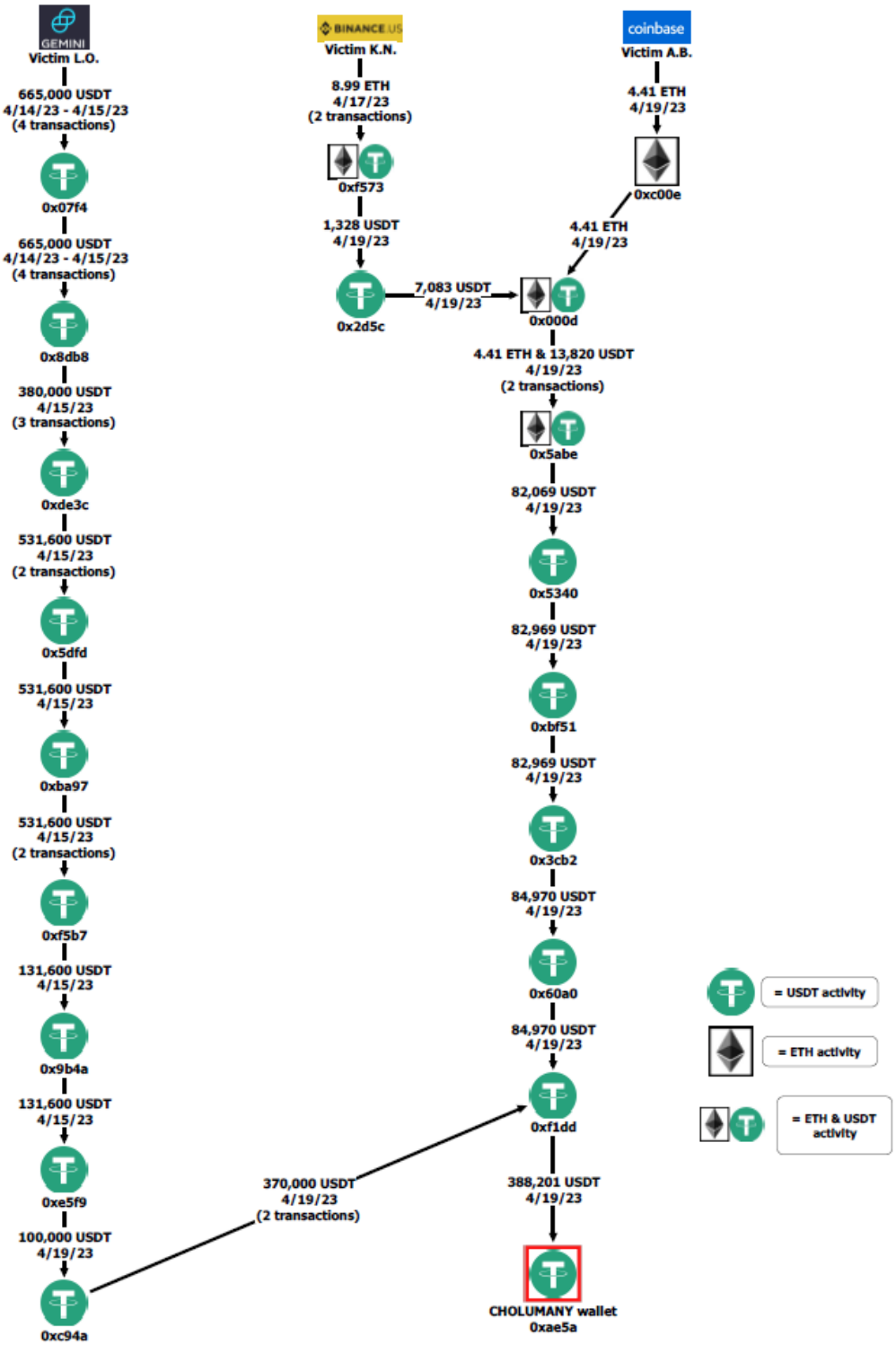
49. Blockchain analysis confirmed the 0xae5a balance of 388,100 USDT was sourced primarily from one transaction on April 19, 2023, totaling 388,201 USDT. FBI forensic accountants traced that transaction backwards on the blockchain and identifed numerous private intermediary and consolidation wallets before arriving at 0 Level wallets[6] (colored blue):

[6] As noted earlier, 0 Level wallets are the first deposit addresses where victim funds are sent. From there, funds are generally sent on to various additional cryptocurrency addresses to launder the proceeds.

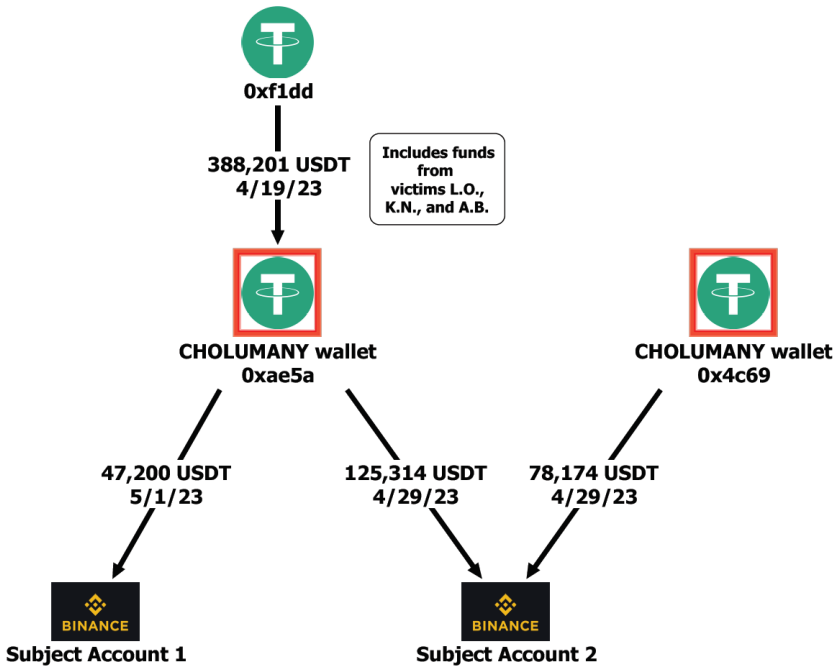


50. Investigators determined that those 0 Level wallets received deposits from numerous wallets at retail exchanges, such as Binance.US, Coinbase, Crypto.com, and Gemini. Through legal process to these exchanges, and subsequent interviews with the account holders, agents identified three additional pig-butchering victims, L.O., K.N., and A.B., whose funds

were ultimately transferred to CHOLUMNUAY's 0xae5a wallet during the same five-day period, as shown below.



51. After executing the search warrant, the Royal Thai Police gave notice to CHOLUMNUAY to refrain from transferring any of his cryptocurrency. But he did not comply with that notice. Instead, on April 29, 2023, CHOLUMNUAY deposited 203,488 USDT to Subject Account 2, 125,314 USDT, which derived from CHOLUMNUAY's 0xae5a wallet containing pig-butchering proceeds. On May 1, 2023, CHOLUMNUAY deposited 47,200 USDT to Subject Account 1 from CHOLUMNUAY's 0xae5a wallet. CHOLUMNUAY entirely depleted the 731,242 USDT balance and disbursed the virtual currently into other wallets and non-custodial addresses shown below:

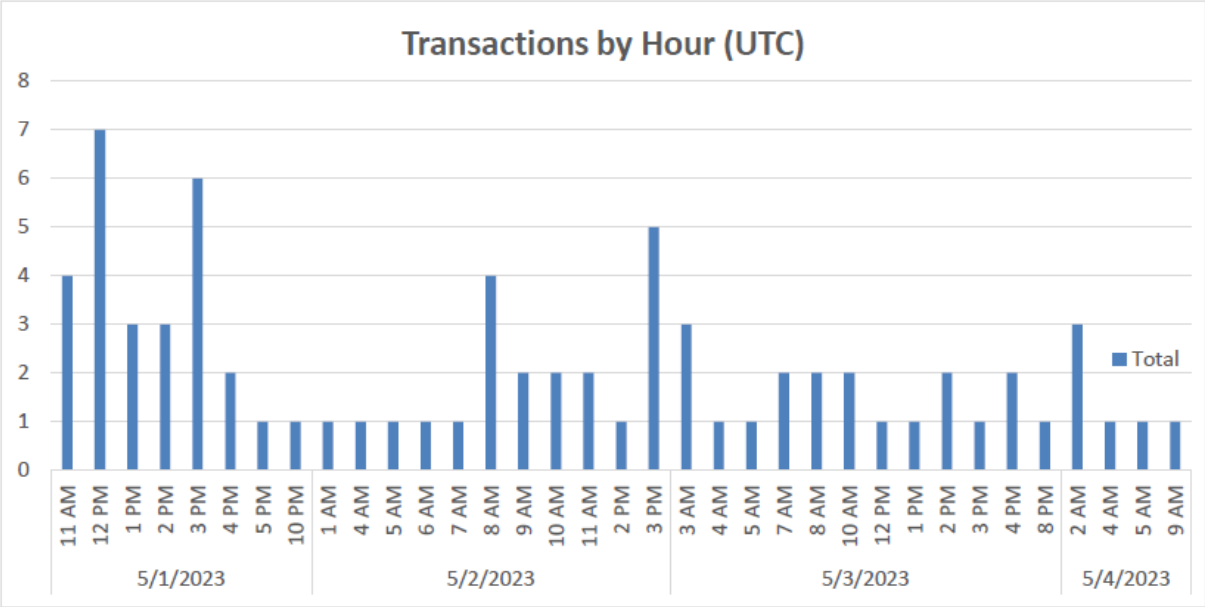


52. In sum, CHOLUMNUAY received pig-butchering victim proceeds on multiple occasions and in multiple wallets. And he took several measures—such as splitting the incoming proceeds and distributing the outgoing proceeds among associates—to conceal the nature, source, location, ownership, and/or control of the criminal proceeds. The evidence

established that Subject Account 1 and Subject Account 2 were both used to launder cryptocurrency.

D. Subject Account 1

53. Subject Account 1 was opened as a "personal account" in the name of Subject 1 on March 5, 2023. From account creation until May 1, 2023, Subject 1 received zero external deposits (not counting internal Binance Pay transfers, as discussed in the next paragraph). But between May 1, 2023 (when CHOLUMNUAY transferred funds into this account) and May 4, 2023, Subject 1's account received 73 deposits. Those deposits arrived in Subject Account 1 consistently throughout each day:



In addition, 88% of all incoming deposits originated from other Binance accounts. Transfers between Binance accounts are not recorded on a public blockchain, rendering them untraceable without legal process and cooperation from the exchange.

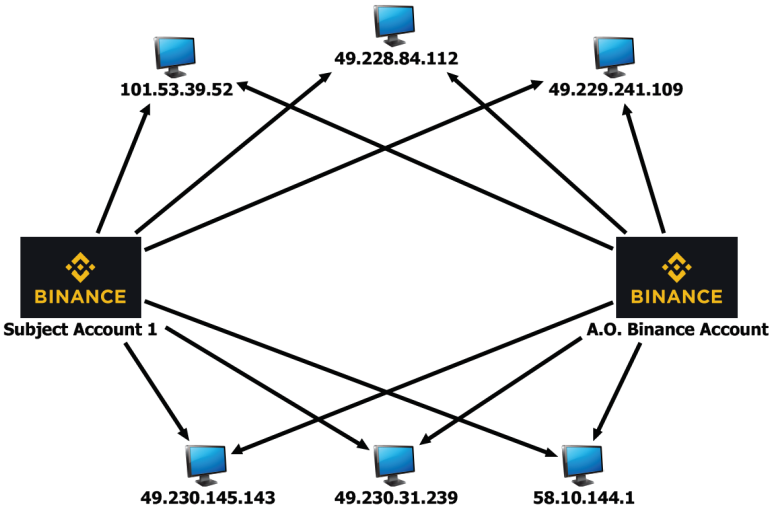
54. Between April 3 and April 15, 2023, Subject Account 1 received 1,747,156 USDT via Binance Pay[7] from a Binance account opened in the name of a person (A.O.) as a personal account (the "A.O. Binance Account"). A comparative analysis of Subject Account 1 and the A.O. Binance Account shows that both accounts were likely controlled by the same individual or group. Both accounts were registered within days of each other, from March 5, 2023 (Subject Account 1) and March 6, 2023 (A.O.'s account). Both accounts were registered via the same IP address that resolved to Bangkok, Thailand, and were accessed from the same IP addresses on multiple occasions following their registration. Both accounts share several Binance IDs, known as "BNC" IDs.[8] Where multiple accounts share the same BNC ID, it likely shows that those accounts were accessed via the same device and web browser on at least one occasion. Both accounts have a similar percentage of deposits from other Binance accounts: 63% for Subject Account 1 and 60% for A.O.s account, respectively.

55. Furthermore, A.O.'s account picture is unusual and may be indicative of duress or an effort to obscure his own identity. Binance requires customers to provide a photograph as part of the "know your customer" process. Most customers provide a "selfie" photograph taken with their own phone. But the photograph provided with A.O.'s account, by contrast, shows an individual with his back against a wall, with eyes scrunched closed and mouth in an apparent grimace. The closed eyes and absence of an extended arm in the frame also suggests that the photograph was taken by a third person and not the individual depicted. Criminals involved in pig-butchering schemes often open, or attempt to open, cryptocurrency exchange accounts in the names of others to further insulate themselves from accounts containing

[7] Binance Pay is another method to transfer cryptocurrency off-chain with zero fees. Binance Pay works like Venmo: a Binance customer can scan an associate, family member, or friend's Binance Pay QR code, enter their email address, phone number, or Binance ID, and send and receive money from that recipient.
[8] These are proprietary IDs for Binance that are generated using their own internal algorithms.

criminal proceeds. Many individuals in Southeast Asia working as part of these pig-butchering organizations are human trafficking victims themselves, lured by the promise of work by criminals and are trafficked into compounds forced to participate in scams.[9] Given this background, A.O. is likely a victim who was forced to provide his information and/or a photograph to open A.O. Binance account.

56. Other evidence likewise indicates that both accounts—Subject Account 1 and the A.O. Binance Account—were controlled by the same individual or group. Binance provided records for Subject Account 1 and the A.O. Binance Account that included access logs containing IP addresses used to access each account. A forensic analysis performed on the IP addresses determined that both accounts were accessed from the same IP addresses. In total, there were 257 access log entries for Subject Account 1 and the A.O. Binance Account in which the same IP address appeared in the access logs for both accounts. The following figures shows the IP addresses used to access both accounts.



[9] United Nations Human Rights Office of the High Commissioner, *Hundreds of Thousands Trafficked to Work as Online Scammers in SE Asia*, (March 29, 2023), https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report; *see also* Last Week Tonight, *Pig Butchering Scams*, at 15:29-22:10, https://youtu.be/pLPpl2ISKTg?si=EFbqVslm0y7oW5r3&t=929.

57. Such activity is an indicia of money laundering. What is more, both accounts were registered within one day of each another via the same IP address that resolved to Bangkok, Thailand. In many instances, the same IP address accessed both accounts within *minutes* of each other. For example, the following figure depicts both accounts being accessed from the same IP address within minutes, which was then immediately followed by a transaction of 750,00 USDT being sent from one account to the other—indicating that the same individual was accessing both accounts to view both sides of this transaction:

Binance Access Log Events:

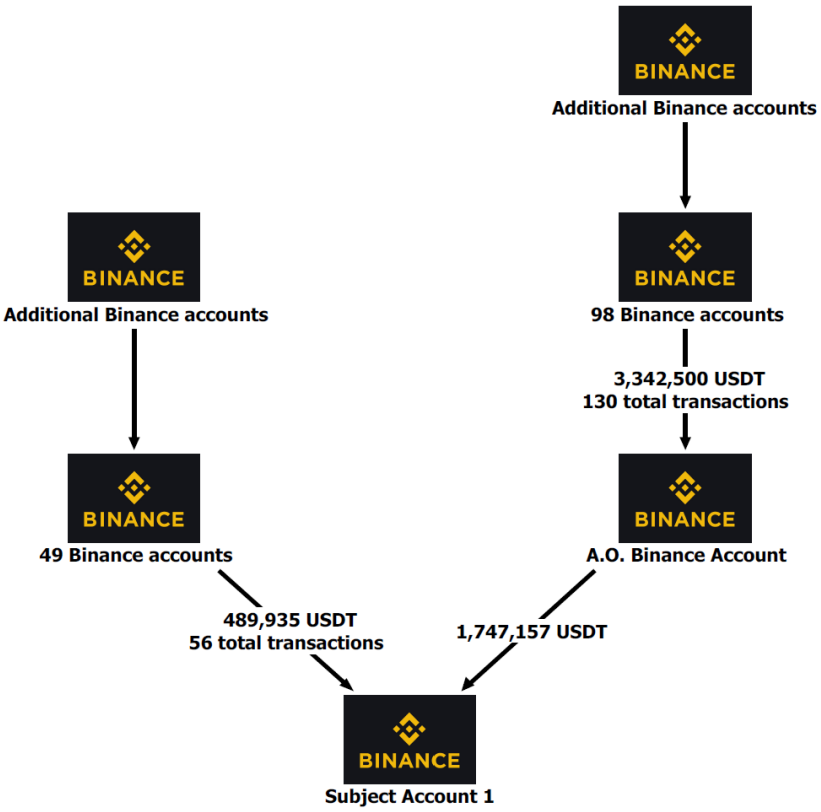
Account Name	Date/Time (UTC)	Event Description	Event Description (English translation)	IP Address	Geolocation Country
A.O. Binance Account	4/10/23 15:18	用户扫码登陆	User scan code login	58.10.144.1	Thailand
A.O. Binance Account	4/10/23 15:18	提现风控校验	Withdrawal risk control verification	58.10.144.1	Thailand
Subject Account 1	4/10/23 15:47	发送邮件验证码对外	Send email verification code to external	58.10.144.1	Thailand
Subject Account 1	4/10/23 15:48	续期登录态	Renewal login status	58.10.144.1	Thailand

Binance Transaction Logs Entries:

Account Name	Date/Time (UTC)	Transaction Type	Counterparty	USDT Amount
A.O. Binance Account	4/10/23 15:49	Send	Subject Account 1	(750,000)
Subject Account 1	4/10/23 15:49	Receive	A.O. Binance Account	750,000

58. As noted above, 88% of all incoming deposits into Subject Account 1 came from other Binance accounts. That 88% figure includes 1,747,157 USDT in deposits from the A.O. Binance Account, as well as a high volume of smaller deposits from 49 other Binance accounts. Similarly, the A.O. Binance Account also had a high volume of deposits from 98 other Binance accounts. It is highly unusual for a cryptocurrency exchange account set up for personal use to have such a high volume of deposits from so many other cryptocurrency exchange accounts.

59. Further, to determine the source of funds in Subject Account 1 and the A.O. Binance Account, investigators analyzed a sample of records from the other Binance accounts that sent USDT to them. The records consistently showed a succession of USDT transactions through multiple layers of *other* Binance accounts—indicative of money laundering and of attempts to conceal the source of funds, given that those transfer transactions are not recorded on the public blockchain, as explained in paragraphs 53–58 above. Such layering makes it extremely difficult for investigators to trace funds, both forward to determine the final cash-out point but also backward to determine the original source of the funds from other victims. The following figure depicts the flow of funds through multiple layers of Binance accounts:



60. In sum, the evidence shows that Subject Account 1 was used to launder illicit proceeds from pig-butchering schemes, among other crimes, and to conceal and disguise the

nature, location, source, ownership, and control of the proceeds of specified unlawful activity. Subject Account 1 received funds from CHOLUMNUAY that contained proceeds from pig-butchering victims. The account activity is heavily composed of Binance-to-Binance deposits used to obfuscate the source of funds. Subject Account 1 is a personal account, but it had numerous transfers in and out, to a degree highly unusual for a personal account. Subject Account 1 received a substantial percentage of deposits from an account opened in someone else's name but accessed from the same devices. There is no legitimate reason, and it is in fact contrary to Binance's terms of service,[10] to open a Binance account under another's name. And the account photograph associated with the account is unusual and may be indicative of duress or an effort to obscure the accountholder's identity. That whoever controlled these two accounts sent funds between them indicates that they sought to layer, comingle, transfer, and obfuscate the source of those funds expediently. The evidence shows that Subject Account 1 was used to launder pig-butchering funds, including the traced 47,200 USDT deposited into the account from CHOLUMNUAY's 0xae5a wallet, and that other funds in the account also bear strong indicia of pig-butchering.

61. At least some of the Defendant Funds seized from Subject Account 1 are subject to forfeiture under Title 18, United States Code, Section 981(a)(1)(C) as proceeds of wire fraud and conspiracy to commit wire fraud, committed in violation of Title 18, United States Code, Sections 1343 and 1349.

62. In addition, all the Defendant Funds seized from Subject Account 1 are subject to forfeiture under Title 18, United States Code, Section 981(a)(1)(A) as having been involved in a concealment money laundering conspiracy, committed in violation of Title 18, United

[10] *See* Binance Terms of Service, *9.2 Restricting Access to Third Parties*, https://www.binance.com/en/terms.

States Code, Section 1956(h), and domestic and international concealment money laundering transactions committed in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) and (a)(2)(B)(i).

E. Subject Account 2

63. Subject Account 2 was opened in the name of Subject 2, a Malaysia national, as a personal account on April 12, 2021. On April 29, 2023, CHOLUMNUAY deposited 203,488 USDT to Subject Account 2. Of that amount, more than half of it—125,314 USDT—derived from CHOLUMNUAY's 0xae5a wallet containing pig-butchering proceeds. (*See* chart in paragraph 53, *supra*.) CHOLUMNUAY's transactions are the last on the account and consist of 99.94% of the remaining balance: 203,610 USDT.

64. Between April 2021 and April 2023, Subject Account 2 received more than 52 million USDT via 354 transactions, with an average transaction amount of 146,892 USDT. One hundred and twelve addresses sent these transactions—the large majority of which sent only one or two total transactions. Frequently, Subject Account 2 received deposits and then completely emptied the account, transferring the entirety of the funds elsewhere. A noncommercial entity engaging is this volume of transactions and different addresses indicates large-scale wire fraud and money laundering. When the government executed the seizure warrant for Subject Account 2, the account contained over 203,000 USDT, including the 125,314 USDT derived from CHOLUMNUAY's 0xae5a wallet that contained pig-butchering proceeds. The evidence thus shows that Subject Account 2 received the proceeds of fraudulent pig-butchering scams and that perpetrators conducted high-velocity, high-volume USDT transactions to launder illicit proceeds.

65. At least some of the Defendant Funds seized from Subject Account 2 are subject to forfeiture under Title 18, United States Code, Section 981(a)(1)(C) as proceeds of wire fraud and conspiracy to commit wire fraud, committed in violation of Title 18, United States Code, Sections 1343 and 1349.

66. In addition, all the Defendant Funds seized from Subject Account 2 are subject to forfeiture under Title 18, United States Code, Section 981(a)(1)(A) as having been involved in a concealment money laundering conspiracy, committed in violation of Title 18, United States Code, Section 1956(h), and domestic and international concealment money laundering transactions committed in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) and (a)(2)(B)(i).

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY
(18 U.S.C. § 981(a)(1)(C))

67. Paragraphs 1 through 66 are realleged and incorporated by reference here.

68. The Defendant Funds, seized from Subject Accounts 1 and 2, include property constituting or derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349.

69. Accordingly, some or all of the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY
(18 U.S.C. § 981(a)(1)(A))

70. Paragraphs 1 through 66 are realleged and incorporated by reference here.

71. The Defendant Funds, seized from Subject Accounts 1 and 2, constitute property involved in (a) domestic and international concealment money laundering transactions committed in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i)

and 1956(a)(2)(B)(i) and (b) conspiracy to engage in money laundering, committed in violation of Title 18, United States Code, Section 1956(h).

72. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Property as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that this Honorable Court issue a warrant of arrest *in rem* according to law; that judgment be entered declaring that the Defendant Property be forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court may deem just and proper.

July 16, 2024
Washington, D.C.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

/s/ Rick Blaylock, Jr.
Rick Blaylock, Jr.
TX Bar No. 24103294
Assistant United States Attorney
Asset Forfeiture Coordinator
United States Attorney's Office
601 D Street, N.W.
Washington, D.C. 20001
(202) 252-6765
rick.blaylock.jr@usdoj.gov

/s/ Jonas Lerman
Jonas Lerman
CA Bar No. 274733
Trial Attorney

National Cryptocurrency Enforcement Team
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Avenue, N.W.
Washington, D.C. 20005
(206) 588-9582
jonas.lerman@usdoj.gov

VERIFICATION

I, Scott Norris, a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *in rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 16th day of July 2024.

Scott Norris
Special Agent
Federal Bureau of Investigation