UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, PLAINTIFF, v. JINGLIANG SU, aka "Jingliang Su Martinez" and "James," DEFENDANT.	**WARRANT FOR ARREST** **24-MJ-4513-LOUIS** ON COMPLAINT CASE NO.: 2:24-mj-07038-DUTY

To: UNITED STATES MARSHAL AND ANY AUTHORIZED UNITED STATES OFFICER

YOU ARE HEREBY COMMANDED to arrest defendant **JINGLIANG SU** and bring him forthwith to the nearest Magistrate Judge to answer a complaint charging him with Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).

REC. BY AUSA: Detention

November 22, 2024 12:39 p.m.
Date

Honorable Alicia G. Rosenberg
Name of Magistrate Judge

Alicia G. Rosenberg
Signature of Magistrate Judge

RETURN		
This warrant was received and executed with the arrest of the above-named defendant at (location):		
DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE OF ARREST		

DESCRIPTIVE INFORMATION FOR DEFENDANT CONTAINED ON PAGE TWO

AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the
Central District of California

United States of America,

Plaintiff,

v.

JINGLIANG SU,
aka "Jingliang Su Martinez" and
"James,"

Defendant.

24-MJ-4513-LOUIS

Case No. **2:24-mj-07038-DUTY**

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. Beginning in or around August 2021 and continuing to on or about April 12, 2024, in the County of Los Angeles in the Central District of California, and elsewhere, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1956(h)	Conspiracy to Commit Money Laundering

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ George Jasek
Complainant's signature

George ("John") Jasek, USSS Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: November 22, 2024

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

AUSAs: Maxwell Coll (1785) and Nisha Chandran (2429)

AFFIDAVIT

I, Special Agent George Jasek, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against **JINGLIANG SU**, also known as "Jingliang Su Martinez" and "James" (hereinafter referred to as "**SU**"), for conspiring to commit money laundering, in violation of Title 18, United States Code, Section 1956(h).

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant and does not purport to set forth all of my knowledge of investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only and all dates, times, and dollar amounts are approximate.

II. BACKGROUND OF AGENT

3. I am a Special Agent ("SA") with the United States Secret Service ("USSS") and have been so employed since March 2018. I am currently assigned to the Criminal Investigative Division in Washington, District of Columbia. In preparation for my employment with USSS, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. Additionally, I completed the Special Agent Training Course

("SATC") at the USSS James J. Rowley Training Center in Laurel, Maryland. While attending SATC, I received a five-day training titled "Basic Investigation of Computer and Electronic Crimes Program." In addition to these training programs, I have completed numerous in-service training courses related to constitutional law. Prior to my employment with USSS, I was a full-time certified Police Officer in New Hampshire for more than five years. My present duties include the investigation of federal offenses, including, but not limited to, those involving financial fraud and its related activities. As part of my duties, I have conducted numerous financial crime and financial fraud investigations. These investigations have included but are not limited to federal violations of wire fraud, bank fraud, money laundering, and identity theft statutes. During the course of these investigations, I have conferred with other investigators who specialize in computer forensics and who have conducted investigations regarding financial fraud crimes. I have received additional training regarding computers which includes Basic Network Intrusion Responder Training, Incident Response Analysis, and virtual currency training.

III. SUMMARY OF PROBABLE CAUSE

4. USSS is investigating an international money-laundering syndicate that launders the proceeds of fraud schemes, including cryptocurrency investment scams and other currency-related frauds commonly referred to as "pig-butchering." Victims of the schemes under investigation were fraudulently induced into transferring millions of dollars to U.S. bank accounts opened in the names of

dozens of shell companies whose sole apparent purpose was to facilitate the laundering of fraud proceeds. Many of these accounts and shell companies were located in the Central District of California. A network of money launderers then facilitated the transfer of those funds to other domestic and international bank accounts and cryptocurrency platforms in a manner designed to conceal the source, nature, ownership, and control of the funds.

5. Specifically, co-conspirators set up approximately 74 U.S. shell companies and opened bank accounts with U.S. financial institutions including Bank of America, JPMorgan Chase Bank ("JPMC"), and Wells Fargo. These bank accounts received millions of dollars in wire fraud proceeds from U.S. victims of cryptocurrency scams. After the receipt of fraud proceeds into these U.S. bank accounts, a network of U.S.-based money launderers executed transactions transferring the proceeds to two bank accounts established at Deltec Bank and Trust ("Deltec Bank") in the Bahamas. The first Deltec Bank account, "Bahamas Account #1," was an account at Deltec Bank opened in the name of the business entity Axis Digital Limited. The second Deltec Bank account, "Bahamas Account #2," was an account at Deltec Bank opened in the name of the business entity GTAL. Both Deltec Bank accounts received millions in fraud proceeds from U.S. victims.[1]

6. **SU** worked with multiple co-conspirators to direct funds into and out of Bahamas Account #1. Co-Conspirator 1 is a U.S. citizen based in Los Angeles and a founder of Axis Digital Limited,

[1] The fraud proceeds first flowed through a Deltec-affiliated bank account at Mitsubishi UFJ Trust and Banking Corporation ("MUFJ Account") in New York, New York.

the Bahamian entity established to open Bahamas Account #1. Co-Conspirator 2 is a U.S. citizen who resided in California and Mexico. **SU**, Co-Conspirator 1, and Co-Conspirator 2 used Bahamas Account #1 to launder fraudulent proceeds and convert the funds into the cryptocurrency Tether ("USDT").[2] **SU** and his co-conspirators received more than $36 million in fraud proceeds into Bahamas Account #1 from U.S. shell company bank accounts and oversaw the conversion of all of the proceeds into USDT, and the transfer of the proceeds to foreign-controlled cryptocurrency wallets. As discussed herein, **SU** maintained Know Your Customer ("KYC") documents for the fraudulent shell entities, was a signatory on Bahamas Account #1, participated in communications with Deltec Bank, and directly received victim proceeds into his personal cryptocurrency account.

7. The government has charged several individuals related to this scheme. First, in United States v. Lu Zhang, et al., 2:23-CR-596-RGK, the government indicted four individuals – LU ZHANG, JUSTIN WALKER, JOSEPH WONG, and HAILONG ZHU – with conspiracy to commit money laundering and substantive money laundering. Defendants LU ZHANG and JUSTIN WALKER pleaded guilty to conspiracy to commit money laundering, and the two remaining defendants are fugitives. Each defendant was involved in the U.S.-based money-laundering network and effectuated financial transactions sending fraud proceeds from U.S. shell company bank accounts to Bahamas Account #1.

[2] Tether, or "USDT," is a stablecoin pegged to the U.S. dollar.

8. Second, in United States v. Daren Li, et al., 2:24-CR-311-RGK, the government indicted two individuals – DAREN LI and YICHENG ZHANG – with conspiracy to commit money laundering and substantive money laundering. Defendant DAREN LI pleaded guilty to money laundering conspiracy. YICHENG ZHANG is presently set for trial in April 2025. Defendant LI was involved in the direction of funds into and out of Bahamas Account #1 and Bahamas Account #2. Defendant ZHANG was involved in the domestic money-laundering network.

9. **SU** and his co-conspirators played integral roles in the laundering of funds through the Deltec Bank accounts.

IV. TECHNICAL TERMINOLOGY

10. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

11. "Digital currency" or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[3] Examples of cryptocurrency are bitcoin ("BTC"), Ether ("ETH"), USDT, and USDC. Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Cryptocurrency can be exchanged

[3] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

directly person to person, through a cryptocurrency exchange, or through other intermediaries. Most cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[4] Cryptocurrency is not illegal in the United States.

12. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. USDT, or Tether, is a type of stablecoin. USDT is pegged to the U.S. dollar, such that $1 is equal to 1 USDT.

13. An "Internet Protocol address" or "IP address" is a numerical address assigned to each computer connected to a network that uses the internet for communication. Internet Service Providers assign IP addresses to their customers. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access an account. The type of application or service provider a particular customer is using often determines how long they will be assigned the same IP address. For instance,

[4] Some cryptocurrencies operate on blockchains that are not public.

someone who rents computer servers can lease an IP address long-term and maintain it for several years. In my training and experience, residential Internet Service Providers often lease the same IP address to a customer over months to a year. Cellular phone provider customer IP addresses often change more frequently. Email providers, internet providers, and even cybercrime forums often record the IP address used to register an account and the IP addresses associated with particular logins to the account. In my training and experience, when the same IP address is used to access different internet services in close temporal proximity, it tends to show the same computer or computer network was used to access those services. When several instances of this IP address overlap exist over time from different service providers, it makes it very likely that the same person or group of people sharing internet infrastructure are behind the accesses.

14. A domain name is a simple, often easy-to-remember way for humans to identify computers on the internet, using a series of characters (*e.g.*, letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

15. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

V. STATEMENT OF PROBABLE CAUSE

16. Based on records, witness interviews, my review of electronic communications, and my knowledge of this investigation, I know the following:

A. Investigation into a Cryptocurrency Investment Scheme

17. In September 2022, law enforcement began an investigation into a criminal money-laundering syndicate operating cryptocurrency investment scams, also known as "pig- butchering." The term "pig butchering" (derived from the Chinese phrase used to describe this scheme) is a type of scam that involves scammers grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. In this syndicate, the scammers promoted spoofed domains and websites purporting to be legitimate cryptocurrency trading platforms to U.S. victims, including within the Central District of California. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

18. Once victim funds were obtained, the syndicate utilized various money-laundering techniques to conceal the nature and source of the victim funds. These techniques include the use of money couriers, a high volume of financial transactions with no legitimate commercial purpose, and shell accounts.

19. Structurally, the money-laundering syndicate comprised of (1) money mules who received the fraud proceeds directly through

shell company accounts; (2) individuals who recruited, trained, and managed the money mules; (3) intermediary companies that facilitated the conversion of the fraud proceeds into cryptocurrency, or received cryptocurrency fraud proceeds directly and transfer them on; and (4) individuals who managed the network, connecting the organizations running the scamming operation with the laundering network.

B. Victim 1 Transfers Funds to Bahamas Account #1

20. On or about December 19, 2022, law enforcement interviewed Victim 1, who resided in Santa Ana, California, within the Central District of California. Victim 1 noted they were a victim of a cryptocurrency investment scam. More specifically, Victim 1 sent approximately $84,460 via wire transfers from their Bank of America account intended to be investments in cryptocurrency through a website called "gammaex.net" ("GAMMAEX"). Victim 1 noted that on or about August 24, 2022, they met an individual named "Daniel" on a Facebook dating app. Around that time, Victim 1 began chatting on WhatsApp and Telegram with Daniel. Victim 1 noted that they believed they were in a romantic relationship with Daniel. Further, Victim 1 provided law enforcement with their chat records with Daniel, and I can confirm the chats were romantic in nature.

21. Victim 1 noted that Daniel soon began promoting cryptocurrency investments and told Victim 1 they could make a lot of money. According to Victim 1, they did not understand cryptocurrency and Daniel provided Victim 1 with a link to a cryptocurrency investment website (GAMMAEX) to start making

investments. Victim 1 further stated that Daniel instructed Victim 1 to consult the online customer service portal to start making payments.

22. On or about September 26, 2022, Victim 1 contacted GAMMAEX customer service through the online portal and was directed to send $25,000 via wire from their Bank of America account to a wire address provided by the GAMMAEX customer service platform. Victim 1 then began to see via the GAMMAEX platform that they had made significant profit, which encouraged Victim 1 to make additional investments. On or about October 12, 2022, Victim 1 wired another $31,000 from their Bank of America account to a JPMC account ending 3886 ("JPMC account 3886"), in the name of Sea Dragon Trading, LLC, that was opened by Hailong Zhu,[5] who was the sole signatory of JPMC account 3886. Further, law enforcement learned JPMC account 3886 was registered to an address in California that is known to be associated with Zhu.

23. On or about October 24, 2022, Victim 1 then attempted to make a withdrawal from GAMMAEX; however, online customer service from GAMMAEX informed Victim 1 that their account was frozen and that they needed to pay $28,460 in taxes. Consequently, on or about October 24, 2022, Victim 1 wired $28,460 from their Bank of America account to another account provided by GAMMAEX. Victim 1 then attempted another withdrawal from GAMMAEX, and customer service informed Victim 1 that their account had been frozen due to suspicious activity and a security deposit of 30% was required

[5] Zhu is a defendant in United States v. Lu Zhang, 2:23-CR-596-RGK, discussed in paragraph 7 above.

to unfreeze their account. On or about November 12, 2022, when unable to withdraw any investment proceeds, Victim 1 concluded they were a victim of a scam and ceased making additional transfers.

24. Victim 1 has been unable to recover any of their funds. Victim 1 shared chat communications with law enforcement, which corroborate the false and fraudulent statements that induced Victim 1 to invest in the scheme.

25. Records obtained for JPMC account 3886 belonging to Sea Dragon Trading, LLC, reflect Victim 1's $31,000 deposit on October 12, 2022. JPMC records reveal that on October 17, 2022, $40,000 was wired from JPMC account 3886 to account associated with Bahamas Account #1.[6] Records obtained from Deltec Bank show that the $40,000 in fraud proceeds originating from JPMC account 3886 were deposited into Bahamas Account #1 on October 17, 2022.

26. Deltec Bank records also reveal that later, on October 17, 2022, the $40,000 in proceeds, including the $31,000 from Victim 1, were transferred to Delchain Limited[7] (hereinafter "Delchain") and used to purchase USDT.

27. Sea Dragon Trading, LLC has been the subject of numerous other victim complaints. California Secretary of State records show that Sea Dragon Trading, LLC was incorporated in Alhambra, California within Los Angeles County, in September of 2022. The

---

[6] As noted above, funds first flowed to a Deltec Bank-owned account at MUFJ in New York, New York, before transferring to Deltec Bank.

[7] Delchain Limited is a virtual-currency entity associated with Deltec Bank.

company is registered to a residential address with a stated business purpose of "General TRADING." Based on my training and experience, and review of documents, the company was not involved in "General TRADING," but rather, was a shell company set up for the sole purpose of receiving fraud proceeds.

28. Victim 1's experience with the fraud is generally consistent with those of hundreds of other victims who have reported their losses to law enforcement, including other victims in the Central District of California. Additionally, the set-up and operation of Sea Dragon Trading, LLC is consistent with that of another 73 shell companies that law enforcement has identified as being connected to this scheme, including numerous other companies incorporated in or associated with the Central District of California.

C. SU Provided Funding to Open Bahamas Account #1

29. According to Deltec Bank Records for Bahamas Account #1, Co-Conspirator 1, a Los Angeles-based individual, was the account owner of Bahamas Account #1, which received approximately $36.9 million in fraud proceeds from USSS-identified shell companies. During the account-opening process, Deltec Bank obtained income verification from Co-Conspirator 1. On or around June 15, 2022, Co-Conspirator 1 provided Deltec Bank with a screenshot of his Binance.US account balance, which showed the balance as $1,016,730.79 as of June 8, 2022. Binance.US is a cryptocurrency exchange.

30. Binance.US records reveal that before June 8, 2022, Co-Conspirator 1 had less than $100 in his Binance.US account.

Records show that on June 8, 2022, Co-Conspirator 1 received 9.9684 ETH (approximately $17,862[8]) from a Binance account. Records also show that Co-Conspirator 1's Binance.US account received three other deposit transactions from another Binance account on June 8, 2022, which include: 640,010 USDT ($640,010), 199.9984 ETH (approximately $358,373), and 1,000 USDT ($1,000). Binance records show that the 9.9684 ETH transaction came from a Binance account associated with **SU**, and the three other deposits came from a Binance account associated with Li.

31. Binance records show that **SU** opened his Binance account in his true name and used the email address jingliangsu@gmail[.]com. The subscriber information for **SU**'s Binance account also lists a mobile phone number of +8613269589330 ("the 9330 phone number"). The KYC documents for **SU**'s Binance account show a Chinese ID card that was issued on March 13, 2012, and a selfie-style photograph used for KYC verification during account opening. The Chinese ID and selfie photograph are included below. I recognize **SU** as the individual depicted on the Chinese ID card and in the selfie-style photograph because the photos match images found of the same individual under the same name in law enforcement databases. The photos also match photos taken of **SU** by authorities in the Dominican Republic, as further described below.

[8] The converted values of cryptocurrency listed herein are as of the time of the transaction, not the present value, unless stated otherwise.

Figure 1

32. On June 10, 2022, two days after the screenshots showing a large balance in Co-Conspirator 1's Binance.US account were taken, Co-Conspirator 1 returned 9.96651 ETH ($16,573) to **SU**'s Binance account. Based on these transactions, I believe Co-Conspirator 1 utilized funds from **SU** and Li, neither of whom were listed as authorized account holders at the time of account opening, to open Bahamas Account #1. Furthermore, the timing of the funds sent by and returned to **SU** indicates that the only purpose of the transfer from **SU** was to intentionally provide false income for Co-Conspirator 1 to facilitate the opening of Bahamas Account #1.

D. SU Actively Participated in Bahamas Account #1 Operations

33. Bank records and communications, including communications between **SU** and Co-Conspirator 1, show that **SU** had knowledge of the activity of Bahamas Account #1 and was an active participant in operating the account.

34. As discussed above, Bahamas Account #1 was used to receive incoming wires in fiat currency (U.S. dollars) and then convert those funds to the cryptocurrency Tether, or USDT. In order to communicate with Deltec Bank employees regarding the purchase and transfer of U.S. dollars to USDT, Deltec Bank (and its cryptocurrency affiliate Delchain) started a group chat on Telegram, an encrypted messaging platform. I have reviewed the message logs in this chat and know that on July 15, 2022, a user with the name "James S" joined the Telegram chat.

35. In these message logs, it appears that on August 5, 2022, at 12:29 p.m., Co-Conspirator 1 wrote, "Hello Delchain team: Please be advise[d] that moving forward on future transactions we will be using the following wallet address as a receiver wallet. TRteottJGH5caJyy9qFuM8EJJGGCpDaxx6 Axis (our team) group please kindly confirm the above information. Thank you." Message logs then show that at 12:30 p.m., "James S" wrote, "confirm."

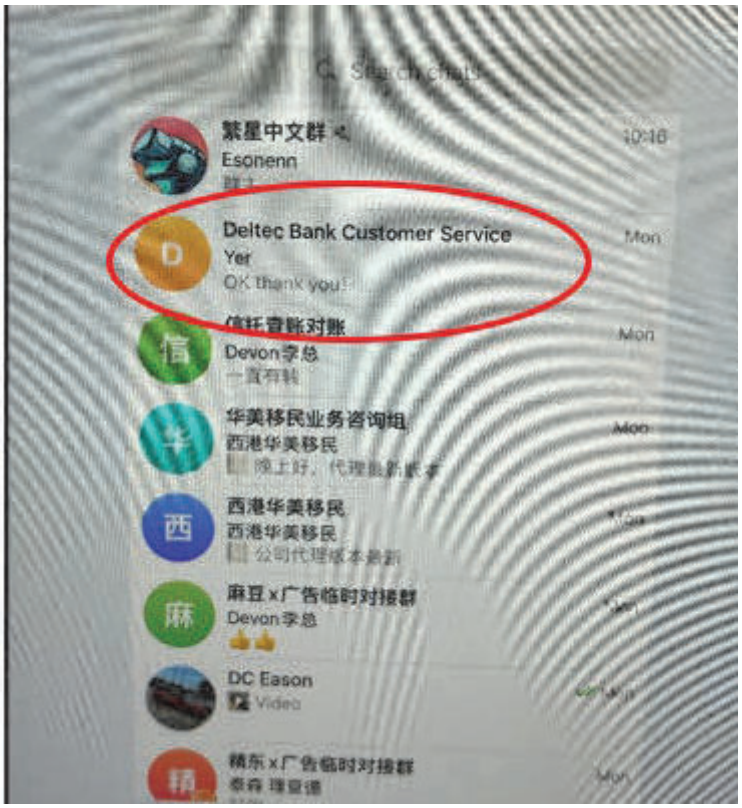
36. In April 2024, **SU** was arrested in the Dominican Republic for fraudulent use of a passport. As a result of that investigation, Dominican Republic law enforcement seized and searched two of **SU**'s cell phones, an Apple iPhone 13 Pro Max and an Apple iPhone 14 Pro Max (hereinafter "**SU**'s iPhone 13" and "**SU**'s iPhone 14," respectively, and collectively, "**SU**'s iPhones"). Dominican Republic law enforcement provided USSS with forensic images of **SU**'s iPhones.[9]

[9] A Mutual Legal Assistance Request to document the transfer of this evidence is pending with Dominican Republic.

37. I have reviewed the forensic images of **SU**'s iPhones and confirmed that the Telegram application was downloaded on **SU**'s iPhones. I have also reviewed messages on a different messaging platform, WhatsApp, between **SU** and Co-Conspirator 1 on **SU**'s iPhone 14. On December 28, 2022, **SU** asked Co-Conspirator 1, "Did the bank reply?" to which Co-Conspirator 1 answered, "Are you in the group? Do you see the activity?" **SU** replied, "I'm in the group, waiting for the bank's reply." From **SU**'s messages sent in this chat with Co-Conspirator 1, I believe the bank that **SU** is referring to is Deltec Bank.

38. I have reviewed additional WhatsApp messages on **SU**'s iPhone 13. On January 17, 2023, **SU** sent a photo of the last conversations in his Telegram chat history. One chat in that photo is titled "Deltec Bank Customer Service," shown below in Figure 2. From this, as well as other communications between **SU** and Co-Conspirator 1, I believe that the "James S" in the Delchain Telegram group chat is **SU**.

Figure 2



39. I have also reviewed messages between **SU** and Co-Conspirator 1 on **SU**'s iPhone 14, where they often discussed Bahamas Account #1. For example, on October 3, 2022, **SU** said to Co-Conspirator 1, "hi, bro. We had a few remittances last week and I want you to help me check if they have arrived." **SU** then sent a PDF titled "$250,000 (20220927)" and another PDF titled "$190,000 (20220927)."

40. The PDF titled "$250,000 (20220927)" is a wiring form from a U.S. financial institution showing $250,000 being sent from an entity called YXJ Trading Corporation to Bahamas Account #1. The PDF titled "$190,000 (20220927)" is a wiring form from another U.S. financial institution showing a wire for $190,000 sent by an

entity called YYJ Consulting Corporation for the benefit of Bahamas Account #1.

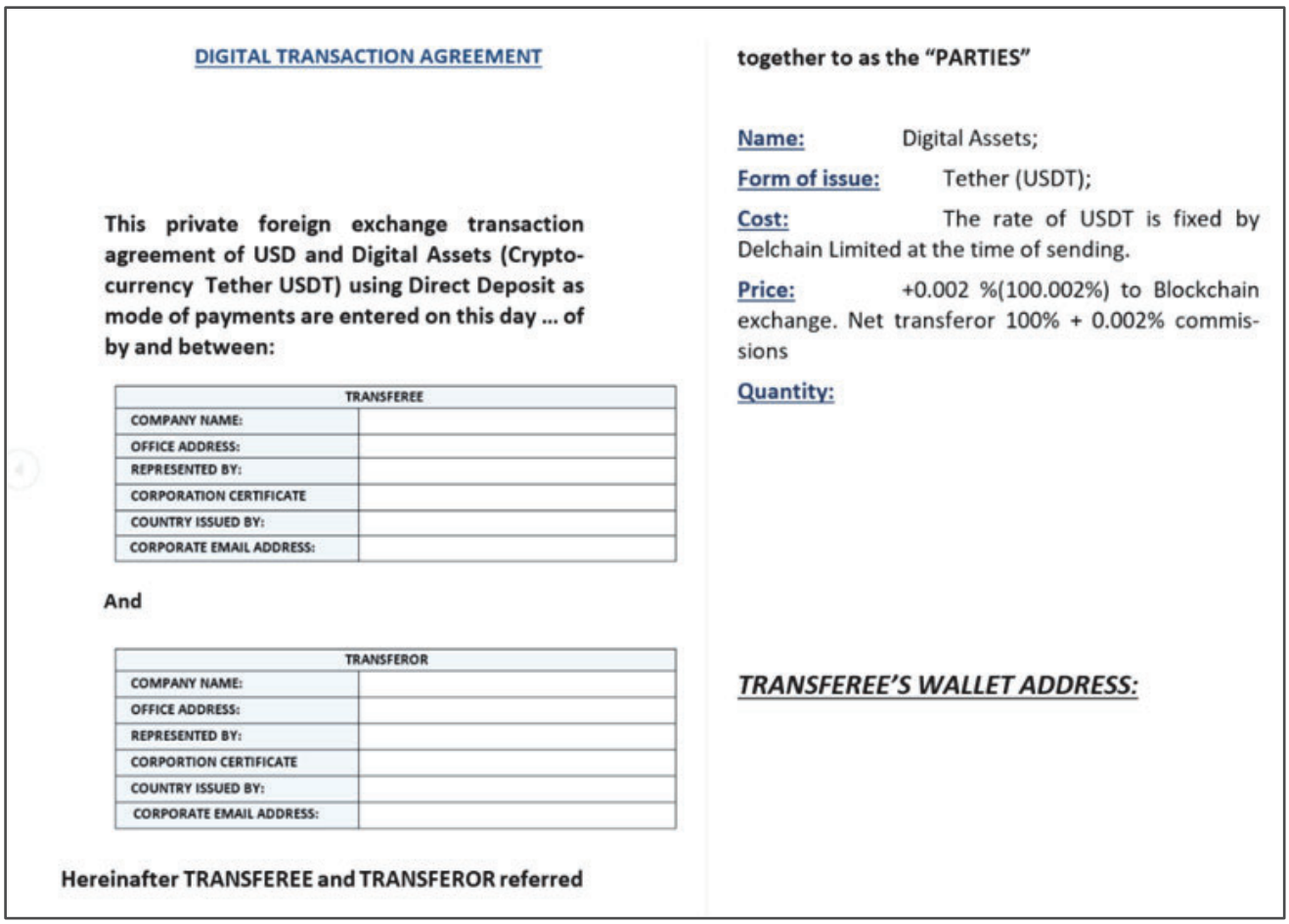
41. I know from the course of this investigation that YXJ Trading Corporation and YYJ Consulting Corporation were created and operated like Sea Dragon Trading, LLC – discussed above in connection with Victim 1. I also know that shell companies were set up in the United States by money mules for the purpose of moving fraud proceeds out of the United States, and that both YXJ Trading Corporation and YYJ Consulting Corporation received victim funds directly. I also know that these money mules would send copies of the wire forms to the group's leadership as proof that they were sending the funds to the intended recipient. The fact that **SU** had copies of and sent these wire forms indicates he was in communication with this group and knew when shell companies had wired funds to Bahamas Account #1.

F. SU Provided KYC Documents for Bahamas Account #1

42. Google records reveal that in July 2022, Co-Conspirator 1 emailed Co-Conspirator 2 a document titled "KYC Axis Digital Chinese." This document included basic client information that a business would typically require from a prospective customer to set up an account, such as identification, contact information, and a signature. In addition, on September 13, 2022, Co-Conspirator 1 sent Co-Conspirator 2 an email with the subject line, "Contract," that contained an attachment of a blank form entitled, "Digital Transaction Agreement", as shown below in Figure 3. The form appears to be a contract agreement between the transferee and

transferor for the exchange of U.S. dollars into USDT for an agreed upon exchange rate:

Figure 3



DIGITAL TRANSACTION AGREEMENT

This private foreign exchange transaction agreement of USD and Digital Assets (Crypto-currency Tether USDT) using Direct Deposit as mode of payments are entered on this day ... of by and between:

TRANSFEREE	
COMPANY NAME:	
OFFICE ADDRESS:	
REPRESENTED BY:	
CORPORATION CERTIFICATE	
COUNTRY ISSUED BY:	
CORPORATE EMAIL ADDRESS:	

And

TRANSFEROR	
COMPANY NAME:	
OFFICE ADDRESS:	
REPRESENTED BY:	
CORPORTION CERTIFICATE	
COUNTRY ISSUED BY:	
CORPORATE EMAIL ADDRESS:	

Hereinafter TRANSFEREE and TRANSFEROR referred

together to as the "PARTIES"

Name: Digital Assets;

Form of issue: Tether (USDT);

Cost: The rate of USDT is fixed by Delchain Limited at the time of sending.

Price: +0.002 %(100.002%) to Blockchain exchange. Net transferor 100% + 0.002% commis-sions

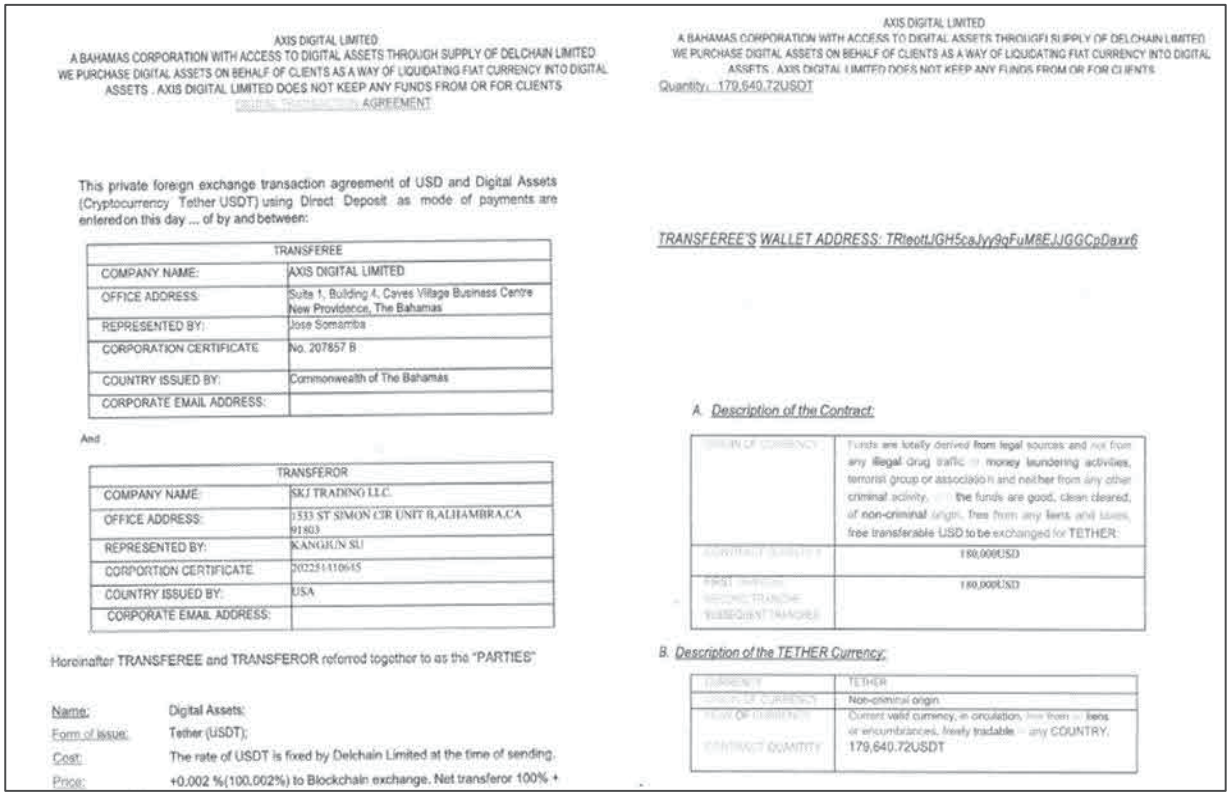
Quantity:

TRANSFEREE'S WALLET ADDRESS:

43. On September 15, 2022, Co-Conspirator 1 sent Deltec Bank four separate emails with subject line "Contract," "Contract 2," "Contract 3," and "Contract 4," all containing executed and signed versions of the same contract agreement that Co-Conspirator 1 sent to Co-Conspirator 2 on September 13, 2022. Figure 4 below shows a purported executed Digital Transaction Agreement between SKJ Trading LLC, a known shell company that received victim proceeds, and Bahamas Account #1 to convert $180,000 into 179,640.72 USDT

that was sent by Co-Conspirator 1 to Deltec Bank on September 15, 2022. All contracts appeared to have the same information in the "Transferee" section, along with the same Transferee wallet address.

Figure 4



AXIS DIGITAL LIMITED
A BAHAMAS CORPORATION WITH ACCESS TO DIGITAL ASSETS THROUGH SUPPLY OF DELCHAIN LIMITED
WE PURCHASE DIGITAL ASSETS ON BEHALF OF CLIENTS AS A WAY OF LIQUIDATING FIAT CURRENCY INTO DIGITAL ASSETS . AXIS DIGITAL LIMITED DOES NOT KEEP ANY FUNDS FROM OR FOR CLIENTS

AGREEMENT

This private foreign exchange transaction agreement of USD and Digital Assets (Cryptocurrency Tether USDT) using Direct Deposit as mode of payments are entered on this day ... of by and between:

TRANSFEREE	
COMPANY NAME:	AXIS DIGITAL LIMITED
OFFICE ADDRESS:	Suite 1, Building 4, Caves Village Business Centre New Providence, The Bahamas
REPRESENTED BY:	Jose Somamba
CORPORATION CERTIFICATE	No. 207857 B
COUNTRY ISSUED BY:	Commonwealth of The Bahamas
CORPORATE EMAIL ADDRESS:	

And

TRANSFEROR	
COMPANY NAME:	SKJ TRADING LLC.
OFFICE ADDRESS:	1533 ST SIMON CIR UNIT B,ALHAMBRA,CA 91803
REPRESENTED BY:	KANGJUN SU
CORPORTION CERTIFICATE	202251410645
COUNTRY ISSUED BY:	USA
CORPORATE EMAIL ADDRESS:	

Hereinafter TRANSFEREE and TRANSFEROR referred together to as the "PARTIES"

Name: Digital Assets:
Form of issue: Tether (USDT);
Cost: The rate of USDT is fixed by Delchain Limited at the time of sending.
Price: +0.002 %(100.002%) to Blockchain exchange. Net transferor 100% +

AXIS DIGITAL LIMITED
A BAHAMAS CORPORATION WITH ACCESS TO DIGITAL ASSETS THROUGH SUPPLY OF DELCHAIN LIMITED
WE PURCHASE DIGITAL ASSETS ON BEHALF OF CLIENTS AS A WAY OF LIQUIDATING FIAT CURRENCY INTO DIGITAL ASSETS . AXIS DIGITAL LIMITED DOES NOT KEEP ANY FUNDS FROM OR FOR CLIENTS

Quantity: 179,640.72USDT

TRANSFEREE'S WALLET ADDRESS: TRieotUGH5caJyy9qFuM8EJJGGCpDaxx6

A. Description of the Contract:

	Funds are totally derived from legal sources and not from any illegal drug traffic or money laundering activities, terrorist group or association and neither from any other criminal activity. the funds are good, clean cleared, of non-criminal origin, free from any liens and taxes, free transferable USD to be exchanged for TETHER.
	180,000USD
	180,000USD

B. Description of the TETHER Currency:

	TETHER
	Non-criminal origin
	Current valid currency, in circulation, free from liens or encumbrances, freely tradable any COUNTRY.
	179,640.72USDT

44. Law enforcement obtained records from Google regarding email account jingliangsu@gmail.com, the same account **SU** used to register for his Binance account. Google records list "James Su" as the name of the subscribing customer, and **SU**'s date of birth as the same date listed on the identity document provided to open **SU**'s Binance account, as shown in Figure 1 above. In addition, the subscriber information for jingliangsu@gmail.com lists the

9330 phone number as both the account holder's phone number and as a recovery phone number.

45. Google records reveal that **SU's** Google Drive contained what appears to be monthly folders with the Digital Transaction Agreements for hundreds of transactions. Based on review of the hundreds of Digital Transaction Agreements in **SU's** Google Drive, the contracts are substantially identical to the contracts shown above in Figures 3 and 4. Additionally, based on review of Bahamas Account #1 bank statements, these Digital Transaction Agreements correspond to transactions that Bahamas Account #1 received.

46. I have reviewed the Digital Transactions Agreements in **SU's** Google Drive. Based on my knowledge of this investigation, I believe that the purpose of these Digital Transaction Agreements agreements is to provide documentation to verify funds being sent to Deltec Bank in order to convert the fiat funds in Bahamas Account #1 into cryptocurrency. The Digital Transaction Agreements also provided a cryptocurrency address that the converted funds should be sent to. The vast majority of the funds were sent to the cryptocurrency address TRteottJGH5caJyy9qFuM8EJJGGCpDaxx6 ("Daxx6"), which is the same address **SU** confirmed was the correct address for the funds to be sent to in the Deltec Telegram chat referenced in paragraph 35 above.

47. In addition to the Digital Transactions Agreements, **SU's** Google Drive also contained multiple KYC forms for many of the shell companies that sent wires to Bahamas Account #1. I have reviewed victim complaints relating to many of these shell

companies reporting that victims fell victim to pig butchering fraud scams and sent funds to those shell companies. These KYC forms in **SU**'s Google Drive include Statements of Information, which often provide a type of business these shell companies were purportedly engaged in. I have reviewed these Statements of Information, and noted the types of business these companies stated, which included "logistics," "wholesale," and "remodeling services." There is no legitimate business reason why wholesale, logistics, or remodeling companies would be sending large dollar wires to a bank in the Bahamas for their funds to be converted into cryptocurrency.

48. Based on my training and experience, the fact that **SU** possessed the monthly Digital Transaction Agreements for hundreds of transactions supports that he participated in the management of Bahamas Account #1.

G. SU Prepared and Sent Ledgers Regarding Bahamas Account #1

49. I have reviewed messages between **SU** and Co-Conspirator 2, and another co-conspirator, Co-Conspirator 3, on **SU**'s iPhone 13. Co-Conspirator 3 is a Chinese national based in Japan. In these messages, **SU** sent what appears to be accounting ledgers showing how the profits would be shared from each shell company deposit into Bahamas Account #1. The ledgers **SU** sent specify a breakdown of payments made to Co-Conspirator 1, Co-Conspirator 2, Daren Li, and Co-Conspirator 3 regarding transactions sent to Bahamas Account #1. The ledgers **SU** sent largely match records provided by Deltec Bank for Bahamas Account #1. An example of a

ledger **SU** sent in a message to Co-Conspirator 2 and Co-Conspirator 3 on November 14, 2022, is shown below in Figure 5:

Figure 5

date	account name	transfer amount	status	cost	Total profit				
27/9/2022	YYJ CONSULTING CORPORATON	190000	1900	380	1520	608	380	380	152
27/9/2022	YXJ TRADING CORPORATION	250000	2500	500	2000	800	500	500	200
06/10/2022	GOOD LUCK TRADING LLC	30000	300	60	240	96	60	60	24
07/10/2022	GUDI TRADING INC	80000	800	160	640	256	160	160	64
07/10/2022	YYJ CONSULTING CORPORATON	45000	450	90	360	144	90	90	36
14/10/2022	GOOD LUCK TRADING LLC	50000	500	100	400	160	100	100	40
14/10/2022	QAG TRADING LLC	110000	1100	220	880	352	220	220	88
14/10/2022	QAG TRADING LLC	60000	600	120	480	192	120	120	48
17/10/2022	YYJ CONSULTING CORPORATON	102000	1020	204	816	326.4	204	204	81.6
17/10/2022	SEA DRAGON TRADING LLC	40000	400	80	320	128	80	80	32
17/10/2022	SEA DRAGON TRADING LLC	15000	150	30	120	48	30	30	12
18/10/2022	QAG TRADING LLC	40000	400	80	320	128	80	80	32
18/10/2022	YYJ CONSULTING CORPORATON	78000	780	156	624	249.6	156	156	62.4
19/10/2022	GUDI TRADING INC	60000	600	120	480	192	120	120	48
19/10/2022	GOOD LUCK TRADING LLC	64000	640	128	512	204.8	128	128	51.2
20/10/2022	QAG TRADING LLC	72000	720	144	576	230.4	144	144	57.6
20/10/2022	YYJ CONSULTING CORPORATON	59000	590	118	472	188.8	118	118	47.2
20/10/2022	SEA DRAGON TRADING LLC	225000	2250	450	1800	720	450	450	180
21/10/2022	GOOD LUCK TRADING LLC	86000	860	172	688	275.2	172	172	68.8
21/10/2022	QAG TRADING LLC	40000	400	80	320	128	80	80	32
24/10/2022	QAG TRADING LLC	53000	530	106	424	169.6	106	106	42.4
TOTAL		1749000	17490	3498	13992	5596.8	3498	3498	1399.2

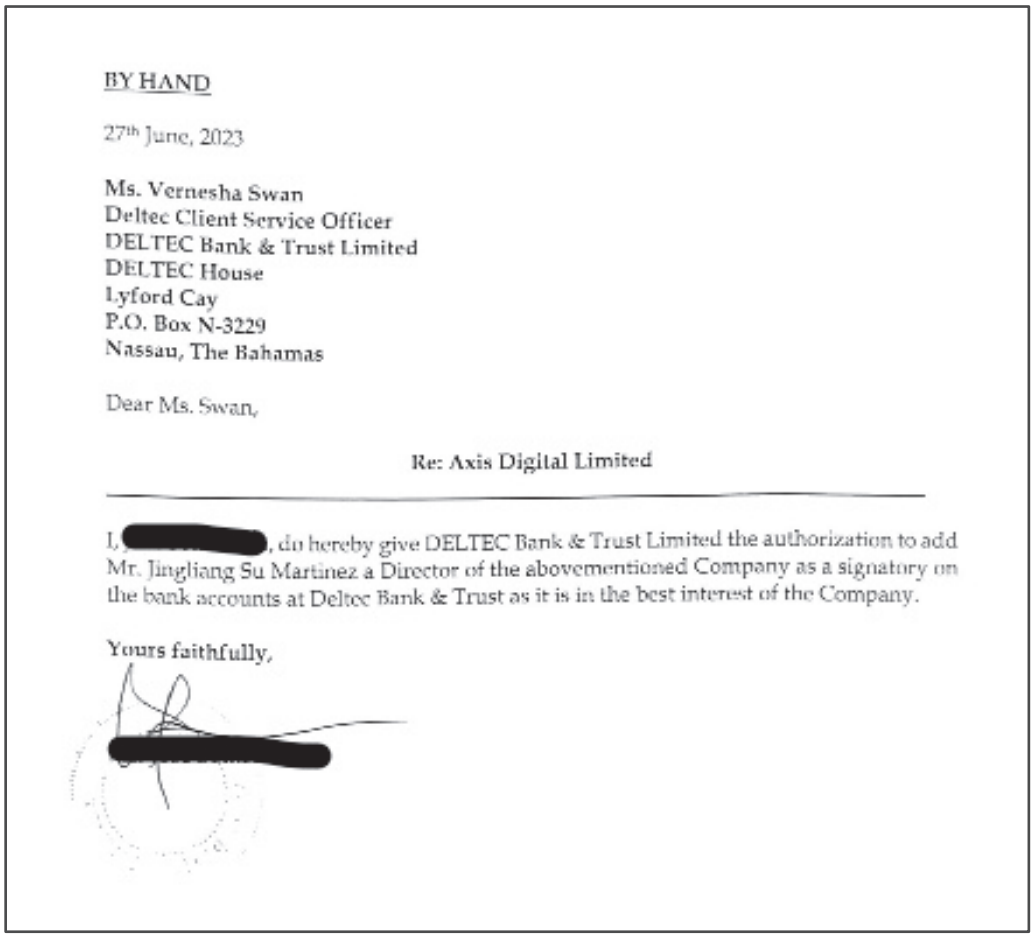
50. **SU** sent similar ledgers on at least two other occasions in messages to Co-Conspirator 2 and Co-Conspirator 3 on January 14, 2023, and February 10, 2023. Moreover, on November 14, 2022, approximately one hour before sending the ledger depicted above as Figure 5, **SU** sent a message in Mandarin that was translated by a USSS Linguist to English that reads, "I just completed the profit sharing." **SU** then sent the ledger depicted in Figure 5.

H. SU Was Added as Signatory for Bahamas Account #1

51. I have reviewed messages between **SU** and Co-Conspirator 1 on **SU**'s iPhone 14. On June 27, 2023, Co-Conspirator 1 sent **SU** a PDF titled "2023-06-27 12-47." The PDF is a memorandum dated June 27, 2023, from Co-Conspirator 1 to Deltec Bank. The memorandum pertains to Bahamas Account # 1 and states that **SU** is

a Director of Bahamas Account #1. The memorandum further gives authorization for Deltec Bank to add **SU** as a signatory of Bahamas Account #1, using the name "Jingliang Su Martinez." The memorandum is attached below as Figure 6.

Figure 6



BY HAND

27th June, 2023

Ms. Vernesha Swan
Deltec Client Service Officer
DELTEC Bank & Trust Limited
DELTEC House
Lyford Cay
P.O. Box N-3229
Nassau, The Bahamas

Dear Ms. Swan,

Re: Axis Digital Limited

I, [redacted], do hereby give DELTEC Bank & Trust Limited the authorization to add Mr. Jingliang Su Martinez a Director of the abovementioned Company as a signatory on the bank accounts at Deltec Bank & Trust as it is in the best interest of the Company.

Yours faithfully,

[redacted]

I. SU's Binance Account Directly Launders Victim Proceeds

52. A financial analysis of **SU**'s Binance account also reveals that **SU** moved direct victim proceeds into the Daxx6 cryptocurrency address. USSS identified an Internet Crime Complaint Center ("IC3") complaint in which an individual ("Victim 2") stated that they fell victim to a pig butchering fraud scam.

Per the IC3 complaint, Victim 2 met an individual on LinkedIn and began to communicate with them online. In the course of these conversations, Victim 2 was convinced to invest in gold options via the purchase of cryptocurrency. Victim 2 stated that they purchased cryptocurrency to "invest" by sending wires to various cryptocurrency exchanges, including Coinbase, from Victim 2's Bank of America account ending in 3898 ("BOA account 3898").

53. I have reviewed Coinbase records for Victim 2's account with that cryptocurrency exchange. These records show that on October 3, 2022, Victim 2 deposited $24,990 dollars from BOA account 3898 into their Coinbase account. The Coinbase records for Victim 2's account show that Victim 2 used these funds to purchase 18.54048775 worth of ETH, and then later that day, transferred the purchased ETH to an unhosted wallet address.[10] Minutes later, the funds were sent to another unhosted wallet address, which then sent nearly the same amount of funds to a service called Tokenlon, where the funds were swapped from 18.47 ETH to 24,274.23 USDT and sent to another unhosted wallet address.

54. The 24,274.23 USDT were then comingled with other funds in the wallet, and the next day, on October 4, 2022, the wallet sent 36,737 USDT, including Victim 2's funds, to another unhosted wallet address. That unhosted wallet subsequently had two withdrawals, with no additional deposits. One of these withdrawals, for 30,000 USDT, was sent again through two additional

[10] An unhosted cryptocurrency wallet is a wallet that is not hosted by a cryptocurrency exchange. The user/users who hold the private keys to the wallet is typically the only one who can access and manage their cryptocurrency assets.

unhosted wallet addresses. Finally, on October 13, 2022, 75,000 USDT, which included Victim 2's funds, were sent from the unhosted wallet address to **SU**'s Binance account.

55. Furthermore, an analysis of the withdrawals from **SU**'s Binance account show that, on October 13, 2022, following the deposit of the 75,000 USDT into **SU**'s Binance account, 69,291.2 USDT were sent from **SU**'s Binance account to Daxx6 (the same address to which the shell company victim funds were sent).

56. Based on the above analysis of Victim 2's Coinbase account, public blockchain ledgers, and **SU**'s Binance account, I believe that **SU** directly received laundered victim proceeds and then moved the funds to the Daxx6 address.

VI. CONCLUSION

57. Based on my training and experience, there is probable cause to believe **SU** and co-conspirators facilitated the transfer of victim funds to domestic and international bank accounts. Co-conspirators set up approximately 74 U.S. shell companies that received millions of dollars in wire fraud proceeds from victims of cryptocurrency investment scams. **SU** worked with co-conspirators to open and manage Bahamas Account #1, maintained information on the fraudulent shell companies, and organized payments between co-conspirators for the scheme. **SU** also received victim proceeds into his personal cryptocurrency account.

58. For all of the reasons described above, there is probable cause to believe that **SU** has committed a violation of conspiracy to commit money laundering, in violation of Title 18, United States

Code, Section 1956(h) involving the proceeds of wire fraud, in violation of Title 18, United States Code, Section 1343.

Attested to by the applicant
In accordance with the requirements
Of Fed. R. Crim. P. 4.1 by
Telephone on this 22nd day of
November, 2024.

Alicia G. Rosenberg
_____
THE HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE