IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

ALL FUNDS, UP TO THE AMOUNT OF $58,465,480 HELD OR STORED AT MITSUBISHI UFJ TRUST AND BANKING CORPORATION ACCOUNT 1110910328, IN THE NAME OF DELTEC BANK AND TRUST	Case No. 1:23-sw-326

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Christopher Saunders, being duly sworn, hereby declare as follows:

AGENT BACKGROUND

1. I am a Special Agent employed by the U.S. Secret Service ("USSS"). I have been employed as a Special Agent with the USSS since 2018. I am thus a "federal law enforcement officer" as defined by Fed. R. Crim. P. 41(a)(2)(C). I am currently assigned to the Global Investigative Operations Center ("GIOC") at the Criminal Investigative Division ("CID") located at USSS Headquarters. I have received specialized training in the area of cryptocurrency crimes. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Glynco, Georgia and the USSS Special Agent Training Course in Beltsville, Maryland. I am a Certified Public Accountant, and my duties include conducting criminal investigations into complex financial crimes, cryptocurrency crimes, computer fraud, access device fraud, wire fraud, mail fraud, identity theft, telecommunications fraud and money laundering. In these investigations, I have been involved in the execution of warrants.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

PROPERTY TO BE SEIZED

3. This affidavit is made to obtain a seizure warrant for all funds, up to the amount of $58,465,480, held or stored at Mitsubishi Bank UFJ Trust and Banking, in account 1110910328 in the name of Deltec Bank and Trust ("SUBJECT ACCOUNT"). MUFJ is located in the Southern District of New York.

LEGAL AUTHORITY FOR SEIZURE

4. Based on my experience and the information contained in the subsequent paragraphs, I have probable cause to believe that funds, up to the amount of $58,465,480 in the SUBJECT ACCOUNT are subject to seizure and forfeiture because they are proceeds of wire fraud, in violation of 18 U.S.C. § 1343; bank fraud, in violation of 18 U.S.C. § 1344; and/or involved in money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and as such are subject to criminal and civil forfeiture, pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 28 U.S.C. § 2461(c), and 18 U.S.C. § 982(a) (criminal forfeiture), and 18 U.S.C. § 981(a)(1)(A) (civil forfeiture).

5. 18 U.S.C. § 1343 (wire fraud) prohibits, in pertinent part, 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, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

6. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, 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 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.

7. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

8. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept. The statute does not, however, allow the government to reach back in time for an unlimited period. A forfeiture action (including a seizure) against property not directly traceable to the offense that is the basis for the forfeiture cannot be commenced more than one year from the date of the offense.

9. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or a conspiracy to commit such is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C). Specifically, § 981(a)(1)(C) provides for the forfeiture of any proceeds traceable to any offense constituting a specified unlawful activity ("SUA"), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of

Title 31 of the U.S. Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

10. Any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 as well as any property traceable to such property is subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

11. Any property, real or personal, involved in a violation of 18 U.S.C. § 1956 or any property traceable to that property is subject to criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

12. 28 U.S.C. § 2461I provides that if a person is charged in a criminal case with a violation for which the civil or criminal forfeiture of property is authorized, the government may include notice of the forfeiture in the charging instrument pursuant to the Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to forfeiture, the Court shall order forfeiture of the property as part of the defendant's sentence. The procedures of 21 U.S.C. § 853 shall apply to all stages of a criminal forfeiture proceeding, except for subsection (d) of that statute.

13. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains, and to divest criminal actors from the apparatus allowing them to engage in criminal activity. *See Kaley v. United States*, 571 U.S. 320, 323 (2014). To that end, in cases involving a money laundering offense, the forfeiture statutes connected to money laundering offenses permit the government to forfeit property "involved in" money laundering. Such property includes "untainted property" commingled with "tainted" property, when that untainted property is used to facilitate the laundering offense, such as by obscuring the nature, source, location, or control of any criminally derived property. *See* Title 18, United States Code, Sections 981(a)(1)(A), 982(a)(1); *see also United States v. Miller*, 911 F.3d 229, 234 (4th

Cir. 2018); *United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013).

14. This Court has the authority to issue seizure warrants for assets located in another district and even outside the U.S. pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that, "[n]otwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)] and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement." 18 U.S.C. § 981(b)(3). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located outside the district.

15. Based on my training, experience, and the information contained in this affidavit, there is probable cause to believe that funds in the SUBJECT ACCOUNT, up to $58,465,480 are subject to both civil and criminal forfeiture as proceeds traceable to a wire fraud scheme, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). The funds in of the SUBJECT ACCOUNT, up to the sum of $58,465,480 are also subject to both civil and criminal forfeiture as property involved in money laundering, pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). The balances in the SUBJECT ACCOUNT are therefore subject to civil and criminal seizure.

TECHINCAL BACKGROUND

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

17. "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.[1] Examples of cryptocurrency are bitcoin (BTC), Ether (ETH), Tether (USDT), and USD Coin (USDC). Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged 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.[2] Cryptocurrency is not illegal in the United States.

18. 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

---

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

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

instance, 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 due to customers being more transient. 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 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.

19. A domain name is a simple, 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.

20. 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.

SUMMARY OF PROBABLE CAUSE

21. Law enforcement has been investigating organized, international criminal money laundering syndicates operating cryptocurrency investment and other wire fraud scams. Victims were fraudulently induced to transfer money into shell companies, at which point the money

underwent a series of transfers, generally ending overseas, designed to conceal the source, nature, ownership, and control of the funds.

22. Specifically, 74 different shell companies received wire fraud proceeds and subsequently transferred those proceeds to and through the SUBJECT ACCOUNT, to ultimate beneficiaries overseas. The SUBJECT ACCOUNT received at least $58,465,480 from these shell companies since June of 2022. As will be discussed in more detail herein, the criminal enterprise used the SUBJECT ACCOUNT to send wire fraud proceeds indirectly to accounts in the Bahamas and structured the transfers in such a way as to avoid scrutiny that typically applies to international wire transfers. Law enforcement identified approximately 157 victims who had transferred money to 63 of these shell companies and interviewed approximately 43 of them.[3] Approximately$13.4 million dollars from the 43 victims interviewed by law enforcement flowed through the SUBJECT ACCOUNT. Approximately $50.2 million from the 63 victim-associated shell companies flowed through to the SUBJECT ACCOUNT. Law enforcement also identified another 11 companies that had similar characteristics and money transfer patterns to the 63 victim-associated entities. These 11 companies transferred an additional $8.2 million to the SUBJECT ACCOUNT. This information is summarized in **EXHIBIT A**, attached to this affidavit. As discussed below, the evidence indicates there is probable cause to believe that the $58,465,480 that has passed through these shell companies and into the SUBJECT ACCOUNT represents the proceeds of wire fraud and/or is property involved in money laundering.

23. Additionally, it appears that Deltec Bank and Trust has misrepresented the purpose and use of the SUBJECT ACCOUNT to Mitsubishi UFJ Trust and Banking (herby after "MUFJ").

---

[3] As discussed further in section C below, victims who were not personally interviewed by USSS law enforcement were identified based on records of complaints they reported.

According to MUFJ, the SUBJECT ACCOUNT is intended to be a "custody account" which means that all transactions in are for the benefit of Deltec. MUFJ noted that the stated purpose of the SUBJECT ACCOUNT is for custodial services, including but not limited to the safekeeping of securities, receipt and delivery of securities, funds transfer, and corporate action processing. However, it appears that in addition to the money laundering transactions discussed above, Deltec has also allowed the account to be used by other third parties, in activity that would not reasonably be anticipated in a custody account and that has allowed individuals to avoid the scrutiny and vetting that international transactions might otherwise receive.

FACTS SUPPORTING PROBABLE CAUSE

A. Investigation Background

24. In September 2022, law enforcement began an investigation into criminal money laundering syndicates operating cryptocurrency investment scams. The scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S. victims. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

25. This type of scam is often called "pig butchering" (derived from the Chinese phrase used to describe this scheme) and involves scammers spending significant time getting to know and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds via wire instructions or through a provided BTC, USDT, ETH or USDC deposit address. While the scammers prefer cryptocurrency deposits, they will also accept bank wires if the victim cannot transfer cryptocurrency. As part of the scheme

to invest, the victims are further told that they can expect to make a sizable return on their investments. As investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which encourages the victim to continue making investments. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve any portion of their investment.

26. As of on or around May 17, 2023, the USSS had identified approximately 143 self-reported victims associated with one particular "pig butchering" syndicate that operates primarily through the use of spoofed domains that is responsible for more than $50 million directly traceable to reported victim losses. Law enforcement continues to identify and notify additional victims of this fraudulent scheme and believes the actual losses are significantly higher than $50 million.

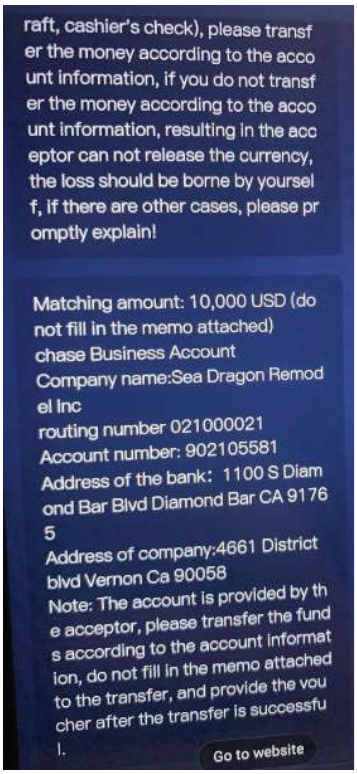
27. Once victims' funds are obtained, the syndicate utilizes various money laundering techniques to conceal the nature and source of the victim funds. These techniques include the use of money couriers, an unnecessary number of financial transactions, and shell accounts.

B. Cryptocurrency Investment Wire Fraud Scheme

28. On or about September 1, 2022, law enforcement conducted an undercover operation in which an undercover agent (hereinafter, "UCA") visited and created an account at one of the spoofed domains at which a number of victims had "invested" and subsequently lost their money. This domain, simexlua.com, spoofed legitimate sites operated by the Singapore International Monetary Exchange (SIMEX). The UCA began communicating with online

customer service, through the chat portal, about making investments. Shortly thereafter, online customer service provided the UCA with instructions to invest funds by sending a wire to a company named "Sea Dragon Remodel Inc," as shown in **FIGURE 1** below.

FIGURE 1



29. Law enforcement obtained legal process for the account displayed in **FIGURE 1**, which is a JPMorgan Chase (hereinafter, "JPMC") account. According to JPMC records, the account ending in 5581 (hereinafter, "JPMC account 5581") was opened by HAILONG ZHU (hereinafter, "ZHU") on October 21, 2022, for a business called Sea Dragon Remodel Inc. ZHU was the sole signatory listed on the account. In the documents used to open the bank account, ZHU provided an address on District Blvd in Vernon, California, along with other information.

30. According to JPMC records, ZHU is also the sole signatory of a JPMC bank account ending in 3886 (hereinafter, "JPMC account 3886"), which was opened as a business checking account on September 9, 2022, for a business called Sea Dragon Trading LLC. In the

documents used to open the bank account, ZHU provided an address located on S El Molino St in Alhambra, California. Law enforcement determined ZHU opened a number of accounts in the names of these two Sea Dragon entities.

31. Transactional records from ZHU's various bank accounts identified wires from multiple individuals later determined to be pig butchering victims. Included among those victims is an individual living in Falls Church, Virginia (hereinafter, "Victim 1").

C. Victim Fund Transfers to ZHU's Sea Dragon Remodel Accounts

32. On or about January 6, 2023, law enforcement interviewed "Victim 1". At all times relevant to this complaint, Victim 1 resided within the Eastern District of Virginia. Victim 1 stated that in or around June 2022, they received an unsolicited call from a female identifying herself as "RACHEL." According to Victim 1, their initial conversation started with "RACHEL" apologizing for dialing the wrong number but quickly transitioned into a more general conversation. "RACHEL" also moved the conversation to Telegram.[4]

33. Victim 1 stated that over several months the conversations became more romantic, and "RACHEL" introduced cryptocurrency investment ideas. According to Victim 1, "RACHEL" provided a link to a fraudulent cryptocurrency investment domain named "coinasx.com" where Victim 1 was led to download an application directly to his mobile device. The downloaded platform used the name "ASX," which mimicked the Australian Securities Exchange.

34. Victim 1 spoke with a purported customer service representative on the "coinasx.com" online chat portal, who explained to Victim 1 how to invest in "coinasx.com." "RACHEL" encouraged Victim 1 invest in "ASX." Victim 1, who was not familiar with

[4] Telegram is an encrypted messaging service that also offers audio and video calling and file sharing.

cryptocurrency, agreed to make his investment into "ASX" by sending wire transfers. These conversations occurred while Victim 1 was located in the Eastern District of Virginia.

35. On or about August 12, 2022, and after Victim 1 was provided with wire instructions from an "ASX" online customer service representative, Victim 1 made a $1,100 investment from their bank account in the Eastern District of Virginia. Victim 1 then began seeing significant "profits" in their account and invested additional money via at least six other wire transfers between August and at least November 2022. Victim 1 initiated these wires from within the Eastern District of Virginia.

36. "ASX" customer service provided Victim 1 with different addresses for each wire transaction. On November 25, 2022, Victim 1 invested $5,000 via a wire to Bank of America ("BOA") account 9529 belonging to Sea Dragon Remodel Inc., for which ZHU is the sole signatory. Victim 1 also sent wires to accounts in the name of entities including Haights Kim Trading Inc ($1,100 on August 12, 2022), PBB International Consulting ($15,100 on September 2022), and Jishun Limited ($5,000 on November 17, 2022). Victim 1 informed law enforcement that they have been unable to make any withdrawals or recover any amount of their investments. In addition to Sea Dragon Remodel Inc., as reflected in **EXHIBIT A**, PBB International Consulting also transferred funds to the SUBJECT ACCOUNT.

37. To date, law enforcement has identified approximately six other victims who have transferred money into either ZHU's BOA account 9529 or his JPMC account 3886.

38. Relatedly, none of the entities to which Victim 1 transferred money had names with any relation to "ASX," coinasx, or any other cryptocurrency investment site. Additionally, law

enforcement has reviewed victim complaints within FBI's Internet Crime Complaint Center (IC3)[5] that indicate these other businesses have received funds from other fraud victims. Like ZHU's Sea Dragon entities, these other companies appear to also be shell companies incorporated to launder pig butchering proceeds.

D. Sea Dragon Account Funds Traceable to and through SUBJECT ACCOUNT

39. Records obtained for BOA account 9529 belonging to Sea Dragon Remodel Inc. reflect Victim 1's $5,000 deposit on November 25, 2022. On November 29, 2022, $53,000 was wired from BOA account 9529 to Mitsubishi UFJ Banking and Trust Account 1110910328 held by Deltec Bank (the SUBJECT ACCOUNT). **FIGURE 2** below depicts the wire instructions executing this transaction reflected in BOA account 9529's records.

FIGURE 2

11/29/22	WIRE TYPE:WIRE OUT DATE:221129 TIME:0939 ET TRN:2022112900296167 SERVICE REF:367903 BNF:MITSUBISHI UFJ TR AND BKG ID:000544777694/(BC BNF BK:JPMORGAN CHASE BANK, N. ID:0002 PMT DET:414 866558 FOR FURTHER CREDIT TO 1110910328 DB	-53,000.00

40. These instructions reveal the initial recipient of the transfer was an account ending 7694 at MUFJ held by BANK 1. Further investigation revealed that MUFJ account 7694 is BANK 1's correspondent account at MUFJ. Based on my training, experience, and investigation, I know that a correspondent account is generally used by a financial institution for transactions on behalf of another financial institution; as such, a correspondent account is typically not listed as a direct beneficiary from individual customers.

41. The instructions next included additional directions reading "For Further Credit to 1110910328 DB," which is the SUBJECT ACCOUNT. The "for further credit" instruction

[5] The FBI's Internet Crime Complaint Center (IC3) is an online portal that provided victims a reliable and convenient way to self-report internet crimes to law enforcement.

(sometimes written as "FFC") means that the proceeds should be "further credited"—i.e., transferred—from BANK 1's account 7694 to the SUBJECT ACCOUNT. At this point, the character limit has been met for this specific bank, so any additional instructions beyond this point are not visible on the bank statement.

42. Law enforcement identified eight total transactions from November to December 2022 totaling $384,600 from ZHU's BOA account 9529 first to BANK 1's account 7694 and then to the SUBJECT ACOUNT. Law enforcement also identified approximately seven other pig butchering victims who had transferred money into BOA account 9529.

43. ZHU's JPMC account 3886 engaged in similar transactions. For example, on October 12, 2022, JPMC account 3886 received $31,000 from an individual who informed law enforcement that they were a victim of a pig butchering scheme. On October 17, 2022, ZHU or other co-conspirators wired $40,000 from JPMC account 3886 to the SUBJECT ACCOUNT. **FIGURE 3** depicts the wire transfer as reflected in the JPMC account 3886 statements. JPMC wire forms indicate that the initial recipient of this wire was again BANK 1's account 7694 at MUFJ. The wire then directed that the money be further transferred to the SUBJECT ACCOUNT at "DBT." Further investigation has determined that "DBT" means Deltec Bank and Trust. Finally, the additional instructions include "FFC 1002179 00 Axis Digital Limited." Further investigation revealed that these additional instructions meant the funds were ultimately to be transferred to a Deltec customer named Axis Digital Limited.

FIGURE 3

DATE	DESCRIPTION	AMOUNT
10/17	10/17 Domestic Wire Transfer A/C: Mitsubishi Ufj Trust And Banking New York NY 10020- US Ref: Mitsubishi Ufj Trust And Banking Corporation, NY Branch Further Credit :1110910328 Dbt Ffc 1002179 00 Axis Digital Limited Trn: 3503062290Es	$40,000.00

44. Additionally, as shown in **FIGURE 3**, it appears that ZHU or other co-conspirators

indicated this transfer was a domestic wire.[6] I also reviewed other instances of online wire forms transferring proceeds from JPMC account 3886 to the SUBJECT ACCOUNT that contained the same FFC instructions to Axis Digital Limited. The online wire forms specifically reflect that the wires were domestic wires with a U.S. beneficiary. However, the Axis Digital Limited account is an account at Deltec Bank, which is located in the Bahamas. By using this system of "for further credit" instructions, ZHU and his co-conspirators sent money overseas without complying with the regulatory scrutiny and requirements that normally accompany international transfers.

45. Law enforcement also identified numerous other transactions out of ZHU's Sea Dragon accounts that were first routed to BANK 1's account 7694; then to the SUBJECT ACCOUNT; and then to Deltec bank account number 1001924, held by an entity named "GTAL." These transactions were similarly marked as domestic wires, despite ending overseas. Based on my training, experience, and this investigation, it is not common for customers to utilize, much less know, banking correspondent account numbers to be listed in the wire form.

E. Investigation of Sea Dragon and Related Entities

46. Investigation has revealed that Sea Dragon Trading and Sea Dragon Remodel are not legitimate businesses. I reviewed the incorporation documents for Sea Dragon Trading and Sea Dragon Remodel. Sea Dragon Trading was incorporated with the stated purpose of "general TRADING," and Sea Dragon Remodel was incorporated for "remodel and distribution of construction material." Based on review of the associated bank records, there were no transactions which appeared to be related to "trading" or for "remodel and distribution of construction material," such as incoming or outgoing payments to or from construction suppliers or other

[6] JPMC accounts indicate whether a wire was domestic versus international. If the wire is domestic, the description will read "domestic wire transfer" and if the wire is international, the description will read "international wire transfer."

trading businesses. Additionally, these businesses have no online presence and searches in the California Database of licensed contractors for Sea Dragon Remodel, Sea Dragon Trading, and ZHU, found no results.

47. Furthermore, a review of financial records related to the Sea Dragon bank accounts found mostly round number wires (*e.g.* $100,000 or $75,000) coming in from remitters throughout the United States, including Massachusetts, Florida, Maryland, Illinois, Rhode Island, Kansas, Connecticut, New Jersey, Pennsylvania, South Dakota, Nebraska, Montana, and Louisiana, as well as one from Canada. First, it is highly unusual for a "Remodeling" or "Trading" company based in California to receive wires from customers out of state. Second, it is highly unusual for a business account to receive so many transfers in round numbers, which do not reflect the typical cost variables associated with supplies, taxes, and services rendered in remodeling or "trade" businesses.

48. Furthermore, ZHU was arrested on March 21, 2023 and was subsequently indicted for conspiracy to commit money laundering in case number 1:23-cr-81. At the time of his arrest, ZHU voluntarily participated in a *Mirandized* interview. ZHU stated he became involved in the scheme when he responded to an online advertisement and was promised $70,000 to create entities, open business accounts, and execute wire transfers. Though ZHU reported no personal knowledge of how to create entities and open businesses, he reported he received directions from another individual, J.W. ZHU was told that he could expect that some of the accounts he created would be closed and that he might be blacklisted by banks. ZHU reported that he did not provide any services for the businesses that he created.

49. Also on March 21, 2023, USSS agents executed search warrants at J.W.'s residence. During the search warrants, USSS agents seized numerous iPhone mobile devices

belonging to J.W. One bookbag in particular contained five devices. A review of the devices led agents to conclude that J.W. used at least three of these devices to conduct banking activity, including directing wire transfers, in the names of different people, to include ZHU. During the search warrants, agents seized check stock, credit cards and bank statements related to Sea Dragon Trading LLC, Sea Dragon Remodel Inc, Good Luck Trading LLC, Mingxing Trading LLC, Mingxing Remodel LLC, and Hong's Trading LLC, among others. Through IC3 reports and victim interviews, law enforcement determined that between October 2022 to December 2022, all of these shell companies had received fraud proceeds and then subsequently wired such proceeds to the SUBJECT ACCOUNT. *See* **EXHIBIT A**.

50. For example, Victim 2 was fraudulently induced to invest $230,000 via four wires into a cryptocurrency investment platform later determined to be fraudulent. One of these wires was for $25,000 on October 27, 2022, to Mingxing Trading, LLC's JPMC account ending 5251. MUFJ records show that on November 9, 2023, $200,000 was transferred from this account to the SUBJECT ACCOUNT. The wire included the instructions "for further credit to" the SUBJECT ACCOUNT, with additional instructions "FFC" GTAL.[7]

51. USSS agents also seized a Bank of the West cashier's check from J.W's vehicle, which was remitted by Good Luck Trading LLC and made payable to Good Luck Trading LLC for $72,172. The memo of the cashier's check stated, "Checking account closure." Further investigation has revealed that J.W. was not the individual who had registered Good Luck Trading

[7] Note that MUFJ records do not show the initial transfer to BANK 1. MUFJ records do however show that the instructions state, "for further credit to" the SUBJECT ACCOUNT and "FFC" GTAL. Based to the fact that the transfers contain "for further credit to" the SUBJET ACCOUNT indicates that the funds passed through another account before the SUBJECT ACCOUNT. As discussed above and shown in Figures 2 and 4, it has been determined that the funds initially passed through BANK 1.

LLC as a business and was not the signer on the Good Luck Trading account, but MUFJ bank records reveal the address listed on the Bank of the West Good Luck Trading LLC account was the address where J.W. resided. I know that money launderers will often use the residential address of an individual in the conspiracy to ensure they are able to retrieve the closing out cashier's check if the account is closed due to fraud. Law enforcement believes that J.W. played the same role directing and supervising the opening and control of the Good Luck Trading's bank accounts that he did for ZHU's Sea Dragon bank accounts.

52. As a result of the information discussed above, there is probable cause to believe that all of the transactions into ZHU's accounts and the other accounts found to be under J.W.'s control are fraudulent in nature and that there is no "clean" money passing through these accounts.

F. Analysis of the SUBJECT ACCOUNT and Identification of Funds Subject to Seizure

53. Law enforcement reviewed transactional records for the SUBJECT ACCOUNT. The account is owned by Deltec Bank and Trust (hereafter, "Deltec"), a bank licensed and operating in the Bahamas. Deltec opened the account on or around September 2021.

54. Information provided by MUFJ indicated that the SUBJECT ACCOUNT is a "custody account." According to MUFJ, the stated purpose of the account was to receive custodial services, including but not limited to the safekeeping of securities, receipt and delivery of securities, funds transfer, and corporate action processing. MUFJ also noted that Deltec is the beneficiary of funds coming in to the SUBJECT ACCOUNT, and those funds are to be used for security purchases that will be held in safekeeping (i.e., "custody") until transferred to Deltec. MUFJ noted that upon receipt of funds into the SUBJECT ACCOUNT, the funds are invested according to instructions received from Deltec. The investments are wired back to Deltec based on the settlement date of the investment.

55. MUFJ informed law enforcement in April 2023 that they learned that Deltec appeared to be treating the SUBJECT ACCOUNT in part as a correspondent account,[8] which is not the original purpose established at the time of account creation. Custodial services generally do not include receiving funds from third parties for the benefit of another customer. Therefore, MUFJ conducted a review of the SUBJECT ACCOUNT. During this review, MUFJ noted a high volume of wires that initially went to the BANK 1 correspondent account ending 7694 and then contained additional instructions to forward the money to Axis Digital Limited or GTAL—the same transaction patterns discussed above. MUFJ reported that they found these transactions suspicious because the source of funds was unknown and an economic business purpose could not be determined.

56. Additionally, MUFJ conducted open-source research on the companies originating the suspicious transactions and concluded they appeared to be shell companies. Separately, MUFJ was unable to obtain Know-Your-Customer documentation related to Axis Digital Limited or GTAL from Deltec. By law, banks operating in the United States are required to keep such Know-Your-Customer information regarding their customers. Law enforcement has also not yet been able to identify the registered agents, business locations, or business purposes of Axis Digital Limited and GTAL.

57. MUFJ records revealed 224 wire transfers from June 2022 to the present into the SUBJECT ACCOUNT, totaling approximately $29.5 million, that records clearly show were transferred to either Axis Digital Limited or GTAL.

58. Law enforcement then analyzed the other transfers into the SUBJECT ACCOUNT

[8] A correspondent bank is a financial institution that provides services to other financial institutions, usually in another country. It acts as an intermediary, facilitating wire transfers, accepting deposits and other financial transactions on behalf of another bank.

and identified approximately 253 additional wire transactions totaling approximately $29 million. Although the records do not clearly show the direction further transferring funds to Axis Digital or GTAL, I submit that they were made as part of the same fraud and money laundering scheme described above for several reasons. First, MUFJ has orally confirmed to agents that the Axis Digital Limited and GTAL accounts were the only accounts to which the shell company deposits included "for further credit" instructions, although MUFJ has not yet provided records confirming this fact. Second, these additional incoming wires came from the same accounts and business entities that had also received funds from victims of fraud schemes and that records show had also transferred funds to Axis Digital and GTAL. As discussed above, review of bank records shows that wire transfers from certain banks exceed the character limit and the additional FFC instructions are cut off. In any event, law enforcement was able to attribute to fraudulent activity both 1) wires totaling $29.5 million containing FFC instructions to Axis Digital Limited or GTAL and 2) wires totaling $29 million not containing FFC instructions, but originating from the same account numbers, business entities, and/or business addresses as the others, and confirmed by MUFJ to be directed to Axis Digital Limited and GTAL, for a total of $58,465,480.

G. Identification of Victims and Additional Scam-Associated Entities

59. **EXHIBIT A** lists these entities that transferred money into the SUBJECT ACCOUNT that have been tied to fraudulent schemes. To create this list, law enforcement queried investigative databases, to include IC3, on the entities transferring money into the SUBJECT ACCOUNT with directions to further transfer money to Axis Digital or GTAL. Law enforcement identified approximately 157 victim complaints reflecting approximately 208 wire transactions related to socially engineered wire fraud schemes. The majority of these schemes were pig butchering scams using spoofed cryptocurrency websites, as described above. Law enforcement

also identified approximately ten victims who had fallen prey to tech scams and fake order scams, and found that the proceeds for these scams were being laundered through the same shell companies and accounts, using the same pattern of transferring the funds from the shell account, "for further credit" to the SUBJECT ACCOUNT, and then "FFC" to Axis Digital or GTAL.[9] Attribution factor A in **EXHIBIT A** identifies the 63 entities for which law enforcement identified victims. Additionally, in **EXHIBIT A**, the column titled "Identified Victim Transactions" reflects the number of fraudulent transfers by victims into these entities that law enforcement has been able to identify to date. Entities with victim complaints against them transferred a total of $50.2 million to the SUBJECT ACCOUNT from June 2022 to the present.

60. Law enforcement then interviewed approximately 42 of the 157 potential victims who had submitted complaints to law enforcement. These individuals sent approximately 68 wire transactions to the business entities that subsequently transferred money to the SUBJECT ACCOUNT. In **EXHIBIT A**, the column titled "USSS Interviewed Victims Transactions" reflects the number of transactions transferred to the shell companies by USSS interviewed victims.

61. Through victim interviews and investigative analysis, law enforcement was able to confirm that the entities receiving victim funds and transferring them to the SUBJECT ACCOUNT followed the same patterns identified above in the accounts associated with ZHU and J.W. Representative examples of these financial transactions and methodologies are discussed below.

a. Victim 3 Transfers Traceable to the SUBJECT ACCOUNT

62. On or about May 1, 2023, law enforcement interviewed Victim 3. Victim 3 stated

[9] "Tech scams" relate to scammers posing as tech support such as "Geek Squad" and "MacAfee." These scammers induce victim payments by making them believe they paid for a subscription or required tech services. "Fake order scams" relate to when scammers make victims believe they are receiving proceeds from sales. These "proceeds" are fictitious, and the scammer will induce the victim to wire a portion of these "proceeds" back to the scammer.

they were first contacted around July 2022 through unsolicited text message from an individual who identified herself as "RACHEL." Victim 3 stated that "RACHEL" insisted they move their conversation to Telegram. "RACHEL" then led the conversation to cryptocurrency. Victim 3 stated they knew nothing about cryptocurrency, but "RACHEL" informed them that she would teach them how to invest.

63. According to Victim 3, "RACHEL" eventually promoted a cryptocurrency investment domain named "coinasx.com," (the same domain used by Victim 1, discussed above). Victim 3 visited the URL and downloaded an application associated with the platform onto their mobile device. Victim 3 also stated they would switch to a domain named "asxcoins.com" when the coinasx.com site would go down. Victim 3 was directed to invest in "ASX" from the "ASX" online customer service chat platform and received wire instructions from an "ASX" online customer service representative. Between December 2022 and January 2023, Victim 3 invested approximately $60,000. Included in these investments was a $30,000 wire on January 31, 2023, to Bank of America National Association account ending 6409 in the name of FUYU Commerce LLC.

64. Victim 3 stated that in February 2023, they attempted to withdraw money out of their "ASX" account, which showed purported investment gains. Victim 3 was told by the "ASX" online customer service chat platform that they would need to pay a "management review fee" of $62,000 before any money could be withdrawn. On or around March 6, 2023, Victim 3 wired $62,000 to pay this fee. Victim 3 stated that when they attempted another withdrawal, an "ASX" online customer service representative again informed them they needed to wire an additional $62,000 in order to withdraw the funds. Victim 3 has been unable to recover any of their funds.

65. Analysis of MUFJ records showed that on the day after Victim 3's transfer to

FUYU Commerce LLC on January 31, 2023, the controller of FUYU Commerce LLC wired $100,000 on February 1, 2023 to the SUBJECT ACCOUNT. The wire included the instructions "for further credit to" the SUBEJCT ACCOUNT with additional instructions that these funds be FFC to Axis Digital.

66. A review of California Secretary of State records found that FUYU Commerce was incorporated in California on or about September 1, 2022, with a stated purpose of "General Trading." The listed mailing and principal address for FUYU Commerce was the same address provided for Sea Dragon Trading, discussed above.

67. Analysis of a device belonging to J.W. seized by USSS during a search warrant at J.W.'s residence revealed videos of an unknown individual directing transfers from the FUYU BOA account discussed above, including transfers to the SUBJECT ACCOUNT. For example, I reviewed records for a wire on January 31, 2023, where FUYU Commerce LLC's account at BOA transferred $99,000 through BANK 1 to the SUBJECT ACCOUNT.

68. Law enforcement identified four additional, separate IC3 victim complaints of "pig-butchering" scams where the victims were all directed to wire money to various accounts belonging to FUYU Commerce LLC. Between January 18, 2023 and February 8, 2023, FUYU Commerce LLC wired approximately $1.2 million to the SUBJECT ACCOUNT, as reflected in the column "Total Wires to SUBJECT ACCOUNT" in **EXHIBIT A**. Of these five victim complaints related to FUYU Commerce, USSS agents interviewed 2 victims (including Victim 3 above) and confirmed their losses, as reflected in the column "USSS Interviewed Victims Transactions" in **EXHIBIT A**.

b. Victim 4 Transfers Traceable to the SUBJECT ACCOUNT

69. Law enforcement reviewed approximately nine IC3 complaints related to pig-

butchering scams involving YYJ Consulting Corporation. According to these complaints, from August 26, 2022, through November 4, 2022, these nine victims were directed to send wires to YYJ Consulting Corporation accounts at Bank of America and JPMC totaling $675,000.00.

70. According to records from MUFJ, from September 21, 2022, through October 26, 2022, YYJ Consulting Corporation bank accounts sent $1,330,000 to the SUBJECT ACCOUNT with directions that these funds be further credited to both Axis Digital and GTAL.

71. On May 1, 2023, law enforcement interviewed Victim 4. Victim 4 stated they invested approximately $2 million into three fraudulent cryptocurrency investment platforms at the direction of individuals who gained Victim 4's trust after contacting them on Telegram.

72. Victim 4 stated that to fund their accounts on these investment platforms, they would wire money from their bank account to their accounts on various cryptocurrency exchange platforms. From there, they would send cryptocurrency to their newly created "investment accounts" at fraudulent cryptocurrency investment platforms. Victim 4 reported approximately $1.7 million in losses total, which was a combination of cryptocurrency and wire transfers to various business. Included in the wire transfers is a $190,000 wire on September 26, 2022, to a YYJ Consulting Corporation account at JPMC.

73. On or about September 30, 2022, the YYJ Consulting Corporation account wired $178,000 to the SUBJECT ACCOUNT. The wire included the instructions "for further credit to" the SUBJECT ACCOUNT and also included the additional instructions for "FFC" GTAL.

74. Victim 4 stated they were unable to withdraw any of the money that they had invested into the three fraudulent cryptocurrency investment platforms.

c. Victim 5 Transfers Traceable to the SUBJECT ACCOUNT

75. On or around April 28, 2023, USSS interviewed Victim 5. Victim 5 informed

agents they were a victim of a cryptocurrency investment scam whereby they invested an approximate total of $800,000 via a combination of traditional wire transfers, cryptocurrency transactions, and CashApp. Victim 5 reported that they believed they were investing in a cryptocurrency website, which was later determined to be fraudulent.

76. Victim 5 stated on or around December 13, 2022, they received a random text message on their iPhone from an unfamiliar phone number. Victim 5 reported that the person texting claimed to be an Asian female named Anna Lee (hereafter, "LEE"). Victim 5 stated that they believed they were building a relationship and LEE shared personal stories about her life. Victim 5 then stated that LEE requested their conversations move over to Telegram and began talking about cryptocurrency. Victim 5 stated that LEE eventually sent them a link to access the fraudulent cryptocurrency platform and had them create cryptocurrency accounts. In March 2022, Victim 5 began investing and stated that they recalled seeing investment gains in their account. Victim 5 also noted that at one point they withdrew some of the money from their investment account, which increased their confidence in the platform and induced them to invest more.

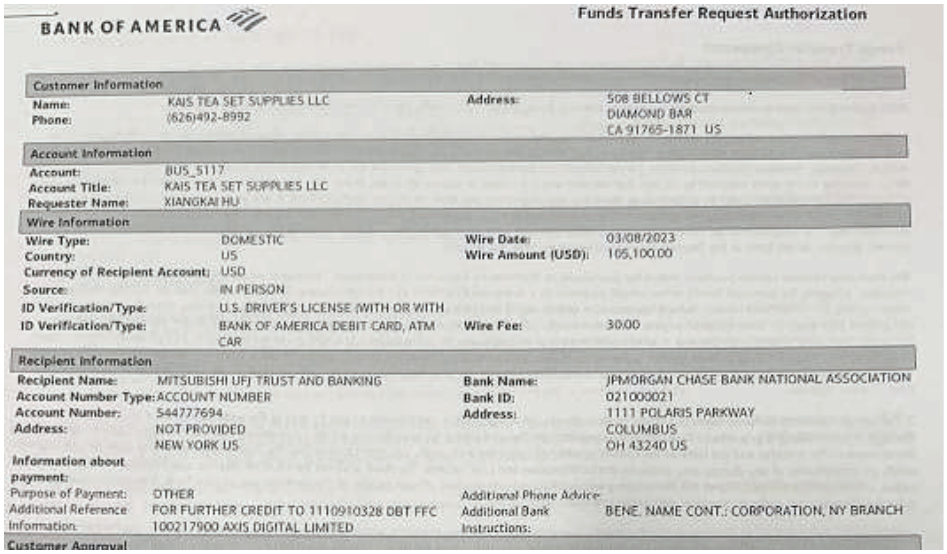
77. Victim 5 then began speaking with the platform administrator who encouraged additional investment. Victim 5 then stated they tried to withdraw their investments, but the platform administrator said that Victim 5 owed roughly $430,000 in taxes and claimed that they could not withdraw their funds until they paid taxes on the balance. In addition to investments transferred from cryptocurrency accounts, Victim 5 stated that they had "invested" roughly $675,000 via wire transfers.

78. One of these wires was a $50,000 transfer on March 9, 2023, to a company named Kais Tea Set Supplies LLC using JPMC account ending 8539. MUFJ records show that on March 10, 2023, Kais Tea Set Supplies LLC JPMC account ending 8539 wired $139,800 to the

SUBJECT ACCOUNT. The wire included the instructions "for further credit to" the SUBJECT ACCOUNT and also included the additional instructions to "FFC" Axis Digital Limited.

79. Additionally, law enforcement recovered from J.W.'s iPhone a wire form, depicted in **FIGURE 4**, reflecting a transfer from Kais Tea Set Supplies LLC BOA account ending 1871. As noted in **FIGURE 4**, the controller of Kais Tea Set Supplies LLC sent a wire for $105,100 on March 8, 2023, to the BANK 1 correspondent account 7694 at MUFJ. The wire directed the money be further credited to the SUBJECT ACCOUNT, followed by an additional transfer to Axis Digital Limited. MUFJ bank records confirm the SUBJECT ACCOUNT received this incoming wire.

FIGURE 4



BANK OF AMERICA

Funds Transfer Request Authorization

Customer Information

Name:	KAIS TEA SET SUPPLIES LLC	Address:	508 BELLOWS CT DIAMOND BAR CA 91765-1871 US
Phone:	(626)492-8992		

Account Information

Account:	BUS_5117
Account Title:	KAIS TEA SET SUPPLIES LLC
Requester Name:	XIANGKAI HU

Wire Information

Wire Type:	DOMESTIC	Wire Date:	03/08/2023
Country:	US	Wire Amount (USD):	105,100.00
Currency of Recipient Account:	USD		
Source:	IN PERSON		
ID Verification/Type:	U.S. DRIVER'S LICENSE (WITH OR WITH		
ID Verification/Type:	BANK OF AMERICA DEBIT CARD, ATM CAR	Wire Fee:	30.00

Recipient Information

Recipient Name:	MITSUBISHI UFJ TRUST AND BANKING	Bank Name:	JPMORGAN CHASE BANK NATIONAL ASSOCIATION
Account Number Type:	ACCOUNT NUMBER	Bank ID:	021000021
Account Number:	544777694	Address:	1111 POLARIS PARKWAY COLUMBUS OH 43240 US
Address:	NOT PROVIDED NEW YORK US		
Information about payment:			
Purpose of Payment:	OTHER	Additional Phone Advice:	
Additional Reference Information:	FOR FURTHER CREDIT TO 1110910328 DBT FFC 100217900 AXIS DIGITAL LIMITED	Additional Bank Instructions:	BENE. NAME CONT.: CORPORATION, NY BRANCH

Customer Approval

H. Total Victim Losses Include Other Wire Addresses and Cryptocurrency

80. Total Victim losses from these types of scams are usually not limited to one transaction. As discussed above, Victims 1 through 5 all sustained additional losses from the same scam. These additional losses are also in form of cryptocurrency (e.g. Victim 4 and Victim 5). As discussed above, approximately $13.4 million of reported victim proceeds were traced to the 74 Shell Companies and flowed through the SUBJECT ACCOUNT. However, total proceeds from victim losses, to include wire transfers to other entities and cryptocurrency transfers, are far greater

than just what was sent to the 74 Shell Companies as shown in EXHIBIT A.

81. In another example, Victim 6, who was interviewed by the USSS on or around March 31, 2023, was promoted spoofed cryptocurrency websites by scammers and reports to have lost approximately $14.5 million from May 2022 through March 2023. However, USSS agents have reviewed bank statements and wire forms provided by Victim 6 only supporting $8 million in losses, of which approximately $5.7 million were losses incurred from sending cryptocurrency to the spoofed cryptocurrency platform. USSS reviewed bank statements and wire forms provided by Victim 6 noting they wired approximately $5.7 million to their Coinbase and Gemini accounts. Victims 6 informed law enforcement these funds were then converted into cryptocurrency (e.g. BTC, USDT and USDC) and then transferred to the spoofed cryptocurrency website.

82. Victim 6 also noted as part of the investment scheme, they were provided wire addresses to make investments onto the spoofed cryptocurrency platform. Victim 6 provided wire forms and bank statements showing they has wired approximately $2.3 million to various international and domestic bank accounts. Victim 6 noted they obtained these wire instructions from the spoofed cryptocurrency platform. Of the approximate $2.3 million in bank wires, Victim 6 transferred $200,000 to YHM Trading LLC on February 14, 2023 and $80,000 to KQQ Trading LLC on March 15, 2023. Victim 6 noted each attempt to withdrawal their funds has been unsuccessful and has not be able to recover their investments.

83. Therefore, similar to Victims 1-5, Victim 6 sustained significantly more losses than just what was sent to YHM Trading LLC and KQQ Trading LLC, Shell Companies listed in EXHIBIT A. Based on my training and experience with "pig butchering" cases, scammers provide victims with numerous wire addresses and also encourage victims to invest using cryptocurrency.

I. Common Patterns Among Shell Companies and Accounts

84. The means by which the shell companies and their remitter accounts were established reflect a common scheme designed to disguise the control, ownership, and purpose of the accounts and the money passing through them. For example, J.W. directed ZHU and other money couriers to incorporate business for the sole purpose of opening business accounts. ZHU's Sea Dragon Remodel business was incorporated on October 17, 2022. ZHU and J.W. then used the Sea Dragon Remodel incorporation documents to open BOA account 9529 and JMPC account 5581 on October 21, 2022. Those bank accounts began receiving victim funds shortly thereafter.

85. Law enforcement also observed a pattern in which the same shell companies were used to open numerous bank accounts. For example, bank records reveal that ZHU, at the direction of J.W., opened the following accounts listed in **FIGURE 5**. As illustrated below, our investigation has shown that ZHU and J.W. opened additional accounts as their other accounts were restricted or closed due to fraud. As shown below, ZHU and J.W. opened Sea Dragon Trading and Sea Dragon Remodel shell companies at BOA, JPMC, Wells Fargo, and East West Bank (though not all of these accounts transferred money to the SUBJECT ACCOUNT). I know that is it not normal business practice to operate so many accounts using the same business name.

FIGURE 5

Date	Bank Account	Entity	Status
9/9/2022	BOA account 3881	Sea Dragon Trading	Opened
9/9/2022	JPMC account 3886	Sea Dragon Trading	Opened
10/19/2022	BOA account 3881	Sea Dragon Trading	RESTRICTED due to Fraud
10/20/2022	BOA account 9529	Sea Dragon Remodel	Opened
10/21/2022	JPMC account 5581	Sea Dragon Remodel	Opened
10/27/2022	EWB account 4241	Sea Dragon Trading	Opened
10/28/2022	EWB account 4340	Sea Dragon Remodel	Opened
11/1/2022	WF account 6778	Sea Dragon Remodel	Opened
11/14/2022	JPMC account 3886	Sea Dragon Trading	RESTRICTED due to Fraud
11/14/2022	JPMC account 5581	Sea Dragon Remodel	RESTRICTED due to Fraud
12/8/2022	BOA account 9529	Sea Dragon Remodel	RESTRICTED due to Fraud
12/28/2022	BOA account 3881	Sea Dragon Trading	CLOSED for Fraud
1/3/2023	WF account 6778	Sea Dragon Remodel	CLOSED for Fraud

86. The other shell companies listed in **EXHIBIT A** reflect a similar pattern. **FIGURE 6** contains a representative sample of shell companies with numerous bank accounts. Based on review of the MUFJ records, at least 34 of the 75 shell companies had multiple bank accounts that transferred funds to the SUBJECT ACCOUNT.

FIGURE 6

Shell Company	Number of Bank Accounts
CMD EXPORT AND IMPORT	3
H & C TRADING LLC	3
KAIS TEA SET SUPPLIES LLC	3
QAG TRADING LLC	3
SHANGHAI FOOD & GROCERIES LLC	3
SKJ TRADING LLC	3
ASPECT TRADING LLC	2
BAISHUNXING TRADING INC	2
BFC REMODEL LLC	2
BFC SUPPLY LLC	2
BITOO CONSULTING INC	2
CZY REMODEL INC	2

87. Incorporation records for the other shell companies listed in **EXHIBIT A** reveal that most of the business entities and accounts transferring money into the SUBJECT ACCOUNT were not pre-established businesses or accounts with historical activity, but were instead created shortly before receiving victim payments. Based on my experience, I know that this is a common money laundering technique. **FIGURE 7** below contains a representative sample of dates that companies were incorporated and the dates when the first identified victim transactions were reported associated with those companies.

FIGURE 7

Shell Company	Incorporation Date	First Reported Victim Transaction
YYJ CONSULTING CORPORATION	8/25/2022	8/26/2022
GUDI TRADING INC	9/12/2022	9/16/2022
VANTOP TRADING	7/22/2022	8/2/2022
QAG TRADING LLC	9/7/2022	9/22/2022
KAIS TEA SET SUPPLIES LLC	2/7/2023	3/1/2023
XIEYUNZHU TRADING INC	11/23/2022	12/16/2022

88. Additionally, investigative efforts have shown that numerous shell companies are incorporated using a derivative of the same name. For example, ZHU incorporated both Sea Dragon Remodel Inc. and Sea Dragon Trading LLC. J.W. also oversaw the individual who created Mingxing Trading LLC, Mingxing Remodel LLC, and MINGXINGTRANDING, Inc. Law enforcement has also learned that J.W. directed individuals, including ZHU, to incorporate businesses that relate to the name of the account holders. For example, Sea Dragon is the English translation for Hailong (ZHU's first name), Mingxing is the name of the individual who registered the entity, and BFC Supply refers to the initials of the individual who registered that company. Many of the other shell companies listed in **EXHIBIT A** appear to follow a similar pattern of using their registrants' initials and names.

89. Companies with similar names were also incorporated using the same address, indicating control by the same individual. **FIGURE 8** below contains a representative sample of shell companies with similar names and the same address. Based on my training and experience, I know this practice of creating multiple variations of the same business name registered at the same addresses to be highly unusual and is indicative of an intent to use the business as a shell company to engage in fraud activity, money laundering, or both.

FIGURE 8

Shell Company A	Shell Company B	Shell Company Address
YHM TRADING LLC	YHM SUPPLY LLC	401 S CANYON BLVD APT C MONROVIA CA 91016
BFC REMODEL LLC	BFC SUPPLY LLC	408 W GLENDON WAY SAN GABRIEL CA 91776-4086 US
SMX BEAUTY INC	SMX TRAVEL INC	132 E EMERSON AVEAPT C MONTEREY PARK CA 91755-
YZX LUXURY LLC	YZX TRENDING LLC	1036 S GARFIELDAVE APT B ALHAMBRA CA 91801-4773 US
YXJ TRADING CORPORATION	YYJ CONSULTING CORPORATION	212 S CHANDLER AVE APT A MONTEREY PARK CA 91754-
LJS REMODELING LLC	LJS SUPPLY LLC	1441 PASO REAL AVESPC 254 ROWLAND HGHTS CA 91748-

90. Based on review of MUFJ bank records, there are numerous shell companies with the same address, even when they do not share similar names. In numerous cases, an address was used across many different shell companies. Attribution factor "B" in **EXHIBIT A** identifies the shell companies that share addresses with other shell companies, while **FIGURE 9** below provides a representative sample of shell companies sharing the same address. In addition, internet searches for the addresses indicate that they appear to be residential properties, not business addresses.

FIGURE 9

Shell Company	Shared Shell Company Address
8898 MANAGEMENT INC	13518 NORTHERN BLVD FLUSHING NY 11354-4007
TAHNJIN INC.	
TSYSON INC	
WYNNING 998 INC	
XIEYUNZHU TRADING INC	1036 S GARFIELDAVE APT B ALHAMBRA CA 91801-4773 US
YZX LUXURY LLC	
YZX TRENDING LLC	
MINGXINGTRANDING, INC.	2220 FALLING LEAF AVE ROSEMEAD CA 91770-3563 US
GOOD LUCK TRADING LLC	
MINGXING TRADING LLC	
CREATIVE HOMEGOODS LLC	823 W HUNTINGTON DR APT B ARCADIA CA 91007-6638 US
LEADING CONSTRUCTION LLC	
LQH SUPPLY LLC	
SUNRISE SUPPLY LLC	

91. Many of the shell companies have both identified victims and common addresses, which is represented as A & B. There are 11 shell companies for which law enforcement did not identify a victim, but which share an address with a shell company that did receive direct victim proceeds. **FIGURE 10** depicts these 11 entities and the company with which they share an address. Law enforcement was also able to confirm through open-source incorporation searches that 10 of these 11 shell companies also shared a registered owner with a company with at least one identified victim.[10] Additionally, as shown in **FIGURE 10**, there are commonalities between the shell companies that share an address. For example, registration documents show that Yubo Miao is both the name of an entity and the name of the registered owner for MYB Supply LLC. Therefore, it is likely that "MYB" in MYB Supply are initials related to the name Yubo Miao.

FIGURE 10

Attribution B Shell Company	Shared Address - with an Attribution A Shell Co.	Shared Registered Owner - with an Attribution A Shell Co.
8898 MANAGEMENT INC	WYNNING 998 INC	WYNNING 998 INC
TAHNJIN INC.	WYNNING 998 INC	WYNNING 998 INC
TSYSON INC	WYNNING 998 INC	WYNNING 998 INC
Wynne Win Inc	WYNNING 998 INC	WYNNING 998 INC
PBB International Consulting Corp	SKJ TRADING LLC	SKJ TRADING LLC
MINGXINGTRANDING, INC.	GOOD LUCK TRADING LLC	MINGXING TRADING LLC
	MINGXING TRADING LLC	
QAG Trading Inc	QAG TRADING LLC	QAG TRADING LLC
ZHONGYONG TRADE INC	CZY REMODEL INC	CZY REMODEL INC
YM HOUSE REMODELING COMPANY	MYB SUPPLY LLC	MYB SUPPLY LLC
Yubo Miao	MYB SUPPLY LLC	MYB SUPPLY LLC
YONGDI TRADING CO., LIMITED	ORDECO TRADING CO LIMITED	Unknown

92. I have learned through this investigation that the account owners and controllers

[10] The exception, as shown in **FIGURE 10**, is Yongdi Trading Co., Limited. Yongdi Trading Co., Limited is a foreign-based entity and registered owner searches were inconclusive.

will use the same addresses to ensure they receive the account balance cashier's check upon the account being closed. Law enforcement seized J.W.'s iPhone and recovered numerous video recordings of J.W. calling banks to inquire about frozen accounts. During the calls, the bank informed J.W. (who was posing as ZHU and the other couriers he managed who had opened the accounts) that the accounts had been frozen due to suspicious activity and would be closed. J.W. did not appear concerned about the account status but rather asked questions about the balance and when the closing cashier's check would be mailed. Law enforcement recovered at least one such check in J.W.'s vehicle.

93. Yet, while some of the *businesses* were registered using the same address, investigation revealed that the bank *accounts* for these entities used addresses that differed from the entities' addresses. For example, for the Sea Dragon Remodel JPMC account ending in 5581 lists a business address identical to that used to register Sea Dragon Remodel, but the Sea Dragon Remodel BOA account ending 9529 uses a different address. Based on my training and experience, I know it is not a normal practice for legitimate businesses to list different business addresses in different places; instead, this is a tactic used to conceal the ownership and nature of a business. Similarly, FUYU Commerce LLC lists a wire address in San Gabriel, CA but the registration documents list an address in Alhambra, CA.

J. Finally, the patterns of transactions into these accounts indicated these entities and accounts were not being used for legitimate business purposes. As discussed above, transfers into the Sea Dragon accounts were typically round number amounts. This pattern was also present in other shell company accounts transmitting money on to the SUBJECT ACCOUNT. This is unusual given the purported business purposes of these entities. For example, the California incorporation documents for LJS Remodeling LLC indicate that

the stated purpose of the business is "wholesale." This is a vague description (similar to "general trading"), but based on my training and experience, I would expect account transfer values for such a business to reflect off-sets or variation that would be common in legitimate business transactions due to factors like sales tax, distribution fees, and the varying costs of materials and services. But MUFJ bank records reveal LJS Remodeling LLC sent the SUBJECT ACCOUNT four wires totaling $259,000 from January 10, 2023, to January 19, 2013 (two of which forwarded on to Axis Digital). It is not normal business practice for a "wholesale" company to send four round number wires in such a short period of time. On the other hand, we consistently see victims making "investments" in round figures.Transaction Structure Designed to Conceal the Source, Ownership, and Control of Funds

94. Based on my training and experience, I know that the structure of the transactions from the shell companies to the Axis Digital and GTAL accounts through the use of a series of "for further credit" instructions does not reflect standard business practices. Instead, I believe this transaction structure was designed to conceal the source, ownership, and control of funds, as well as to facilitate the transfer of those funds overseas without the standard scrutiny. Under normal circumstances, a customer seeking to transfer funds would simply identify the intended ultimate beneficiary. For example, the Sea Dragon Trading account could directly transfer funds to the Axis Digital Account at Deltec Bank in the Bahamas. This would give the transferring banks the opportunity to identify and, if necessary, vet both the transferor and the intended recipient. Additionally, when the intended recipient is overseas, a transferor would be required to state that the wire was international, again exposing the transfer to potential additional scrutiny and reporting requirements.

95. Moreover, the use of BANK 1's correspondent account and Deltec's "custody" account further concealed the source, ownership, control, and intended international destination of the funds. Under normal circumstances, transfers from one account holder to another would only pass through a bank's correspondent account based on the bank's own internal instructions; in other words, customers typically do not specify the specific routes their funds should take. Moreover, the use of the custody account reduced transparency by routing the funds through a large central account where they became "mixed" with Deltec's own funds. Only Deltec—an overseas bank known not to be cooperative with foreign law enforcement requests—has records detailing the breakdowns of funds within its own accounts. As a result, it became more difficult to track the proceeds of the fraud once they entered the SUBJECT ACCOUNT.

CONCLUSION

96. Based on my knowledge, training, and experience, and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the SUBJECT ACCOUNT contains the proceeds of a wire fraud scheme performed in violation of Title 18, United States Code, Section 1343 and accordingly are subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), and that same code section combined with Title 28, United States Code, Section 2461(c). There is further probable cause to believe that a greater amount of funds constitute property involved in money laundering transactions and accordingly are subject to forfeiture and seizure pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). Therefore, I respectfully request that a warrant be issued authorizing the seizure of funds up to the amount of $58,465,480 held or stored at Mitsubishi UFJ Trust and Banking account 1110910328 in the name of Deltec Bank and Trust.

Christopher Saunders

Christopher Saunders
Special Agent
United States Secret Service

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 12th day of June 2023.

Lindsey Vaala Digitally signed by Lindsey Vaala Date: 2023.06.12 11:02:06 -04'00'

The Honorable Lindsey R. Vaala
United States Magistrate Judge