United States District Court

CENTRAL **DISTRICT OF** **CALIFORNIA**

In the Matter of the Seizure of
(Address or Brief description of property or premises to be seized)

Any and all funds, cryptocurrency and/or other negotiable instruments stored in the account held by Binance associated with User Identification Number [redacted] held in the name of [redacted]

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

CASE NUMBER: 2:22 MJ-04906

FILED
CLERK, U.S. DISTRICT COURT
12/15/2022
CENTRAL DISTRICT OF CALIFORNIA
BY: ib DEPUTY

I, [redacted] **, being duly sworn depose and say:**

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that

in the CENTRAL **District of** CALIFORNIA
there is now concealed a certain person or property, namely **(describe the person or property to be seized)**

See Attachment A

which is **(state one or more bases for seizure under United States Code)**

subject to seizure and forfeiture under 18 U.S.C. §§ 981(a)(1)(A) & (C) and (b)(2), 982(b), 28 U.S.C. § 2461(c), 18 U.S.C. § 982(a)(7), and (b)(1) and 21 U.S.C. §§ 853(e) and (f).

concerning a violation of Title 18 **United States Code, Section(s)** 1343, 1349, and 1956

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

Continued on the attached sheet and made a part hereof. X **Yes** __ **No**

[redacted]

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

Sworn before me in accordance with requirements of Fed. R. Crim. P. 4.1 by telephone

12/15/2022
Date

Los Angeles, California
City and State

Hon. Alexander F. MacKinnon, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AUSA Dan G. Boyle; jw

ATTACHMENT A

LIST OF ITEMS TO BE SEIZED

1. Any and all funds, cryptocurrency and/or other negotiable instruments held in the following Binance account associated with the following User ID and Registered Email:

User ID	Name	Email Address
[redacted]	[redacted]	[redacted]

The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each account to cryptocurrency addresses controlled by the United States.

AFFIDAVIT

I, Special Agent [redacted] (Affiant), Federal Bureau of Investigation, having been duly sworn, declare and state as follows:

INTRODUCTION

1. [redacted].

2. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not set forth all of my knowledge about this matter. All dates are on or about the date specified. All amounts are approximate.

PURPOSE OF AFFIDAVIT

3. I make this Affidavit in support of an application for a warrant to seize any and all assets (the "**SUBJECT FUNDS**") stored in the following account held by Binance:

a. User identification number [redacted] held in the name of [redacted] ("[redacted] registered on [redacted], from [redacted] (the "**Subject Account**").

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that unknown subjects have violated Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud) and laundered the proceeds of that activity in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) (money laundering and conspiracy to commit money laundering). There is also probable cause to believe that the **Subject Account** received the proceeds of the wire fraud scheme described below and that the **SUBJECT FUNDS** are subject to seizure pursuant to Title 18, United States Code, Section 981(b)(2) and (3) and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), and 28 U.S.C. § 2461(c). Moreover, as indicated below, there is probable cause to believe that the remainder of the **SUBJECT FUNDS** are subject to seizure and forfeiture as involved in money laundering transactions, pursuant to Title 18, United States Code, Section 981(a)(1)(A). In addition, the **SUBJECT FUNDS** are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(a)(7) and (b)(1), and 21 U.S.C. § 853(f), because there is probable cause to believe that the **SUBJECT FUNDS** would, in the event of conviction on the alleged underlying wire fraud offenses, be subject to criminal

forfeiture, and an order under 21 U.S.C. § 853(e)(providing for restraining orders and injunctions) would not be sufficient to assure the availability of the property for forfeiture.

5. Accordingly, I request that the Court authorize the attached warrant for seizure of the assets described herein.

BACKGROUND ON CRYPTOCURRENCY AND VIRTUAL CURRENCY EXCHANGES

6. Virtual currencies, also known as cryptocurrency, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin ("BTC") is the most well-known virtual currency in use.

7. Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

8. The identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), but analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

9. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. A user of virtual currency can utilize

multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

10. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

11. Many virtual currencies publicly record all of their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

12. USDT (also known as Tether) is a cryptocurrency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is equivalent to approximately one U.S. dollar, making it what is known as a "stablecoin." USDT is issued by Tether Ltd., a company headquartered in Hong Kong. USDT is hosted on the Ethereum and Tron blockchains, among others.

13. Ethereum ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track

the movement of ETH.

FACTS SUPPORTING PROBABLE CAUSE

THE SCHEME

14. The FBI Phoenix Division is investigating an investment fraud scam, commonly referred to as "Pig Butchering," perpetrated on victims throughout the United States, including in the Central District of California. According to the Global Anti-Scam Organization, a nonprofit aiming to raise awareness and provide tools to combat cybercrime, Pig Butchering originated in China in 2019.[1] The scheme often begins when a scammer sends a victim a seemingly innocuous and misdialed text or WhatsApp message. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

15. The victims in Pig Butchering schemes are referred to as "pigs" by the scammers because the scammers will use elaborate storylines to "fatten up" victims into believing they are in a romantic or otherwise close personal relationship. Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme. The investment schemes have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy.

[1] Based upon my training and experience, and conversations with other law enforcement personnel, I believe that the locus of Pig Butchering activity moved from China after the country banned cryptocurrency, to nearby locations in Southeast Asia. Based upon the Know Your Customer ("KYC") information provided to Binance, the **Subject Account** was registered from a country which I know that Pig Butchering Schemes originate from (Thailand).

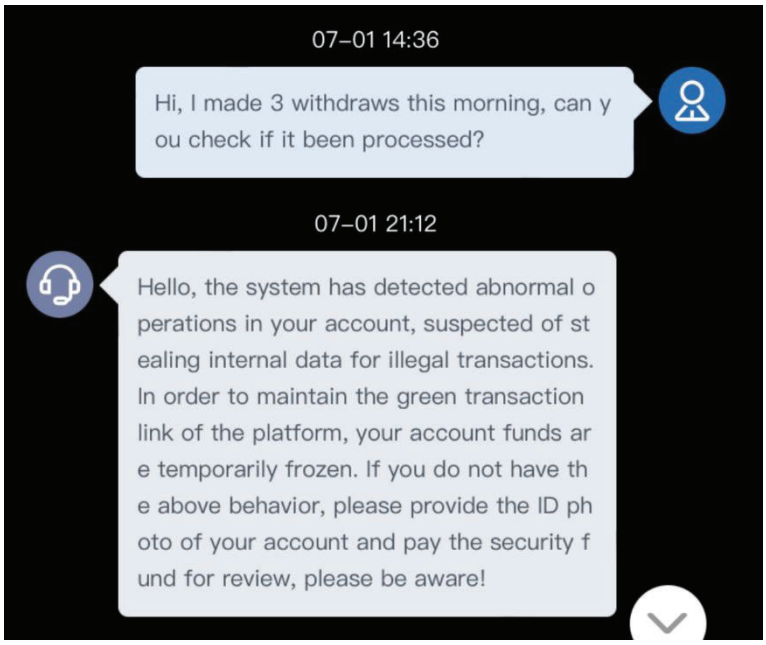
This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns.

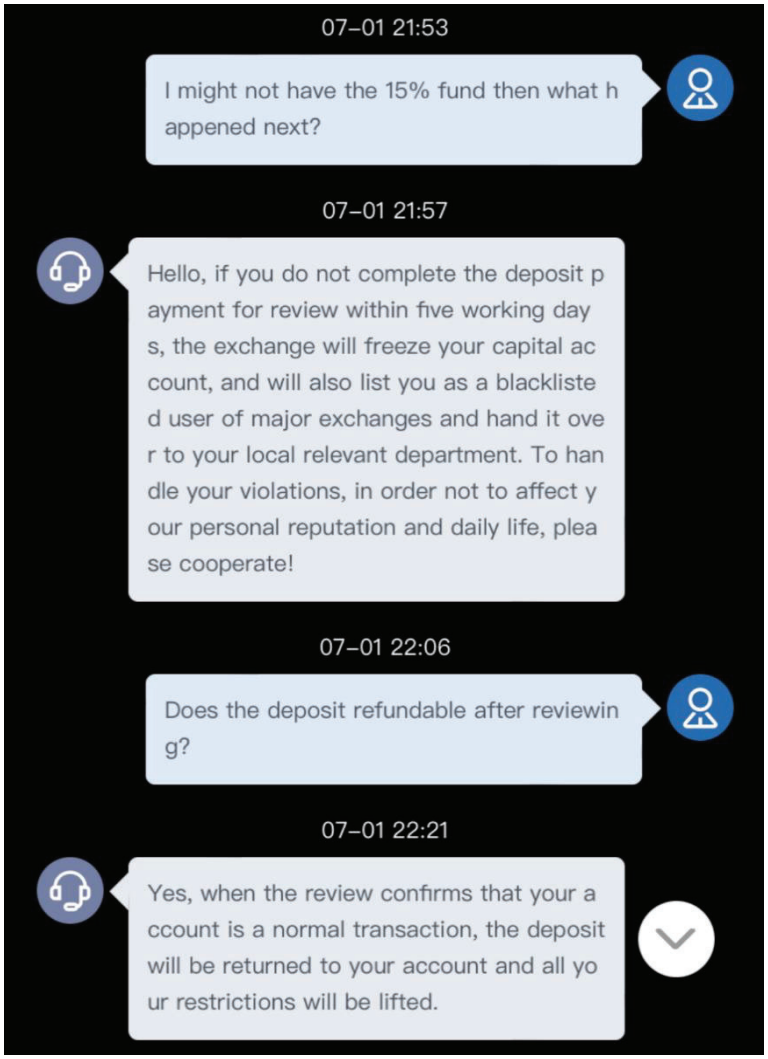
16. The investment platforms are a ruse, and the funds contributed are routed directly to a cryptocurrency address the scammers control. When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses or even required to pay "taxes" in order to release their funds. The "tax" payments are an attempt by the scammers to elicit even more money out of the victims. Eventually, most victims are completely locked out of their accounts and lose all of their funds.

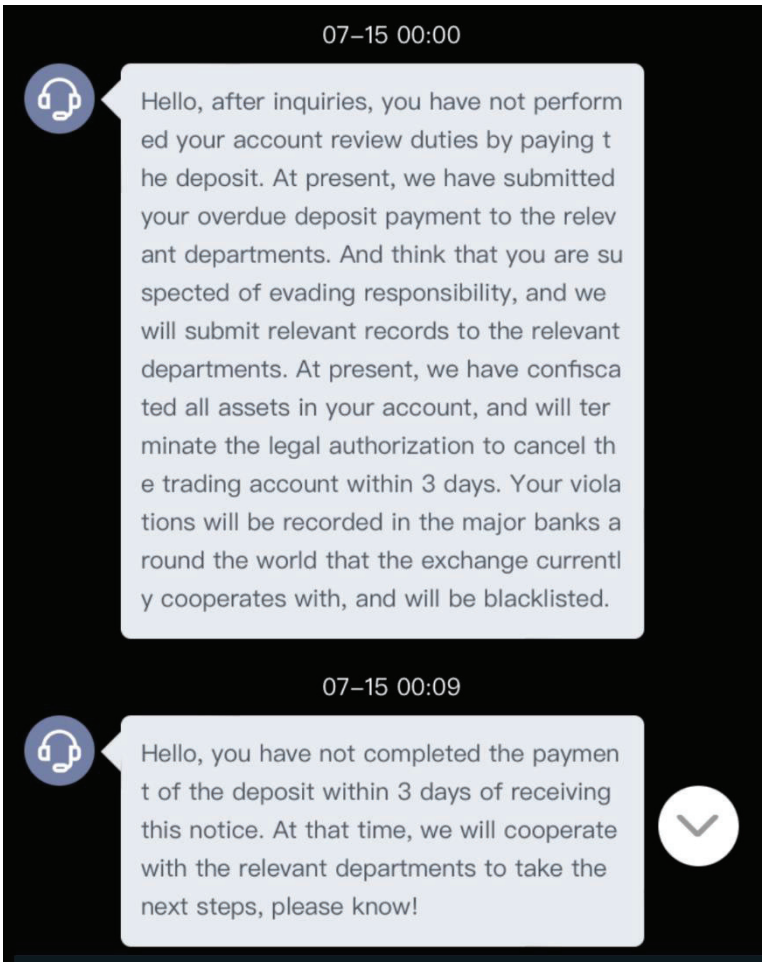
17. In this case, the FBI Phoenix Division has identified at least 69 victims with an estimated loss of at least $33.9 million related to these various fraudulent investment platforms. The fraudulent investment platforms are sometimes offshoots of legitimate platforms. Some of the domain name iterations identified are as follows: www.deribit-e.com; www.deribit-x.com; www.deribit-exchange.net; www.deribitexin.site; www.mcus.me; www.mgcckjs.com; www.toptankapp.com; and www.penzolead.com. As set out below, the FBI has identified at least 10 victims of this scheme whose funds were directed to the **Subject Account**.

18. The FBI is aware of several different domain names that were utilized in the scam, below is one example of a website:

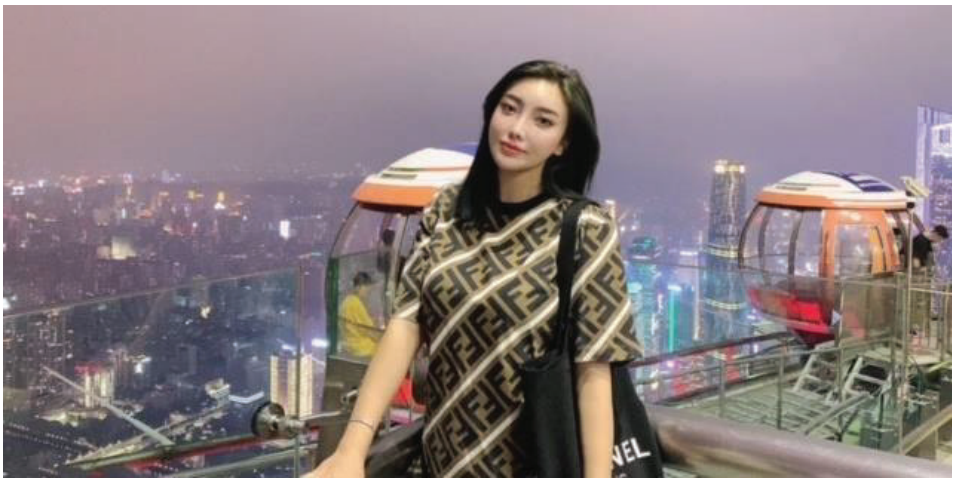
19. Many of these victims did not realize they were part of a scam until they attempted to withdraw some, or all, of their money. Some victims received non-sensical excuses when attempting to withdraw their funds:


07-01 14:36
Hi, I made 3 withdraws this morning, can y ou check if it been processed?
07-01 21:12
Hello, the system has detected abnormal o perations in your account, suspected of st ealing internal data for illegal transactions. In order to maintain the green transaction link of the platform, your account funds ar e temporarily frozen. If you do not have th e above behavior, please provide the ID ph oto of your account and pay the security f und for review, please be aware!


07-01 21:53
I might not have the 15% fund then what h appened next?
07-01 21:57
Hello, if you do not complete the deposit p ayment for review within five working day s, the exchange will freeze your capital ac count, and will also list you as a blackliste d user of major exchanges and hand it ove r to your local relevant department. To han dle your violations, in order not to affect y our personal reputation and daily life, plea se cooperate!
07-01 22:06
Does the deposit refundable after reviewin g?
07-01 22:21
Yes, when the review confirms that your a ccount is a normal transaction, the deposit will be returned to your account and all yo ur restrictions will be lifted.



20. Some victims received pictures purportedly of the individuals that they were in contact with:



Victims and Tracing of Victim Funds to the Subject Account

21. The FBI Phoenix Division have interviewed multiple victims and FBI Phoenix Division Forensic Accountants have traced some of these victims' cryptocurrency from the initial wallet addresses to the **Subject Account**.[2]

Fraudulent Investment Platform MGCCKJ-FX

Victim J.Z.

22. J.Z. was approached on Facebook by an unknown female YUCHAN WANG, aka JENNY ("JENNY"). After a short conversation, and finding out J.Z. is retired, JENNY asked to continue their conversations on WhatsApp. JENNY presented herself as very successful, concentrating in real estate and financial investments. She claimed to have a degree from the business school at the University of Pennsylvania.

[2] This Affidavit does not include all of the cryptocurrency and blockchain analysis performed throughout this investigation, but rather focuses on the tracing of specific funds from victims into the **Subject Account** in order to demonstrate the concerted effort to launder and obfuscate the flow of funds into the **Subject Account**. Cryptocurrency addresses are truncated throughout this Affidavit.

23. JENNY claimed to be an expert in gold spot trading. JENNY introduced the MT-5 trading platform to J.Z. through MGCCKJ-FX, which she represented was a reputable company from Hong Kong. JENNY indicated to J.Z that her best friend, "QI" was the CFO of the company. JENNY claimed to have $3 million in her account, and sent J.Z. several screen shots of her trading with apparent large profits. JENNY convinced J.Z. to open an account with a minimal starting balance. J.Z. then traded under the guidance of JENNY. JENNY then convinced J.Z. to add more funds to his account to cover for the fluctuation in the market for gold prices. JENNY told J.Z. he could have financial freedom if he deposited more funds. MGCCKJ-FX also ran a "promotion" to encourage account holders to deposit more money by stating if your account reached $1 million, the reward from the platform would be $199,999 plus 60% discount on trading fees.

24. By early March 2022, J.Z. had deposited $1.1 million and with his apparent trading gains, was up to $2.4 million. JENNY continued to pressure J.Z. to deposit more money, setting a "goal" for him of $6 million. J.Z. refused to add more funds as he did not want to touch his retirement accounts. JENNY responded to this by guiding J.Z. to make very aggressive trades. The result was the apparent loss of the entire $2.4 million. JENNY apologized to J.Z. for the loss and told him if he could come up with $300,000, she would loan him $650,000 to make up for his losses. J.Z. then added additional funds, including an additional $100,000 from his retirement account. After several trades, J.Z.'s account was apparently back up to $2.8 million. After refusing to add more funds to his account, JENNY told J.Z. she wanted him to pay back the $650,000 she loaned him. J.Z. made a withdrawal request from MGCCKJ-FX, but the withdrawal request was turned down,

purportedly because the original loan from JENNY was now considered possible money laundering. The platform requested evidence of the source of the $650,000 loan. JENNY refused to provide this information to the platform as it would expose her financial information.

25. J.Z.'s account was frozen by the platform and MGCCKJ-FX stated J.Z. needed to pay a verification fee of 16.5% of his account balance, or approximately $466,000 to unfreeze his account. J.Z. made this payment out of his retirement account as he was afraid of losing access to his account. After this, J.Z. was again required to pay an additional 7% of his account balance, or approximately $230,000, for "final" verification. MGCCKJ-FX representatives told J.Z. he could withdraw all of his account funds after the fees were paid. If not, then MGCCKJ-FZ would again freeze his account. JENNY provided a screen shot to J.Z. with a guarantee from her best friend, QI, purportedly CFO of MGCCKJ-FX, that J.Z. would be able to withdraw all of his money once final verification is made. J.Z. then paid the final verification fee.

26. Shortly thereafter, J.Z. attempted to withdraw $50,000 from his account. MGCCKJ-FX told him the withdrawal could not be made because of blockchain congestion and he couldn't make the withdrawal unless he deposited $99,999 to be a VIP member of the platform. J.Z. made the additional deposit. J.Z. was then told his $50,000 withdrawal was successful but he never received the funds.

27. J.Z. attempted to contact the platform but received no further communication from anyone at MGCCKJ-FX. JENNY blocked J.Z. from her social media accounts and never talked to him again. J.Z. lost his entire investment of approximately $2.36 million.

Tracing of Victim J.Z.'s Funds to the Subject Account

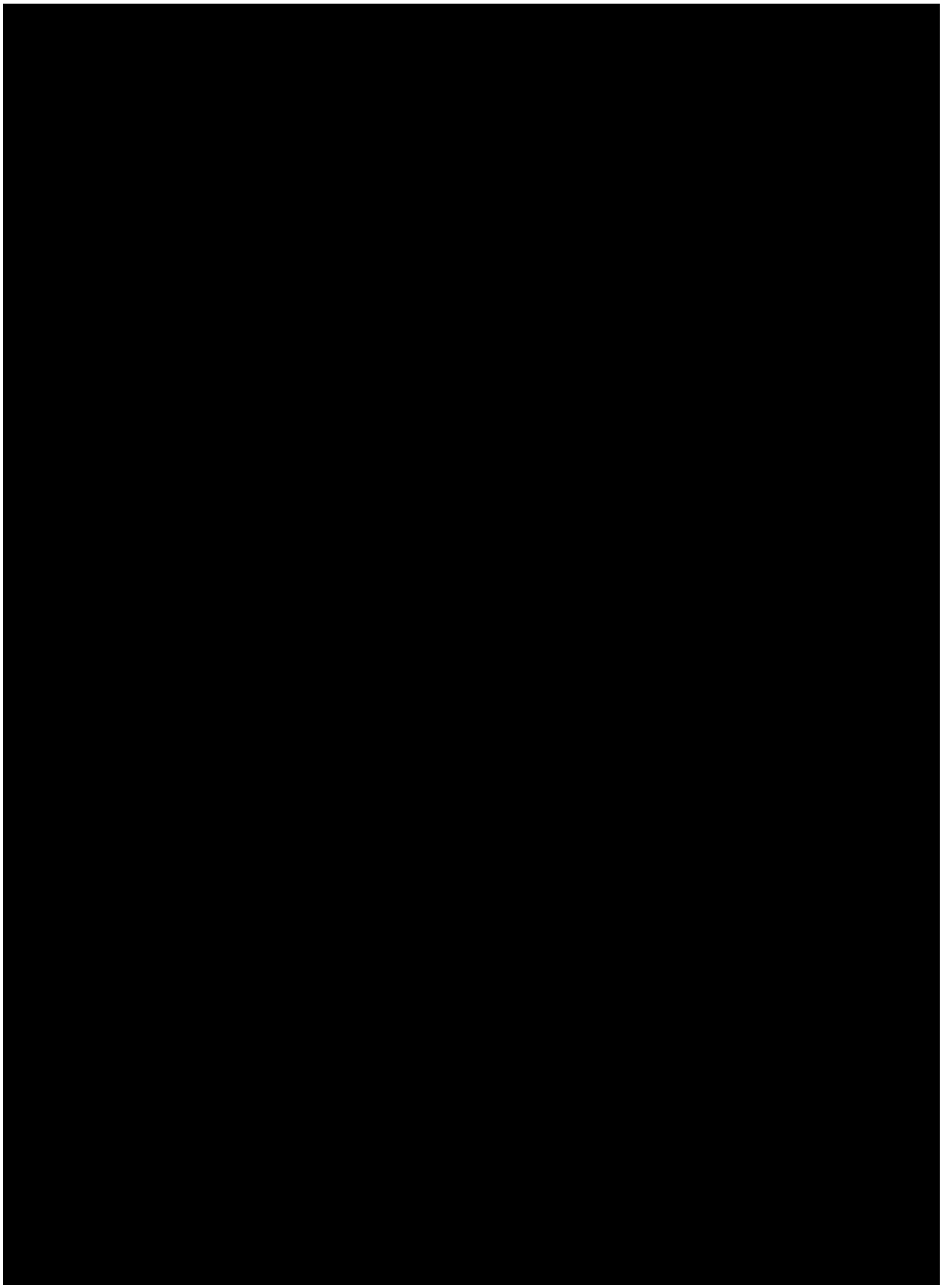
28. Funds in J.Z.'s Coinbase account were converted from $489,980 into 15.05 BTC and, on May 11, 2022, transferred to wallet address [redacted] at JENNY's direction. In addition, on May 18, 2022, funds in J.Z.'s Coinbase account were converted from $244,990 into 8.26 BTC and transferred to wallet address [redacted] at JENNY's direction.

29. For purposes of blockchain analysis, [redacted] is in a cluster of addresses herein referred to as the "MGCCKJ-FX Cluster".[3] The MGCCKJ-FX Cluster also includes other Bitcoin addresses identified as being highly likely under control of the same owner based on change address analysis.[4]

30. J.Z.'s stolen funds were swapped from BTC to USDT using imToken and Tokenlon. The USDT was consolidated into wallet address [redacted] and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived at the **Subject Account**, as shown in the diagram below:

[3] A Bitcoin cluster will also include all other Bitcoin addresses identified as being highly likely under control of the same owner based on change address analysis.

[4] Based on my training and experience, I know that change address analysis identifies addresses operating as change addresses for a particular wallet, where all addresses are controlled by the same owner. When an address spends bitcoin, it must be spent in its entirety. Sometimes the value of the transaction is higher than what the owner wishes to pay. In this case, the wallet may generate a new Bitcoin address for which the owner also holds the private key, and sends the difference back to this address. This is known as change. Change addresses are therefore highly likely held by the same owner as the original Bitcoin address.



Fraudulent Investment Platform "Top Tank"

Victim L.Y.

31. In March or April of 2022, L.Y. met a person on the social platform LinkedIn who went by the name of BOWEN CHEN ("CHEN"). They began speaking with one another and formed an online relationship that moved from LinkedIn to communication on WhatsApp. CHEN presented himself as an architect who had his own firm. During their communication, L.Y. began to trust CHEN and his advice.

32. Soon their conversations turned to crypto currency. L.Y. did not know anything about crypto currency or how it worked and trusted CHEN when he told her how it worked and how to make money with it. L.Y. was open to learning something new and trusted CHEN and followed his advice when he told her cryptocurrency was the future and she needed to get in on it early before it gets too common. CHEN told L.Y. he hired a group of analysts that were able to predict trade chances for higher returns.

33. CHEN instructed L.Y. to start her crypto trading by downloading and creating an account with Coinbase. After she created an account with Coinbase, CHEN sent her a downloadable link for an application called "Top Tank". The Top Tank app she downloaded was the application she used to make her cryptocurrency trades at the advice and direction of CHEN. During her trades, the Top Tank app showed L.Y. made profits from her trades. L.Y. then tried to withdraw her funds from the Top Tank app and into her Coinbase account. As she tried to withdraw her funds, she was told she had to pay a tax of $75,000 on her balance. L.Y. was in contact with Top Tank's "Customer Service", via the

app, in order to pay her taxes on her balance. L.Y. knew taxes were normal so she paid the $75,000 via cryptocurrency to Top Tank with the help of Top Tank's customer service guiding her through the process of payment.

34. Once she made the tax payment, she again tried to make a withdrawal of funds and was then told her account credit was only at 75% and needed to be at 100% in order to make any withdrawals. L.Y. was told by customer service that in order to get her account credit up to 100%, she needed to pay more money. L.Y. was under the impression CHEN was also investing and had even invested more than she did and may have lost more than she did. L.Y. no longer has contact with CHEN and it seems he disappeared from social media. L.Y. was never able to make any withdrawals from the Top Tank app and lost her entire investment of approximately $175,000.

Victim H.L.

35. H.L. is the hiring manager for her company. Therefore, she is on LinkedIn a great deal. An unknown male, FEI KUANG ("KUANG"), connected with H.L. on LinkedIn. H.L. accepted the request because KUANG appeared to be Chinese and utilized that language to communicate with her. KUANG sent his picture as well as a copy of his green card to H.L.[5] Part of the green card was covered and H.L. thought it was for security purposes so she didn't challenge it. KUANG claimed he used to work on Wall Street and was looking to start his own business. H.L. was "interviewing" KUANG and asking him many questions.

[5] H.L. later determined in talking with law enforcement that the green card was fake.

36. KUANG started discussing crypto transactions with H.L. as she already had a Binance.US account with a balance of $4,000. KUANG told H.L. what he was trading in terms of crypto and offered to teach her. H.L. transferred additional cash into her account. KUANG then instructed H.L. to purchase additional crypto and transfer these funds to her new BXMEX account. Eventually, KUANG told H.L. to move her funds from BXMEX to Top Tank due to lower fees at the latter platform. KUANG attempted to initiate a romantic relationship with H.L. but she thought it was inappropriate due to LinkedIn being a platform for business. KUANG told H.L. to delete LinkedIn as it was not safe.

37. Upon attempting to withdraw funds from Top Tank, H.L. was told she had to pay taxes first. H.L. knew the U.S. would not require taxes in that manner so she researched it online. She found an article that the Chinese government required 20% taxes on any transaction. H.L. then paid the required amount. After sending the money, Top Tank told H.L. her funds were involved in money laundering and insider trading. H.L. then realized she was the victim of a scam as the platform kept on trying to get her to pay more money without allowing her to withdraw any of her funds. Despite repeated attempts, H.L. never was able to make any withdrawals and lost approximately $2.5 million in the Top Tank platform scam.

Victim A.C.

38. In March 2022, A.C. was approached by EDEN LIN ("LIN") on LinkedIn. LIN's profile stated he was a consultant at Crypto.com. A.C. and LIN became good friends and LIN started teaching A.C. futures trading. LIN suggested they utilize the futures trading platform, mcus.me, since he was familiar with the site. Over the next 3.5 months,

LIN convinced A.C. to transfer all of her crypto (she already was invested in various cryptocurrencies) to mcus.me as well as her liquidated retirement accounts and money from her regular bank accounts. A.C. was very sick with COVID during this time frame and was in a weakened state. During this time, A.C. was able to make a successful withdrawal, with LIN's guidance, from mcus.me into her Coinbase account.[6] A.C. thought she was transferring these funds (including USDT and Bitcoin) into her own personal account with mcus.me.

39. When A.C. got sicker, LIN convinced her to withdraw the entire amount (totaling $2.9 million to include apparent trading profits) from her mcus.me account. During the withdrawal process, A.C.'s mcus.me account was frozen as they stated her last crypto transfer had a money laundering issue, thus requiring a security deposit of $293,000 in order to facilitate the withdrawal. A.C. was able to raise $80,000 but not the entire $293,000. LIN told her he would help with the rest and instructed her to transfer the $80,000 to his private wallet. In June 2022, the mcus.me website disappeared. LIN is also not responding to any of A.C.'s messages on social media.

40. In addition to the above mcus.me scam, A.C. was contacted in March 2022 by ZELIN WANG ("ZELIN") by phone. ZELIN claimed to be a University of Chicago alum and wanted advice on how to set up his new company. They started talking over the

[6] Based upon my training and experience, and conversations with other law enforcement personnel, I know that this is a common tactic in pig butchering schemes. Victims are often allowed to make an initial withdrawal, when they have only invested a relatively small amount of money, in order to boost their confidence in the legitimacy of the platform.

phone, and then the messaging app LINE, and became friends. ZELIN wanted to show her how he is trading crypto on a platform called Top Tank, and asked A.C. to transfer in USDT to a newly created account. A.C. transferred $40,000 to ZELIN and he showed her how to trade. The account quickly grew to approximately $60,000. When A.C. attempted to withdraw $30,000, her account was frozen purportedly because of AML issues. Top Tank representatives then required A.C. deposit the equivalent amount of her entire account balance to unfreeze the account. ZELIN assured A.C. that he had withdrawn money from the platform before so A.C. sent in $50,000 to Top Tank with ZELIN telling her he would help with the additional $10,000. However, when ZELIN was transferring the $10,000, he claimed to have mistakenly transferred $100,000 instead. Top Tank then requested A.C.'s driver's license and bank information, which she provided. A.C. thinks Top Tank is connected to https://sinsab.com, as that is where ZELIN asked A.C. to wire the funds.

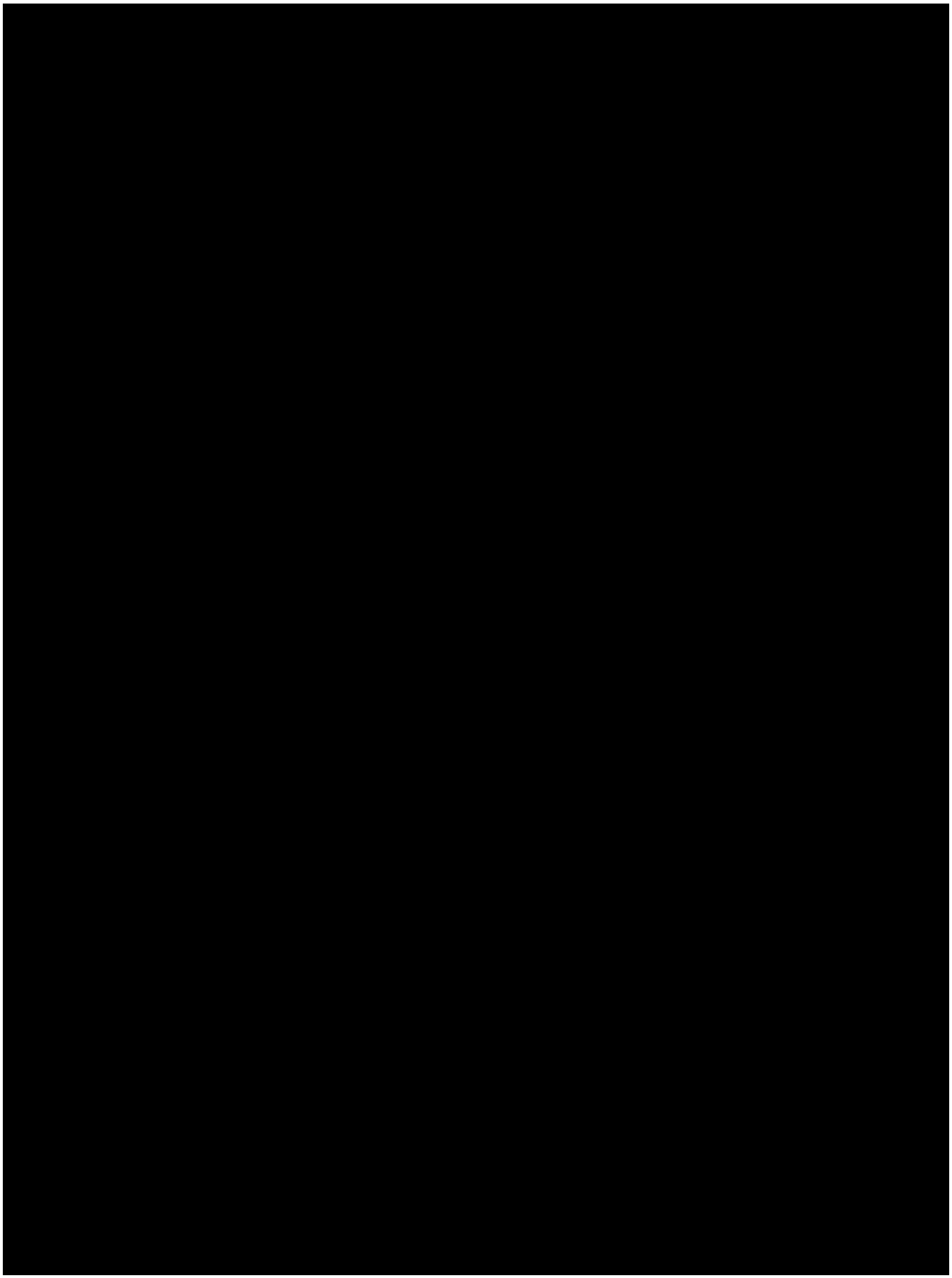
41. Despite repeated attempts, A.C. was never able to make a withdrawal from either of the fraudulent platforms. A.C. lost approximately $1.4 million in the mcus.me platform scam and approximately $100,000 in the Top Tank platform scam.

Tracing of Victim L.Y.'s, H.L.'s, and A.C.'s Funds to the Subject Account

42. On May 23, 2022, funds in L.Y.'s Crypto.com account were converted from $200,000 into 193,282 USDT and transferred to wallet address [redacted] at CHEN's direction. On May 23, 2022, funds in H.L.'s Crypto.com account were converted from $150,000 into 147,472 USDT and transferred to wallet address [redacted] at KUANG's direction. A transfer also occurred on May 24, 2022, after funds in A.C.'s Crypto.com

account were converted into 49,305 USDT and transferred to wallet address [redacted] at ZELIN's direction.

43. L.Y.'s, H.L.'s, and A.C.'s stolen funds were transferred and consolidated together in wallet address [redacted] and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived at the **Subject Account**, as shown in the diagram below:



Fraudulent Investment Platform "Deribit"

Victim L.Z.

44. L.Z. was approached by a purported friend to invest in crypto at a website "deribit-e.net/wap/" (subsequently "deribit-i.xyz/wap/"), and an associated app, in May of 2022. L.Z. was told the platform was a branch of Deribit.com and the company was seeking approval to operate in the U.S. L.Z. eventually invested approximately 239,715 Tether (USDT) in his account on what he thought was the Deribit platform. Through the ensuing months, L.Z.'s account apparently increased greatly. His purported balance in early July 2022 was approximately 5,211,000 USDT.

45. In order to realize the gain and pay expected U.S. taxes due in 2022, L.Z. attempted to withdraw his funds in July 2022. He requested two separate withdrawals of $50,000 and $100,000, respectively. The platform, however, told him he could not make the withdrawals until he paid taxes of 3% of his profit, or approximately 150,000 USDT. They said they would email him the tax form after L.Z. paid the tax, and rejected L.Z.'s request to utilize his own deposited funds of approximately 239,715 USDT to pay the tax. The platform also refused to provide any tax reporting forms for him to complete the transaction. L.Z. again tried to withdraw 180,000 USDT from his wallet and was blocked by the platform.

46. L.Z.'s purported friend identified herself to L.Z. as SIQI LIU ("LIU"). LIU claimed to work at LG Networks in Dallas but the company does not have an employee by that name when L.Z. made an inquiry. She also claimed to be a graduate of Wuhan University but L.Z.'s research showed LIU to be a graduate in a different year than she

claimed. L.Z.'s review of her photos she sent him showed she was likely in Richmond Hill, Ontario, Canada when they were taken.

Victim Q.H.

47. Q.H. was approached on LinkedIn by DORIS LIN ("LIN"). After communicating on LinkedIn for a while, they soon moved their communications to WhatsApp and LINE. LIN introduced Q.H. to investing in crypto on the Deribit platform. LIN claimed she was working on a project team that was database related for Deribit. LIN claimed to have a wonderful opportunity as she noticed trends in how the crypto was traded on the site. LIN said she was testing herself by making small trades. LIN instructed Q.H. to open accounts at Crypto.com and Kraken. Q.H. was then instructed to wire funds from his bank to the new accounts and convert the funds to Tether (USDT). After the conversion, Q.H. was instructed to transfer those funds to what he thought was a legitimate Deribit platform. LIN would then instruct Q.H. on when to make trades.

48. Q.H. eventually wanted to withdraw some of his funds. First, "Support" for Deribit said his account was suspected of illegal activity and required a purported Account Guarantee of $88,000 for review. Once his account was cleared, Support told Q.H. the funds would be returned to his account. Then Support claimed that Q.H. owed $134,000 in taxes. After Q.H. made the tax payment, Support then required Q.H. to pay a Credit Enhancement Guarantee of $55,000. Q.H. was too focused on getting his funds back to take a step back and look at the situation. After making all of the above requested payments, Q.H. attempted to make another withdrawal. Q.H. had done this numerous times by copying and pasting his wallet address to the request. On the latest withdrawal request, the

last digit of his wallet address was somehow manipulated causing the withdrawal request to fail. Support insisted the wallet address was incorrectly entered by Q.H. Support told Q.H. they recovered all of his funds for him but now required Q.H. pay the equivalent of the total fund balance amount to successfully make the withdrawal.

49. Q.H. then realized he was part of a scam. Q.H. cut off contact with LIN after Support required him to pay all of the extra fees. Q.H. was never able to make a withdrawal and lost his entire investment of approximately $337,500 in the scam.

Victim D.C.

50. D.C. was approached by an unknown female named ANNA L. on LinkedIn. D.C. later determined ANNA's other name is LIN YU-QING ("YU-QING"). YU-QING told D.C. she lived in Canada. After connecting on LinkedIn, YU-QING suggested they move their communications to the messaging app LINE. Her name on LINE was Q.

51. YU-QING told D.C. she was working for a tech company on a project in Toronto. She claimed she saw improper and big volume trading in Mana cryptocurrency and told D.C. this was the opportunity of a lifetime. YU-QING instructed D.C. to download an app called Deribit to open an account and complete the trades. YU-QING first instructed D.C. to open accounts with Coinbase and Crypto.com. D.C. was then told to wire transfer funds from his bank to his exchange accounts. After that, YU-QING instructed D.C. to wire funds from his exchange account to the fraudulent platform (an offshoot of Deribit).

52. YU-QING instructed D.C. on how to withdraw money as well. The first withdrawal of $200 was successful so D.C. thought the platform was legitimate. Then one

day when D.C made trades he lost all his money. He then added more money to his account to try and make up what he lost. D.C. approximates he lost $475,000 initially with the fraudulent platform. YU-QING then told D.C. how she made all her money back by borrowing from friends and relatives. D.C. received personal loans and invested again with the fraudulent platform. D.C.'s account was as high as $615,900. He then tried to withdraw his money. The fraudulent platform told him he could not withdraw any money as the system had frozen his account because some of D.C.'s transactions may be illegal. In order to lift the freeze, D.C. was told he would have to pay 15% of his account for review. If he did not pay, D.C.'s account would be terminated. They also told D.C. they would put him on the "black list" and report him to banks around the world. D.C. then contacted YU-QING. YU-QING told D.C. that this had happened to her as well. YU-QING's account was over $10 million and she had to pay $1.8 million to unfreeze her account. YU-QING suggested that D.C. take out several personal loans to pay to unfreeze his account. In his conversations with "support" for the fraudulent platform, D.C. was given the following email address: support@deribit-q.site.

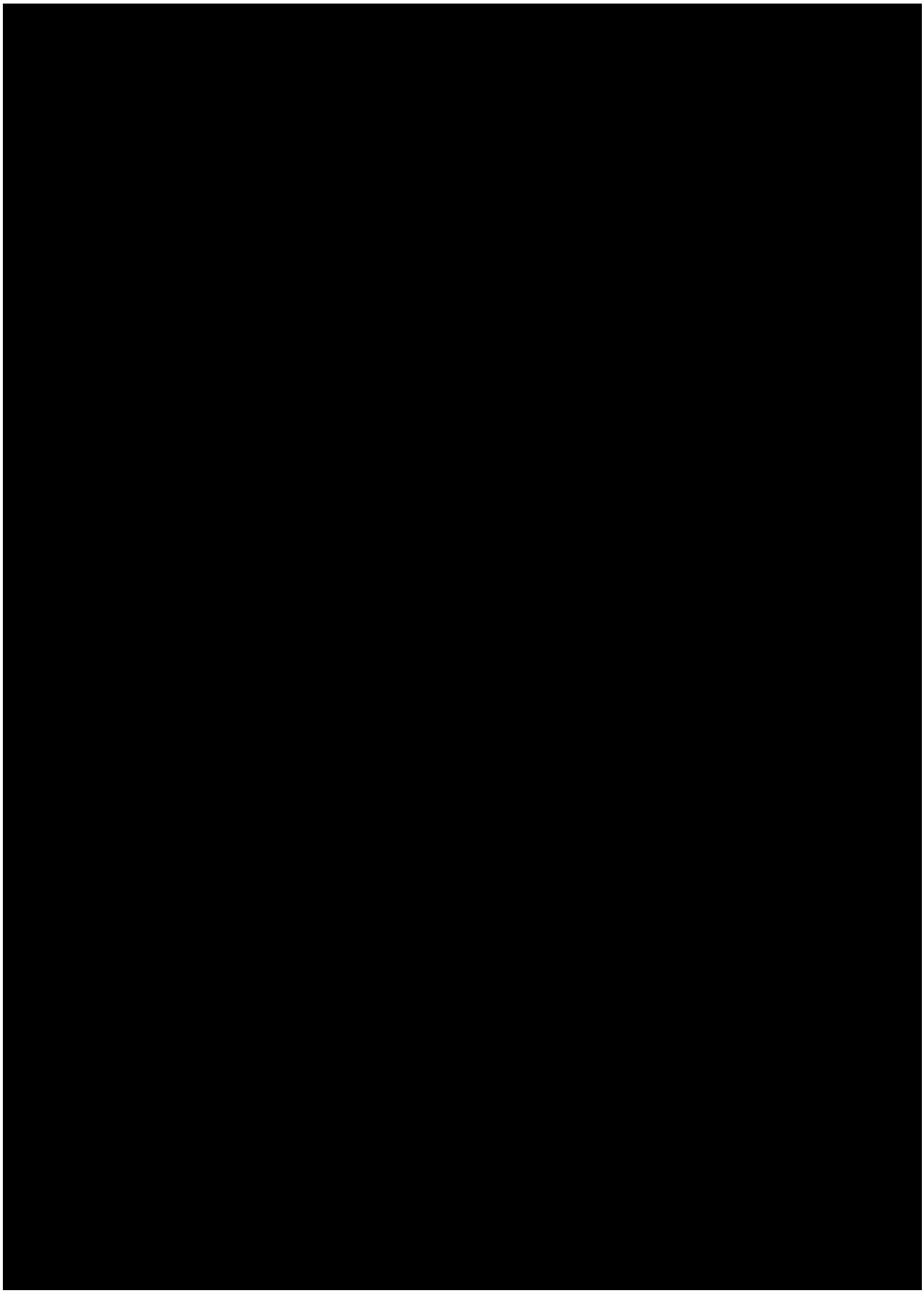
53. D.C. finally realized the fraudulent platform and website were scams. D.C. eventually contacted the legitimate company Deribit, who stated that they were going to open a case and conduct an investigation. D.C. lost his entire investment of approximately $500,000.

Tracing of Victim L.Z.'s, Q.H.'s, and D.C.'s Funds to the Subject Account

54. On May 26, 2022, funds in L.Z.'s Binance.US account were converted from

$25,000 into 24,891 USDT and transferred to wallet address [redacted] at LIU's direction. A transfer also occurred on May 26, 2022, after funds in Q.H.'s Kraken account were converted into 87,636 USDT and transferred to wallet address [redacted] at LIN's direction. On May 26, 2022, funds in D.C.'s Crypto.com account were converted from $25,000 into 24,752 USDT and transferred to wallet address [redacted] at YU-QING's direction.

55. L.Z.'s, Q.H.'s, and D.C.'s stolen funds were consolidated together in wallet address [redacted] and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived at the **Subject Account**, as shown in the diagram below:



Fraudulent Investment Platform "Penzo Limited"

Victim K.F.

56. K.F. was approached in a phone message by an unknown female named JINTONG GUO ("GUO"). Shortly thereafter, they started to communicate via Skype. GUO provided K.F. with a picture purportedly of herself. GUO discussed investing in bitcoin via Antrush. GUO instructed K.F. to wire funds from his bank to Crypto.com. The funds were then transferred from Crypto.com to Antrush. In the beginning, K.F. only invested $20,000 and GUO showed him how to make an apparent 30% return. K.F. then invested substantially larger amount: a total of $480,000 from his bank, $250,000 in personal loans and approximately $100,000 from his 401(k) including an early withdrawal penalty.

57. In June 2022, Antrush told K.F. they were transferring his funds from Antrush to Penzo Limited (www.penzolead.com/en/index). K.F. began to get nervous after the switch to Penzo and tried to withdraw $440,000 of his money. K.F. then changed his mind and successfully withdrew $200. The support person K.F. talked to at Penzo about the withdrawal told him there was a large trading event with large funds to drag the market and he could follow. They instructed K.F. to follow the order. K.F. did follow the large order and within minutes all of his funds were gone. K.F. has lost his entire investment of approximately $850,000.

Victim M.T.

58. M.T. was contacted by text by an unknown female named "OLA" (possible other name Xu Meina). OLA stated she had texted M.T. by mistake as she was trying to

get in touch with a client. OLA claimed to work for a clothing company in Laguna Beach, CA. M.T. researched the company and the actual building using Google Street View. OLA and M.T. then moved their communications to WhatsApp.

59. M.T. thought he was in a romantic relationship with OLA. She talked to him very nicely and sent him romantic songs. She promised to take him back to Hong Kong. She also spoke Cantonese. Sometimes M.T. would communicate with her using Google translate.

60. OLA talked to M.T. about cryptocurrency trading and convinced him to get involved. OLA's instructions were to open an account at Coinbase. M.T. would wire funds from his bank to his Coinbase account. OLA also instructed M.T. to use the Meta Trader 5 app for his crypto trades. From Coinbase, the funds went to Anthereum at the beginning. OLA then told him to stop sending funds there, and instructed him to send funds to "trader.penzolead.com." Shortly thereafter, OLA instructed M.T. to send funds to "m.sunglobal.vip." This last platform was where M.T.'s money was frozen.

61. OLA admitted to M.T. that the crypto trading opportunity she was telling him about was purportedly based on insider trading. OLA did not want to get her broker in trouble. OLA told M.T. that he could make 90% profit in 120 seconds with the trading opportunities.

62. M.T.'s account at Sun Global was then frozen. M.T. wanted to withdraw funds to pay off some of the loans he took out as part of this crypto trading opportunity, but Sun Global representatives told him that he could not withdraw his money without paying taxes first per the "IRS Blockchain Technology Cryptocurrency Authority" and that

M.T.'s money would be released after he pays the tax, M.T. subsequently talked to the U.S. Internal Revenue Service and learned there is no department with that name. OLA urged M.T. to quit his job, liquidate his 401(k) and pay the $200,000 tax bill. M.T. refused and has not spoken to OLA since. M.T. has lost approximately $425,000 in the scheme.

Victim P.N.

63. P.N. was contacted by an unknown female he believed was Chinese named Susan, who told P.N. her Chinese name was Huiming Chen ("CHEN"). CHEN texted P.N. and told him her mother told her to contact him for the possible purpose of marriage. P.N. told CHEN she had the wrong guy. CHEN apologized but kept in contact with P.N. Later, CHEN added P.N. to her friend group in the messaging app LINE.

64. CHEN told P.N. she lives in Orange County, CA and has her own custom clothing business. Soon after, CHEN told P.N. that she invests in cryptocurrency to include Bitcoin (BTC) and USD Coin (USDC) and she was making good money doing so. CHEN claimed she had an uncle that has a team doing investment analysis who would tell her when to make trades. CHEN asked if P.N. was interested, and P.N. decided to give the trading a try.

65. CHEN assisted P.N. with opening an app on his phone to open an account with Penzo Limited. CHEN instructed P.N. to fund a Coinbase account with his money from his bank account. CHEN told P.N. to purchase USDC, then transfer the USDC to his newly opened Penzo Limited account. CHEN told P.N. not to trade on his own but to wait for when she contacted him after she received tips from her uncle. CHEN proceeded to notify P.N. to make trades and he followed her directions. P.N. was apparently making

approximately 20% on his investment. After several successful trades, CHEN encouraged P.N. to invest more money and advised P.N. to take out personal loans that he could easily pay back after a few more trades. P.N. borrowed $280,000 and added approximately $400,000 of his own money to his Penzo account. Soon thereafter, his Penzo account had apparently doubled and was approximately $1.27 million.

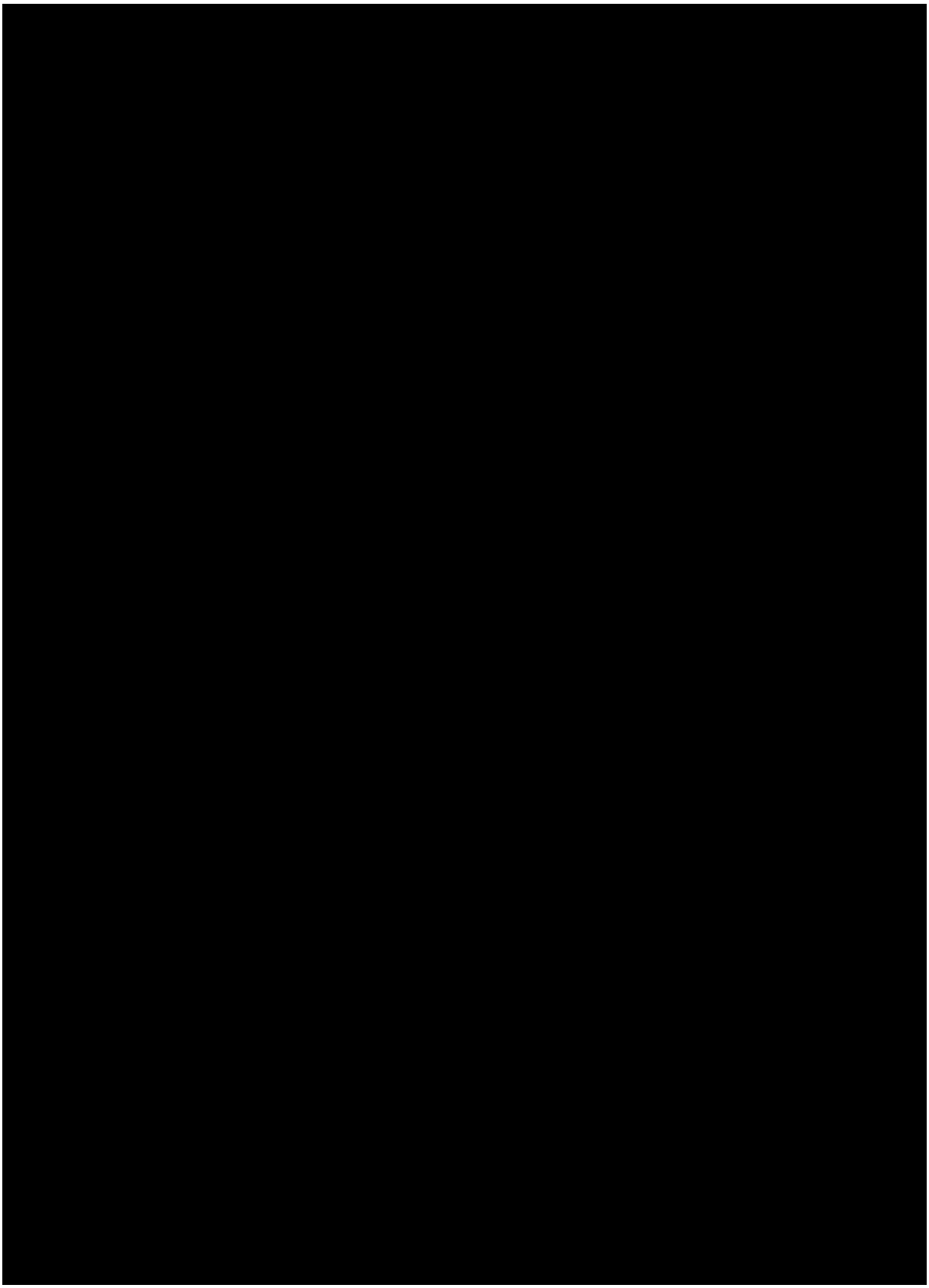
66. In July 2022, CHEN instructed P.N. to make another trade similar to all the previously executed trades. In less than two minutes, all of P.N. funds were gone. P.N.'s Penzo account was now zero. P.N. reached out to CHEN but she disappeared and did not respond. P.N. tried reaching out to Penzo Limited at "support@penzolead.com" per the website "www.penzolead.com/en/index," but was unsuccessful.

Tracing of Victim K.F.'s, M.T.'s, and P.N.'s Funds to the Subject Account

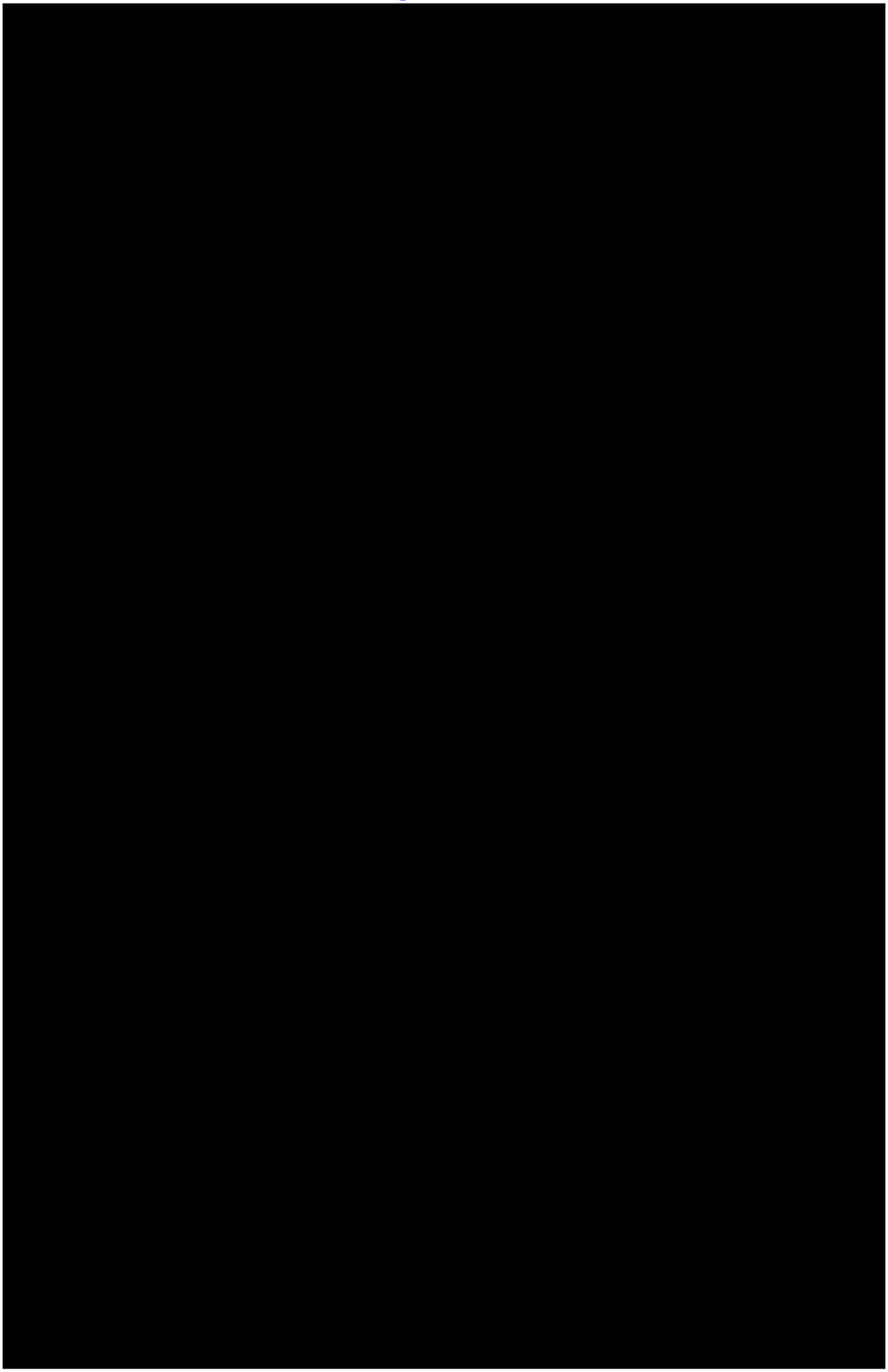
67. On June 14, 2022, funds in K.F.'s Crypto.com account were converted from $110,000 into 107,902 USDT and transferred to wallet address [redacted] at GUO's direction. On June 14, 2022, funds in M.T.'s Coinbase account were converted from $50,110 into 40 ETH and transferred to wallet address [redacted] at OLA's direction. Two transfers also occurred on June 13, 2022 and June 14, 2022, after funds in P.N.'s Coinbase account were converted into 36,000 USDC and 86,950 USDC and transferred to wallet address [redacted] at CHEN's direction.

68. M.T.'s and P.N.'s stolen funds were swapped for USDT using Tokenlon. K.F.'s, M.T.'s, and P.N.'s stolen funds were consolidated together in wallet address [redacted] and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived

at the **Subject Account**, as shown in the diagram below:



69. In sum, each of the 10 victims above were victims of similar Pig Butchering schemes and all 10 of the victims had some portion of their "investments" directed to the **Subject Account**. The following diagram depicts the sophisticated movement of victim funds described above, with the common denominator being that some portion of the victim funds were directed to the **Subject Account**:



70. Even though each of the victims discussed above were targeted by different online personas, each had some of their stolen funds funneled to the **Subject Account**. Based upon my training and experience, and my conversations with other law enforcement personnel, I know that the funneling of funds such as depicted in the diagrams above are common methods used by individuals who are attempting to launder large amounts of cryptocurrency, and, therefore, want to thwart law enforcement's ability to trace, and ultimately recover, criminal proceeds.

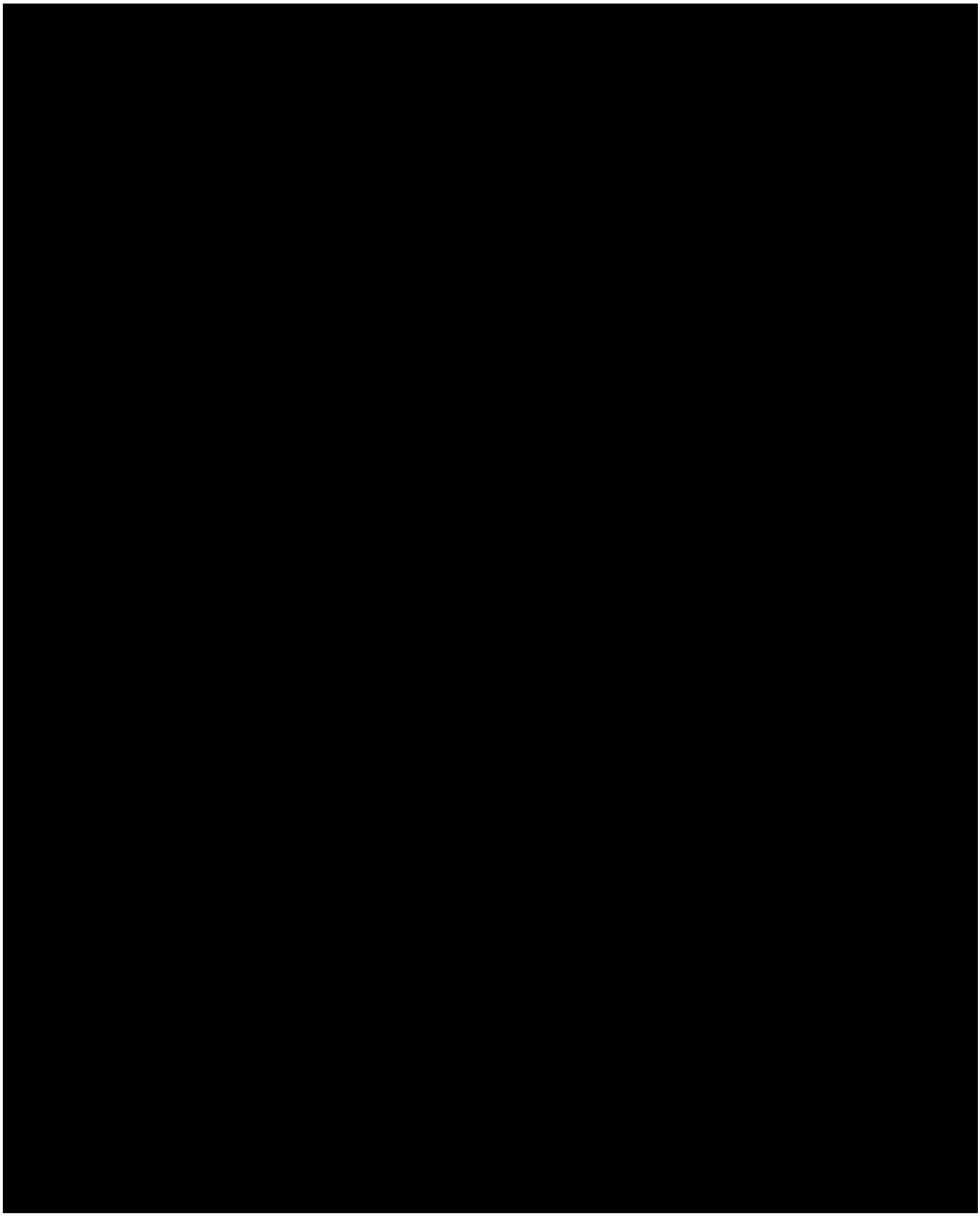
71. In addition, there is no apparent reason, economic or otherwise, for the use of such a complex movement of cryptocurrency through the use of multiple intermediary wallet addresses, unless the purpose is to conceal the nature, source, location, ownership or control of the funds at issue.

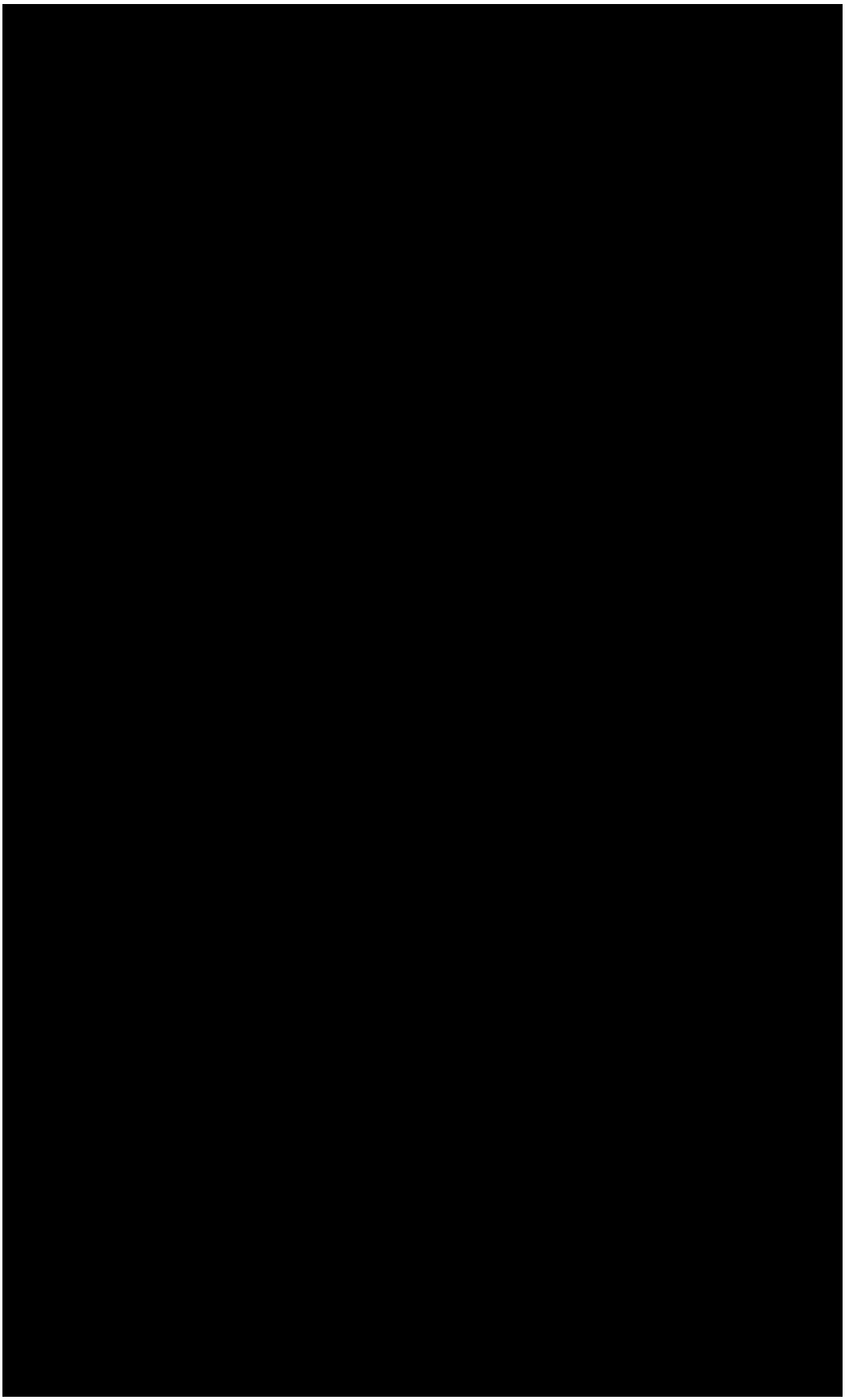
[redacted]

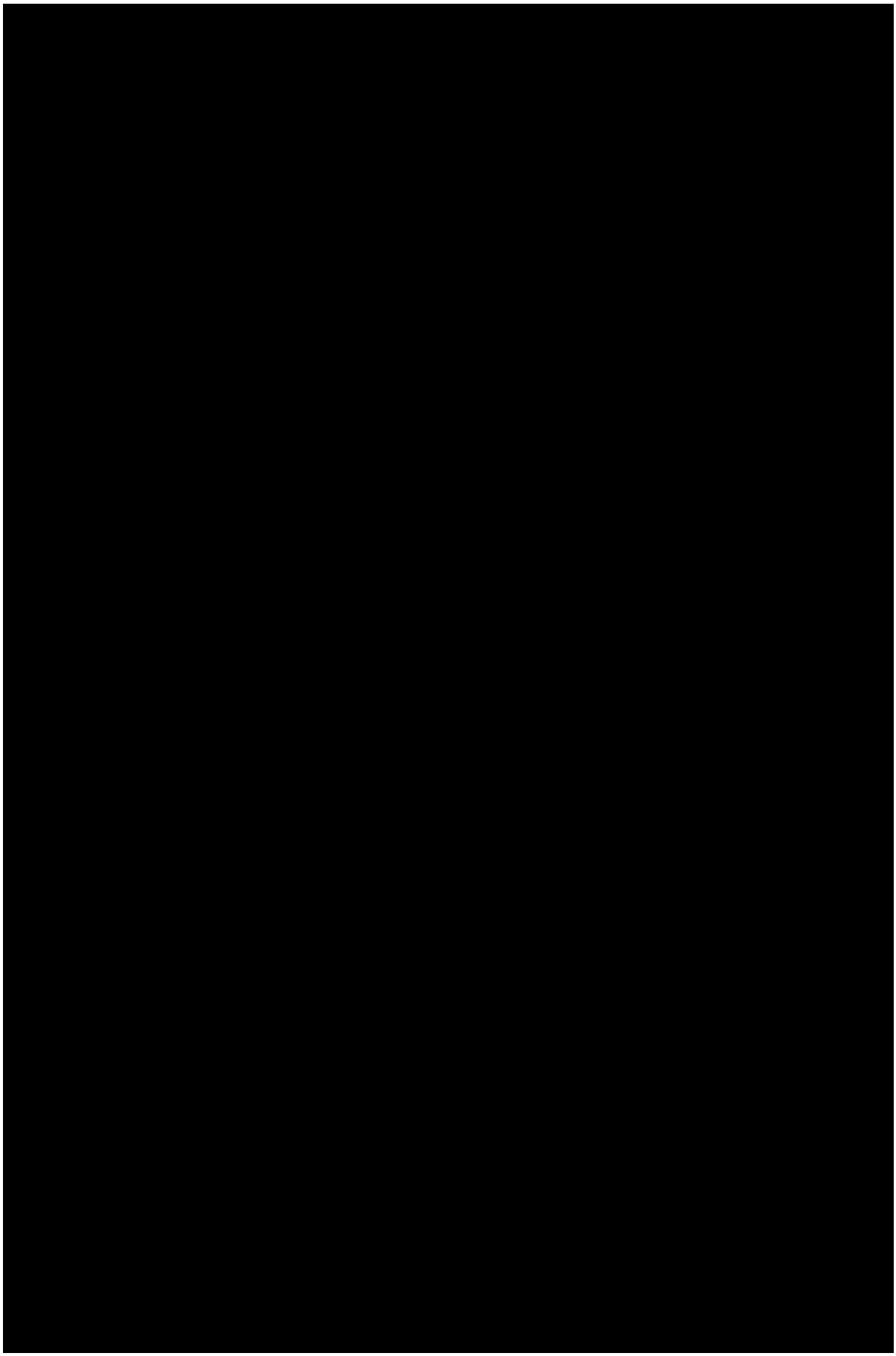
72. On November 15, 2022, and November 29, 2022, [redacted] provided the following information:

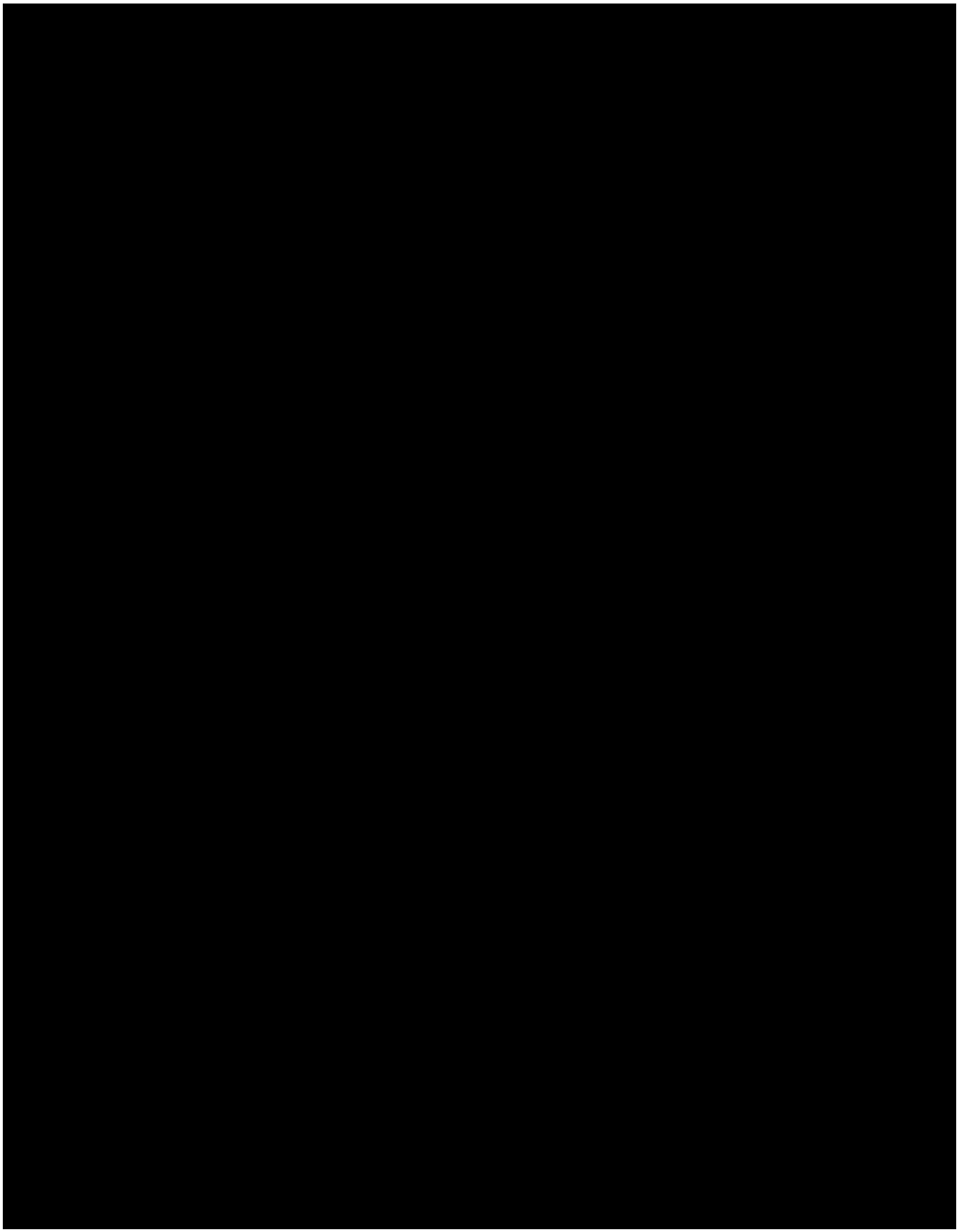
[redacted]

[redacted]







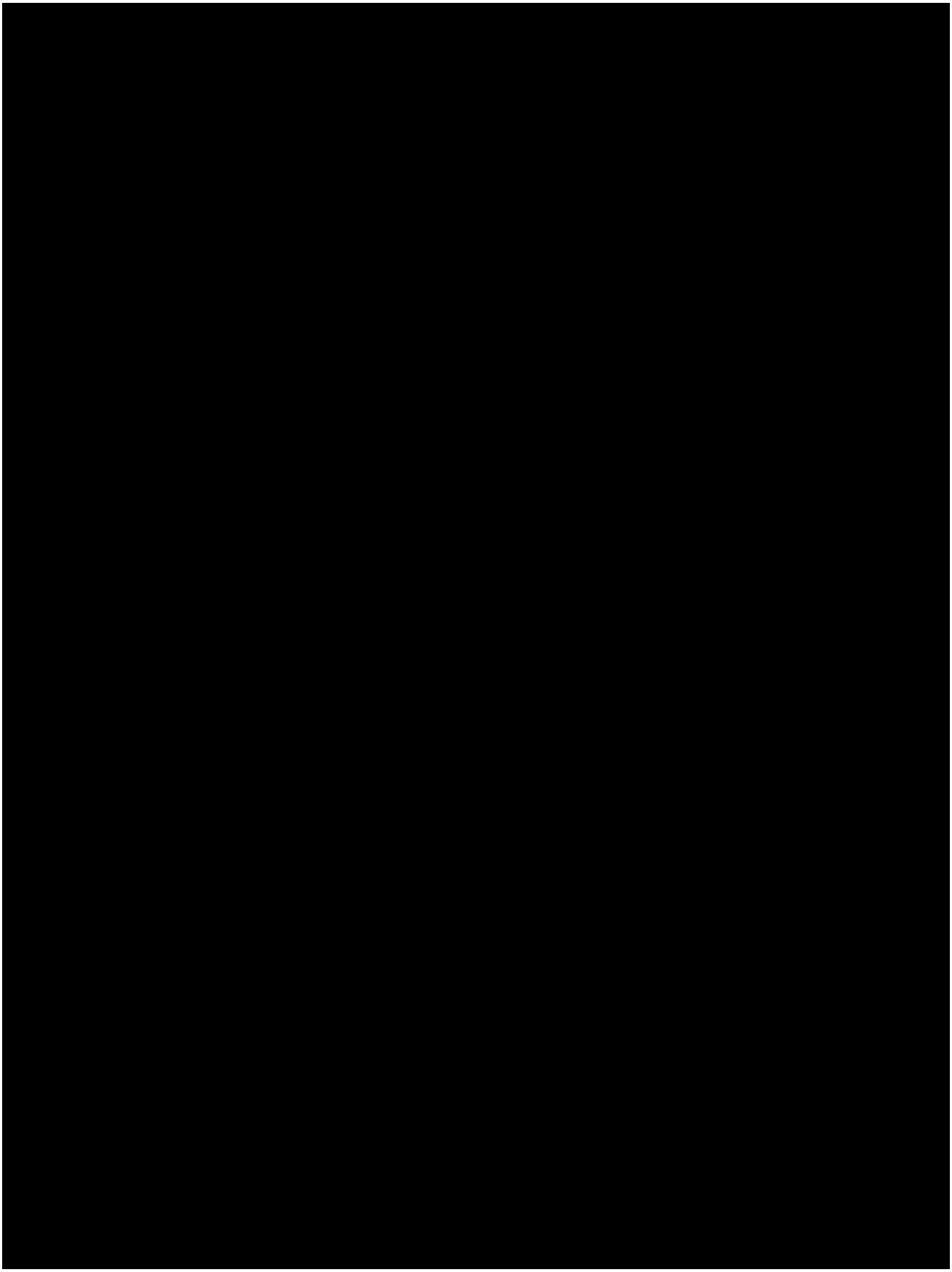


[redacted]

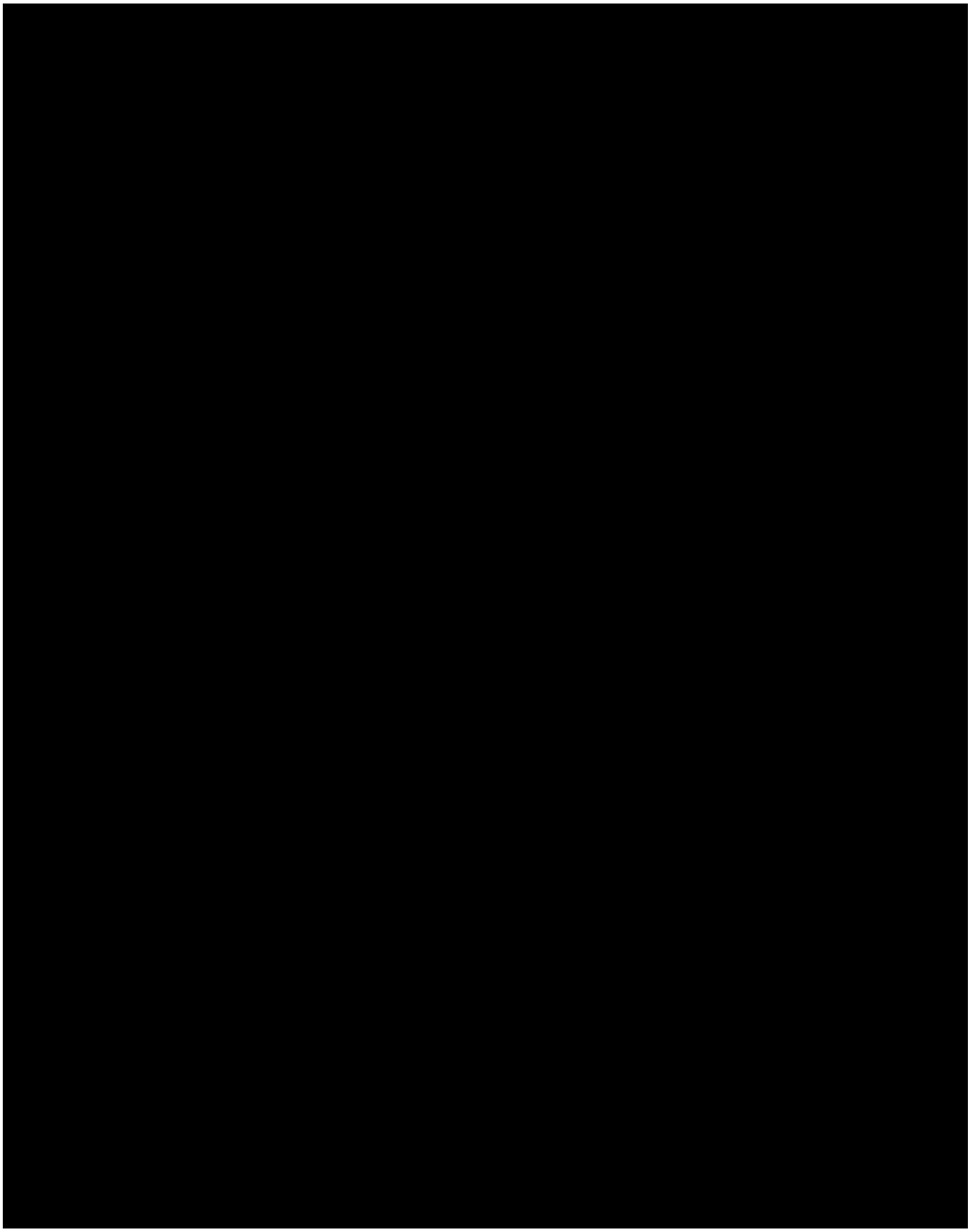
76. On November 21, 2022, Seizure Warrant [redacted] was issued in the District of Arizona. This seizure warrant was for three Binance accounts associated with pig butchering scams, including Binance account in the name [redacted] user identification number [redacted] (the "[redacted] Account").

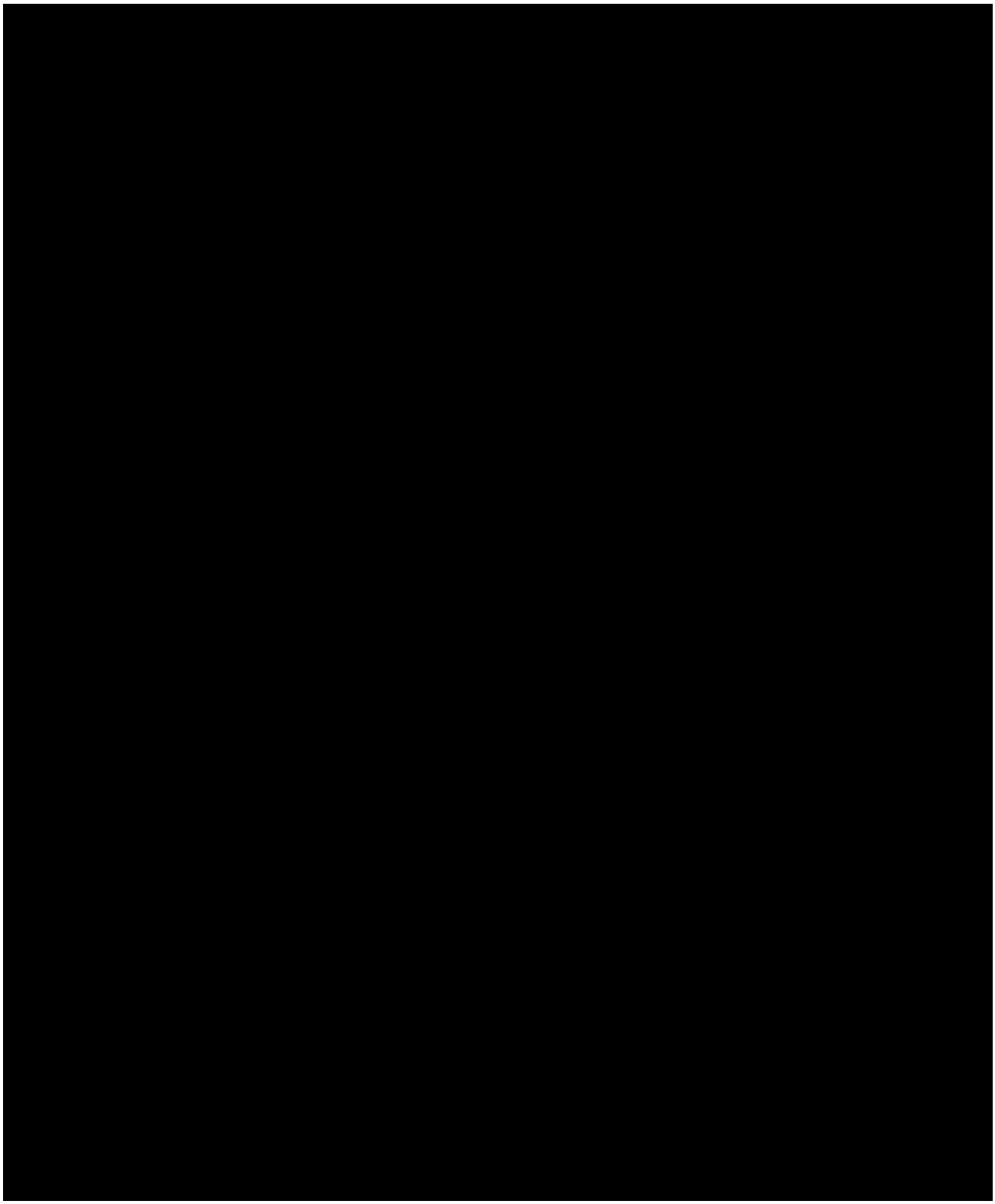
77. While analyzing the [redacted] Account, FBI Forensic Accountants identified that some of the USDT deposits into that account came from the **Subject Account**. The USDT was sent in a coordinated manner from **Subject Account** and one

other Binance account (the "[redacted] Account") and then consolidated and sent on to the [redacted] Account. The following chart shows the flow of funds being traced backwards from the [redacted] Account to the **Subject Account**.



[redacted]





80. Based on my training and experience, and my conversations with other law enforcement personnel, I know that legitimate businesses generally do not access multiple

Binance accounts, including those in other individuals' names, in order to split up transactions and coordinate withdrawals across accounts.

81. Both USDT withdrawals to address [redacted] occurred on the Tron blockchain. However, the preceding USDT deposits into both accounts occurred on the Ethereum blockchain, as shown in the above figure. [redacted]

82. FBI Forensic Accountants attempted to trace the source of these funds backwards, as shown in the above figure. However, the USDT was moved in a series of rapid transactions through multiple private wallets, and exchange accounts. Based upon my training and experience, my conversations with other law enforcement personnel, and what I know of this investigation, this rapid movement of funds through multiple wallets and exchange accounts, with funds being split up, and then later reconsolidated in coordinated movements of funds, can only be described as a concerted effort to obfuscate the flow of funds and to hide entirely the location and source of the funds.

CONCLUSION

83. Based on information derived from the foregoing investigation, there is probable cause to conclude that the **Subject Account** received the proceeds of a wire fraud and money laundering scheme performed in violation of 18 U.S.C. §§ 1343, 1349 (wire fraud and conspiracy to commit wire fraud), and 18 U.S.C. §§ 1956(a)(1)(B)(i), 1956(h) (money laundering and conspiracy to commit money laundering). Those proceeds are

subject to seizure pursuant to Title 18 U.S.C. § 981(b)(2) and (3) and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), and 28 U.S.C. § 2461(c). Finally, there is further probable cause to believe that a greater amount of funds constitute property involved in money laundering transactions, to wit: the entire balance of the funds from the **Subject Account**. The **SUBJECT FUNDS** are accordingly subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A). Accordingly, I respectfully request that a warrant be issued authorizing the seizure of the **SUBJECT FUNDS**.

84. I submit that a protective or restraining order issued pursuant to 21 U.S.C. § 853(e) would be insufficient to ensure the availability of the funds in the **Subject Account** for forfeiture. Cryptocurrency can be transferred faster than traditional bank funds, and once transferred, generally cannot be recalled to an original wallet. Moreover, there is a risk that the funds may be moved to a location where no forfeiture or seizure would be possible, at which point the funds could be further laundered into a "privacy" (*i.e.* untraceable) cryptocurrency. Thus, I submit that a seizure warrant is the only means to reasonably assure the availability of the funds in the **Subject Account** for forfeiture.

I swear, under penalty of perjury, that the foregoing is true and correct.

Respectfully submitted,

[redacted]

[redacted]

Special Agent

Federal Bureau of Investigation

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 15th day of December, 2022.

HON. ALEXANDER F. MACKINNON
UNITED STATES MAGISTRATE JUDGE