UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **CHUI KOK WA,** **GISLEN NEUKEU,** **SHAMUSA NINSIIMA,** **CLEMENT MUGIRANEZA,** **MERVEILLE MUDACUMURA, and** **NICODEMUS HINGIMA MONYANCHA,** **Defendant.**	**CRIMINAL NO. 26-mj-**

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, [redacted], after being duly sworn, depose and state as follows:

1. This affidavit is submitted for the purpose of establishing probable cause for a complaint charging that from a date unknown but at least in or about January 1, 2025, through April 2026, while located abroad, CHUI KOK WA (Coconspirator/Defendant 1), GISLEN NEUKEU (Coconspirator/Defendant 2), SHAMUSA NINSIIMA (Coconspirator/Defendant 3), CLEMENT MUGIRANEZA (Coconspirator/Defendant 4), MERVEILLE MUDACUMURA (Coconspirator/Defendant 5), NICODEMUS HINGIMA MONYANCHA (Coconspirator/Defendant 6) (collectively, the "Defendants") all conspired to commit wire fraud against citizens of the United States of America, for violations of 18 U.S.C. §§ 1343, 1349 (Wire fraud conspiracy). Specifically, the Defendants executed a cyber- and crypto-enabled investment fraud ("CIF") scheme from a compound in Madagascar wherein workers did defraud U.S. persons via the use of U.S. wires. I further request that the Court issue an arrest warrant for WA.

2. [redacted] As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions and other financial crimes governed by federal law, including Title 18 of the United States Code.

3. The facts and information contained in this affidavit are based on my personal involvement in this investigation, personal knowledge and observations, my review of records and documents obtained during this investigation, and information received from other individuals, including analysts and other law enforcement officers, as well as my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause to obtain a criminal complaint, it does not set forth each and every fact known by me or the United States.

4. Based on my training and experience and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the District of Columbia and elsewhere, Defendant WA and others have committed violations of 18 U.S.C. §§ 1343, 1349 (Wire fraud conspiracy) from at least in or around January 2025 to in or around April 2026.

JURISDICTION, STATUTES, & VENUE

5. As discussed more fully below, the criminal offenses under investigation began or

were committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. *See* 18 U.S.C. § 3238. Venue is also proper within this judicial district. *Id.*

6. Section 1343 of Title 18 of the U.S. Code criminalizes devising or intending to devise any "scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." Section 1349 of Title 18 of the U.S. Code criminalizes the conspiracy to commit wire fraud, as defined in Section 1343.

PROBABLE CAUSE

I. Background on General Cryptocurrency Investment Fraud

7. The United States is investigating international criminal organizations operating cyber-enabled and cryptocurrency investment fraud (CIF) scams.[1] According to information developed through the investigation and ample public reporting, in CIF scams, victims (often in the United States) are targeted and, over time, deceived into fraudulent investment schemes on fake websites and platforms. Relevant here, these platforms are controlled by criminal actors overseas, primarily associated with Chinese organized crime syndicates, and while the platforms purport to show that victims are making substantial returns on their cryptocurrency "investments," in reality, all victim funds are funneled directly to the scammers.

8. Based on my training and experience in this and other cases, and information relayed to me from other FBI agents, I know that most Southeast Asian scam compounds are

[1] In public reporting, these scams are sometimes referred to as "pig butchering," a term derived from the Chinese phrase used by the scammers to describe this scheme.

owned and operated by groups of individuals made up of family members and business partners that largely originate from Fujian, China. The owner operators of Southeast Asian scam compounds are frequently from the same or neighboring cities. Based on my knowledge of this and other investigations, as well as public reporting, numerous scam compounds have moved from Southeast Asia to other global locations in the last year, to include to the African continent.

9. CIF is a confidence/investment scam perpetrated against victims for financial gain. The perpetrators contact victims, usually online, and form a strong relationship, romantic or otherwise, over days, weeks, or longer. After the subject has gained the victim's trust, the subject introduces the victim to the idea of investing in cryptocurrency. The subject then directs the victim to a specific scam website or app disguised as a legitimate investment platform.

10. The scam websites to which the victims are directed are often accessible on traditional web browsers and mobile applications (or "apps"). However, it is increasingly common for them to also be accessible within a Web3 portal.[2] When fraud victims are interacting with these scam platforms, they are provided with cryptocurrency addresses to fund their account. The victims are instructed to open an account on a cryptocurrency exchange to exchange fiat currency (U.S. dollars) for cryptocurrency and send that cryptocurrency to the cryptocurrency address(es) provided by the websites. CIF scams occur in a variety of different methods ranging from social engineering victims into sending funds themselves, to more technically complex operations which gain access to victims' wallets and/or tokens via the use of phishing websites, malware, or malicious smart contracts.

11. The fraud victims believe sending cryptocurrency to a cryptocurrency address provided by one of these scam websites constitutes depositing money into a legitimate investment

[2] A Web3 Portal is essentially a web browser that allows users to access decentralized websites running on the blockchain. It is common for victims to mistake their cryptocurrency wallet application as the location of their investments.

platform; in actuality, the victims are sending funds directly to scammers, who are then free to move those funds along to associates. The scam websites purport to show the victims' returns on their investment, prompting the victims to "invest" more cryptocurrency into the platform. These investments can take many forms, such as tokenized gold, general cryptocurrency, or Non-Fungible Token (NFT) investments. This scam is continued until a victim becomes aware of the scam or runs out of money, at which time the scammer ceases contact.

12. While fraud victims from numerous countries throughout the world are impacted by CIF schemes, the United States is one of the primary targets due to its global economic status. According to one U.S. government funded study, "the size of this criminal market is still extremely difficult to estimate due to the lack of reporting on what represents a novel form of criminality [but,] as of the end of 2023, a conservative estimate of the annual value of funds stolen by these scam syndicates worldwide now approaches $64 billion a year and involves millions of victims."[3]

13. According to the FBI's Internet Crime Complaint Center (IC3), cyber-enabled fraud schemes were responsible for almost 85% of all losses reported to IC3 in 2025. Within that category, CIF schemes have continued to grow, and the IC3 calculated that the reported losses from CIF scams rose, from $4.57 billion in 2023, to $8.65 billion in 2025, an increase of 89%.[4] These figures, largely based on losses reported by victims, likely significantly under-represent the true loss amounts incurred by Americans, since most fraud victims do not report to IC3, if at all.[5]

---

[3] Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security (May 2024) ("A Growing Threat (May 2024)"), available at https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf (last accessed on November 6, 2025).

[4] IC3, Federal Bureau of Investigation Internet Crime Report (2025), available at https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf (last accessed June 10, 2026).

[5] Statement of Gregory Heeb, Dep. Ass't Dir., FBI (Mar. 25, 2026), *available at* https://www.jec.senate.gov/public/_cache/files/2f5ca5c1-44c9-4e23-944e-8008293856f7/sfr-gregory-heeb.fbi.pdf (last accessed June 10, 2026).

II. General Overview of Madagascar Operation

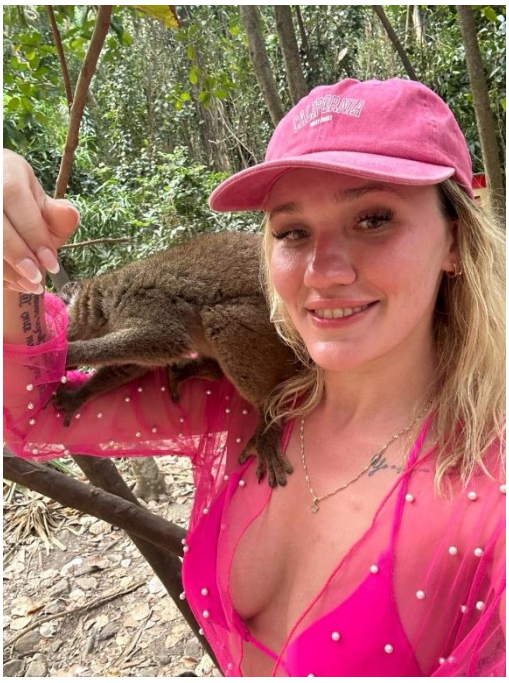
14. In August 2026, the FBI – Honolulu Field Office, in coordination with the Scam Center Strike Force of the United States Attorney's Office for the District of Columbia, and with the United States Attorney's Office for the District of Alaska, deployed a team to Madagascar at the invitation of the Madagascar Ministry of Justice and the Madagascar National Police (MNP). The FBI Team was primarily focused on assisting MNP authorities in Madagascar with computer forensics and triage of approximately 3,200 electronic devices which had been seized from thirteen separate scam compounds. The operation also sought to acquire information and intelligence on how organized transnational cyber-fraud groups infiltrate, establish persistence, and exploit nations which may be at increased risk of becoming safe harbors for organized cyber-fraud activity.

15. While present in Madagascar, the FBI team interviewed three Brazilian nationals who had previously worked in a scam compound in Antananarivo, Madagascar. These individuals reported that they originally responded to work opportunities posted online, and ended up working at a compound located in Cambodia. Later, in part due to an armed conflict between Cambodia and Thailand, and also in response to police activity in Cambodia related to scam compounds, the witnesses were moved to Antananarivo, Madagascar, in early-May 2026. This witness reporting is consistent with other information received by the FBI through its cases that cyber scam centers are increasingly opening in Africa following the closure of such compounds in Southeast Asia. In fact, as described further herein, records from Binance, a cryptocurrency exchange, showed that two conspirators associated with the scheme herein had logged into provider's website from Cambodia in 2025-2026, and then later from Madagascar, in early 2026; two additional conspirators had logged into provider's website from Myanmar and then later from Madagascar.

16. Malagasy authorities further informed the FBI team that in conducting searches of the thirteen scam compounds known to the authorities, the Malagasy authorities had taken into custody approximately 400 individuals, which included approximately 40 Chinese nationals. FBI attempted to interview many of these individuals, and was unable to secure interviews for the Chinese nationals identified as leaders, as the FBI was told by the Malagasy authorities that they were repatriated to China before FBI could do so, or were no longer in Malagasy custody.

III. Initial Identification of NFTWEB3 Scam

17. Upon arrival in Antananarivo Madagascar, the FBI team was presented with multiple devices by the MNP, which were subsequently reviewed by the FBI team. The evidence obtained therein, and legal process obtained from U.S. companies, together showed a scheme to defraud U.S. persons through the use of U.S. wires, through a cryptocurrency Non-Fungible Token (NFT) investment scheme ("The NFTWEB3 Scam"). In general, based on the review of the evidence from MNP as well as victim statements, the NFTWEB3 Scam involved the scammers posing as a beautiful woman who met victims on U.S. dating sites. Two examples follow, which were provided by U.S. victims of the NFTWEB3 Scheme.





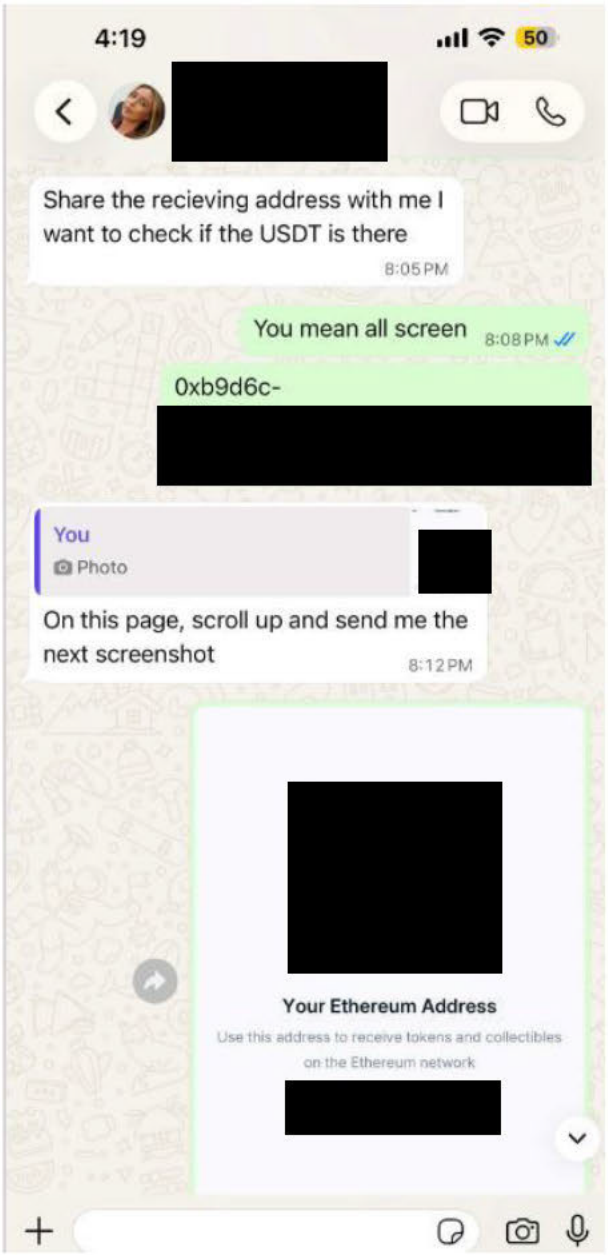
18. Under the scheme, the scammer would convince the victim to invest in NFT's and then have the victim link their cryptocurrency wallet to a specific website. Once linked, the scammer could then control the wallet and pull money without the consent of the victim. The scammer would continue the relationship (still posing as the attractive woman) to get the victim to fund their cryptocurrency wallet, and then once the wallet contained sufficient balance, would steal the cryptocurrency without the victims' knowledge.

19. As described further herein, through tracing on publicly-available blockchains, your Affiant has identified at least approximately 74 cryptocurrency wallets of victims who appear to have been defrauded by the scheme, for an estimate loss of at least approximately $516,695. Through a search of the FBI's Internet Crime Complaint Center (iC3), the FBI's online website for cybercrime reports, your Affiant reviewed multiple complaints related to the scheme, which are described further herein.

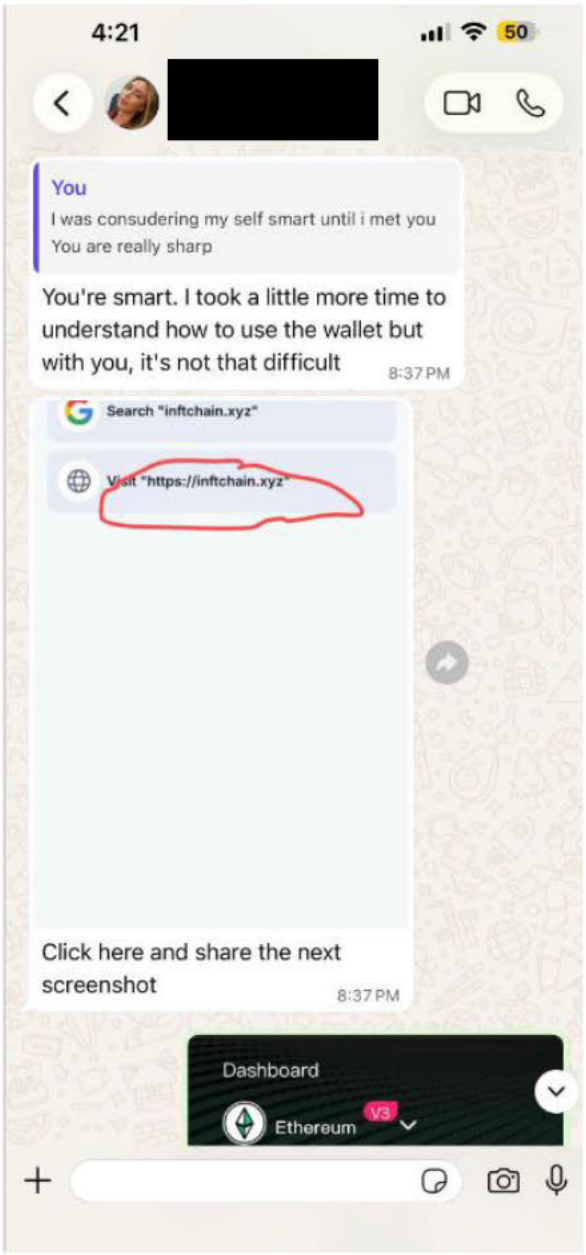
a. For example, a fraud victim in Greenbelt, Maryland (hereinafter, "the Greenbelt-Victim"), reported a loss of $11,926.12 to an NFT scam. The Greenbelt-Victim was introduced to the NFT Scam by a WhatsApp account, which utilized a female profile picture and telephone number ending in 7115. The Greenbelt-Victim initially deposited approximately 900 USDT utilizing the Ethereum Network, on August 24, 2026, into a wallet they controlled and believed they were involved in an NFT investment on the websites "inftvault.com" and "inftchain.xyz". After holding an NFT they believed was valued around $980, the Greenbelt-Victim's account on inftvault.com reflected an apparent gain of $15. The Greenbelt-Victim attempted to withdraw all their funds from the NFT platform, however, was unsuccessful. The following day, the Greenbelt-Victim deposited approximately 1,958.92 USDT into their wallet to conduct additional NFT investing. However, the Greenbelt-Victim

noticed an unauthorized transaction had occurred in their wallet, and 2,858.02 USDT had been sent to an address they did not control. The day after the unauthorized transaction, the Greenbelt-Victim deposited an additional 9,067.64 USDT into their cryptocurrency wallet to conduct NFT staking[6]. An unauthorized withdrawal of all 9,067.64 USDT occurred approximately 33 minutes after the USDT was transferred into the Greenbelt-Victim's wallet. All USDT from the second unauthorized transaction was sent to the same address as the first unauthorized transaction.

[6] NFT staking is a process where NFT owners may receive compensation by locking their digital assets on a platform or protocol. *See* https://www.coinbase.com/learn/advanced-trading/what-is-nft-staking-and-how-does-it-work.



(Screenshot provided by the Greenbelt-Victim of conversation with scammer)



(Screenshot provided by the Greenbelt-Victim of conversation with scammer)

b. A victim in Portland, Oregon (hereinafter, "the Portland-Victim"), reported a loss of $794 to an NFT scam. The Portland-Victim met an individual named Sally on the dating application "Wild". Sally quickly befriended the Portland-Victim and transitioned the conversation to WhatsApp. Sally assisted the Portland-Victim in using the Ethereum Network to transfer approximately 780 USDT to a cryptocurrency wallet under the control of the Portland-Victim, as

well as linking the Portland-Victim's wallet to the website "inftmeta.xyz", which the Portland-Victim also stated displayed as "inftvault.com". On or around April 21, 2026, the Portland-Victim noticed all the USDT in their wallet had been transferred without their knowledge and consent.

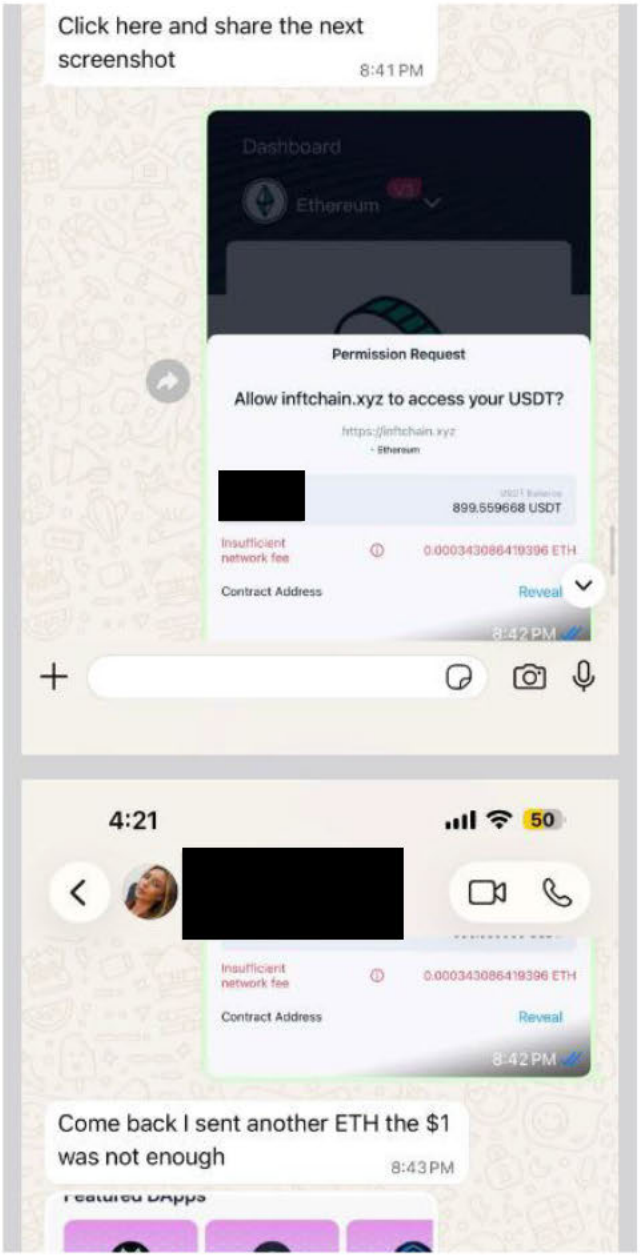
c. The Portland-Victim and Greenbelt-Victim reported the NFT Scam utilized at least two different domain names during the course of the fraud scheme: "inftmeta.xyz" and "inftvault.com". Additionally, the domain "inftchain.xyz" was identified in a screenshot sent by the Greenbelt-Victim. Utilizing publicly-available commercial tools, your Affiant identified "inftmeta.xyz" had a HTML website title of "Everyone's Favorite NFT marketplace". This title was identified as being present on nine separate domains, to include "inftchain.xyz", specifically:[7]

    1. inftchain.xyz
    2. bitnft.net
    3. bitnft.me
    4. bitnft.co
    5. inftx.me
    6. inftx.co
    7. inft.pro
    8. inftx.pro

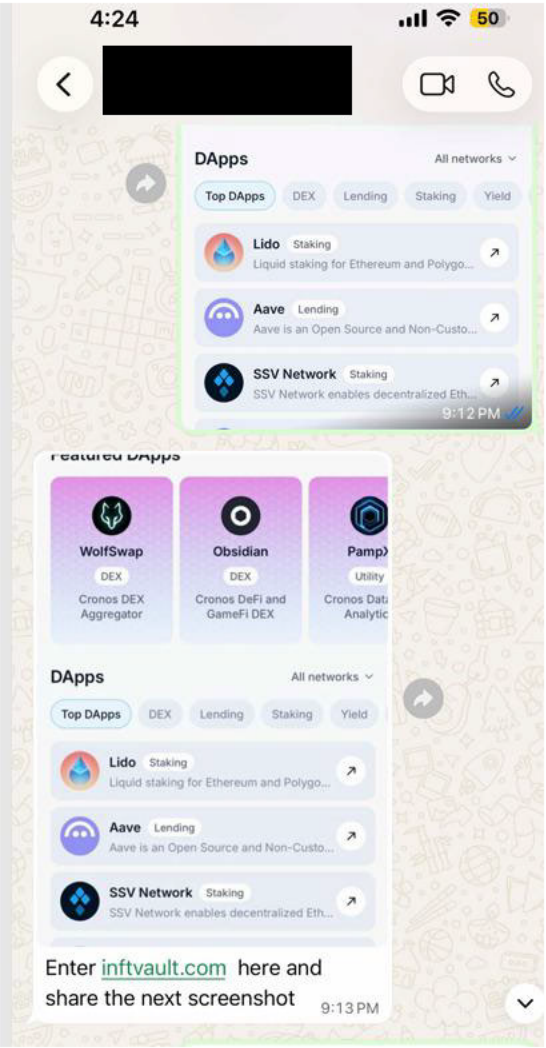
d. On or around August 28, 2026, your Affiant navigated to "inftchain.xyz" utilizing the MetaMask application's built in browser. Your Affiant connected a newly created MetaMask account to the website after being prompted to do so. Shortly thereafter, a second prompt was pushed by inftvault.com for a spending cap request. This request contained data which would, if signed by your Affiant, enable a third-party to transfer unlimited USDT from your

[7] These sites were previously seized by order of this Court, Case No. 26-sz-53.

Affiant's wallet at any time. Based on your Affiant's training and experience, this type of request is commonly utilized to trick victims into allowing scammers access to certain tokens within their wallets without realizing the extent of the permissions they have granted. This type of request is consistent with the activity explained by both the Portland-Victim and the Greenbelt-Victim.



(Screenshot provided by the Greenbelt-Victim of conversation with scammer displaying a similar malicious USDT access request which was observed by Affiant)



(Screenshot provided by Greenbelt-Victim evidencing connection to inftvault.com)

A. Identification of the NFTWEB3 Scam Conspirators

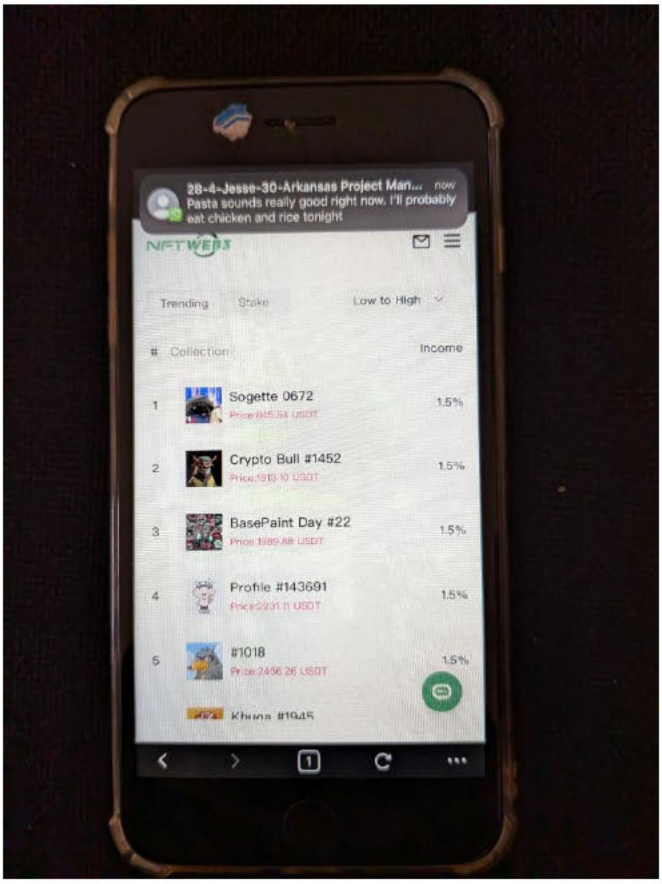
20. Through the review of electronic evidence in Madagascar provided by MNP, the FBI team identified the conspirators, based in Madagascar, who were operating the scheme. Among the devices provided by MNP and reviewed by the FBI team were two devices ("Device 1" and "Device 2"), which based on the FBI team's review appeared to belong to individual(s) in charge and/or working out of at least one of the ten scam facilities which had been raided by the

MNP. Both Device 1 (SN ending in FY2) and Device 2 (SN ending in G00) were Apple iPhone 7 Plus models.

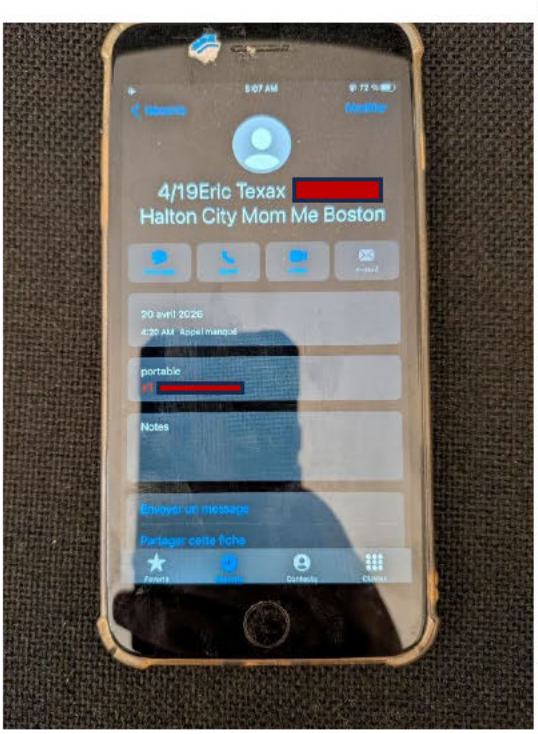
21. As described further herein, both Device 1 and Device 2 contained content related to the NFTWEB3 Scam. Specifically, both appeared to be phones by which scammers were communicating with victims, including those in the United States.

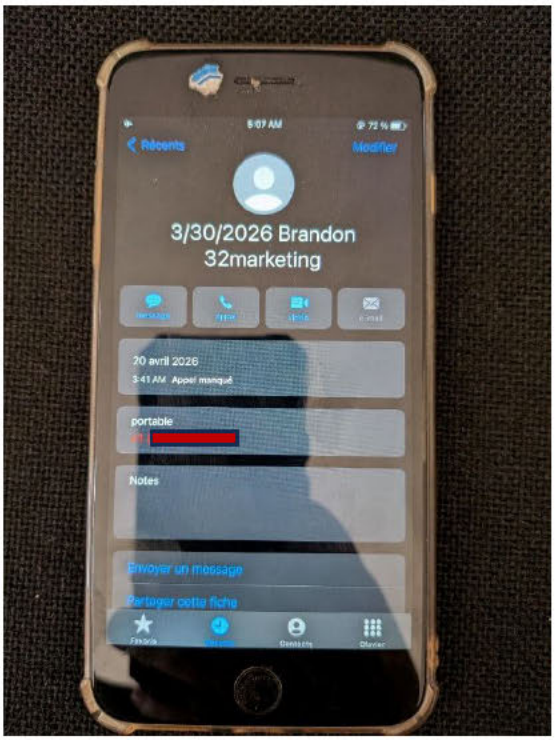
Scammer Communications with U.S. Victims

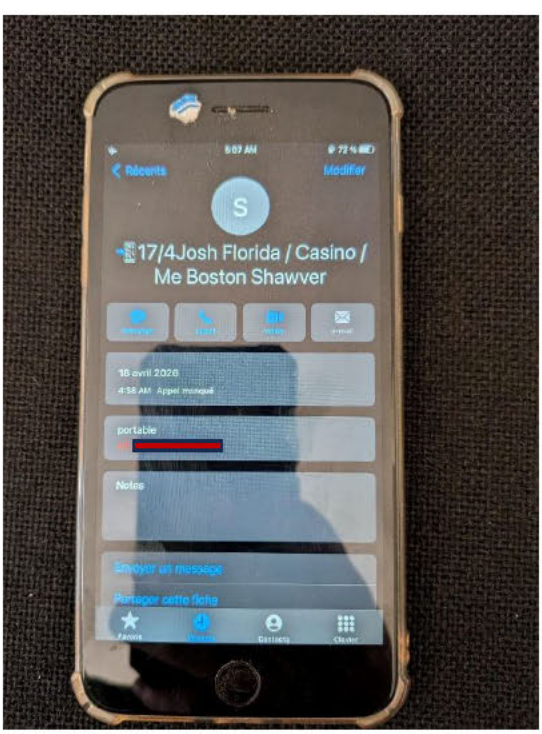
22. For instance, an image depicting a WhatsApp message notification on Device 1 was located and appeared consistent with naming conventions utilized by scam operators to keep track of victims. Based on my training and experience in this and other cases, I know that a single scam line worker can be simultaneously chatting with multiple victims at the same time, and they will often develop name syntax for organization. For instance, the image identified on Device 1 likely indicates the scam operator who utilized Device 1 was speaking with an 30-year-old individual from Arkansas named Jesse, and thus saved in the phone's contact card the name "Jesse-30-Arkansas-Project Manager", as follows.

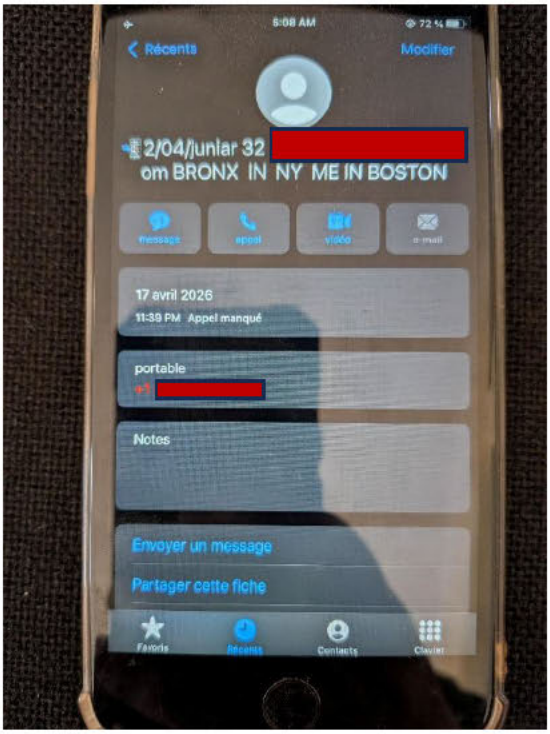


23. Multiple other images were identified on Device 1 which appear to show similar naming syntax, likely used to organize victim information, as follows.

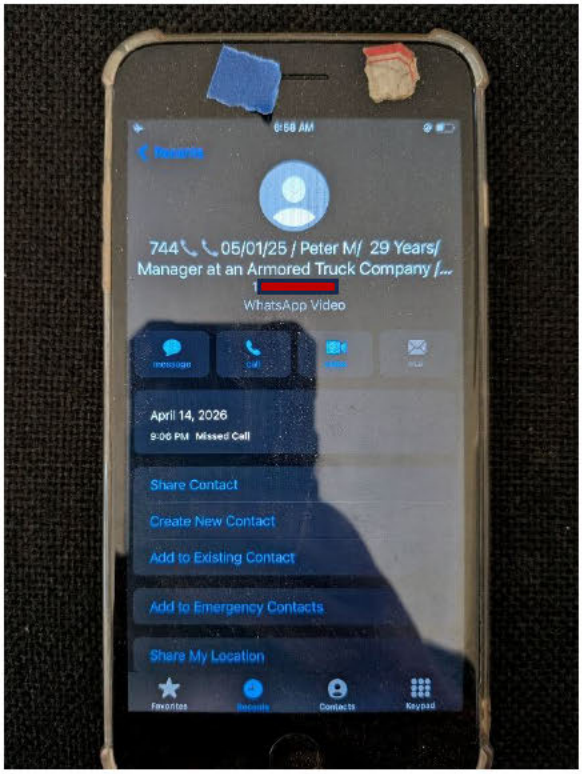


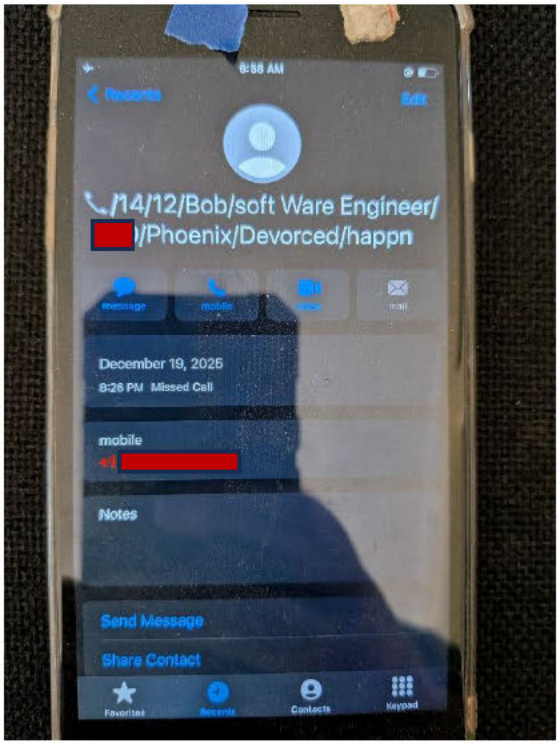




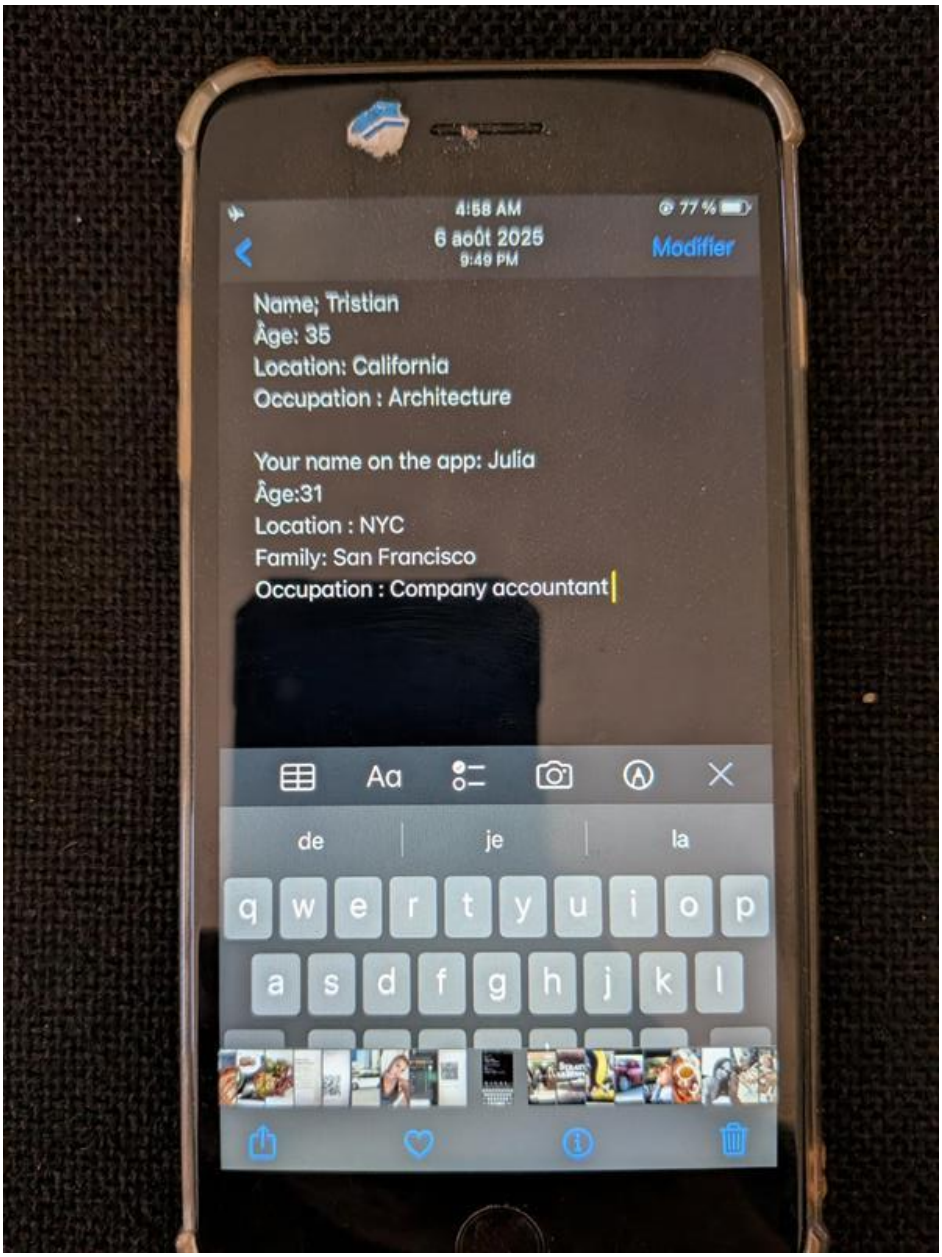


24. Likewise, on Device 2, multiple contacts were identified on Device 2 which had similar naming syntax to Device 1.

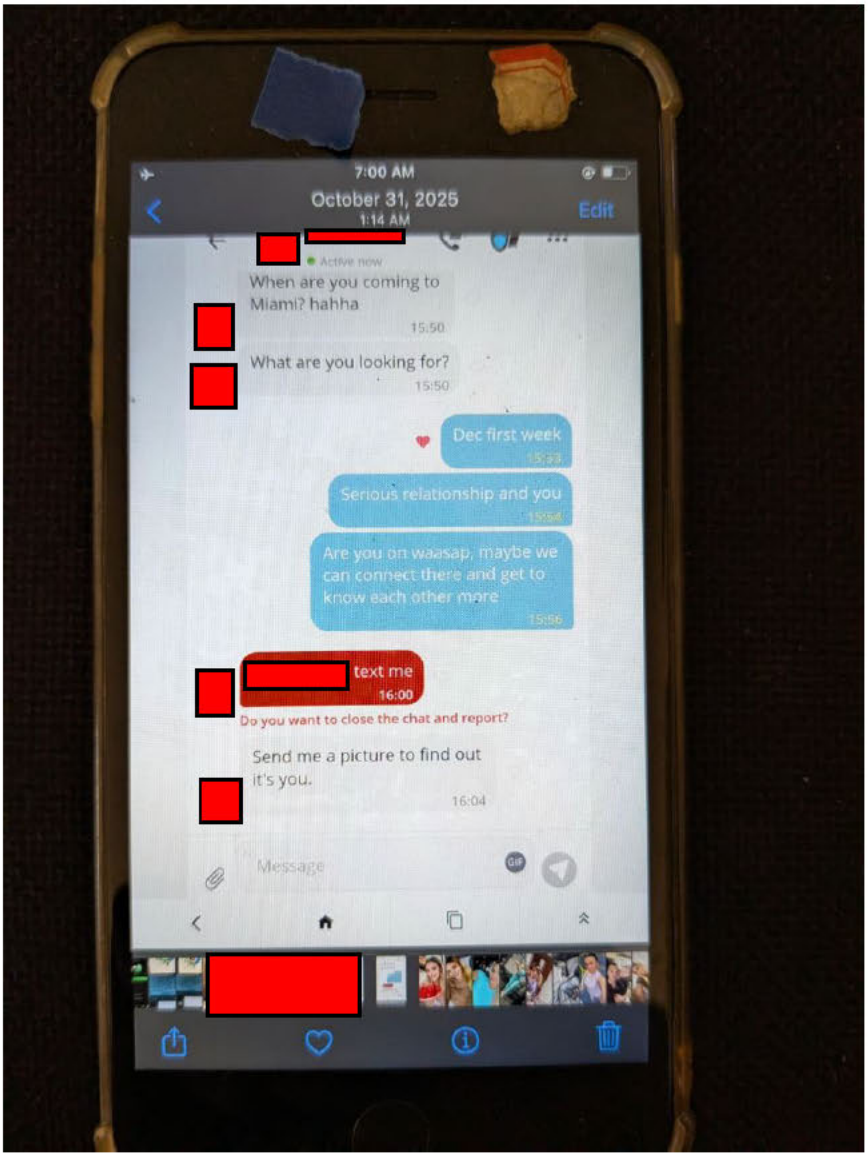




25. Additionally, an image located on Device 1 was located and appeared to be a screenshot of a Notes App entry on Device 1. The image appears consistent with a scam operator organizing information about both their victim and fake persona.

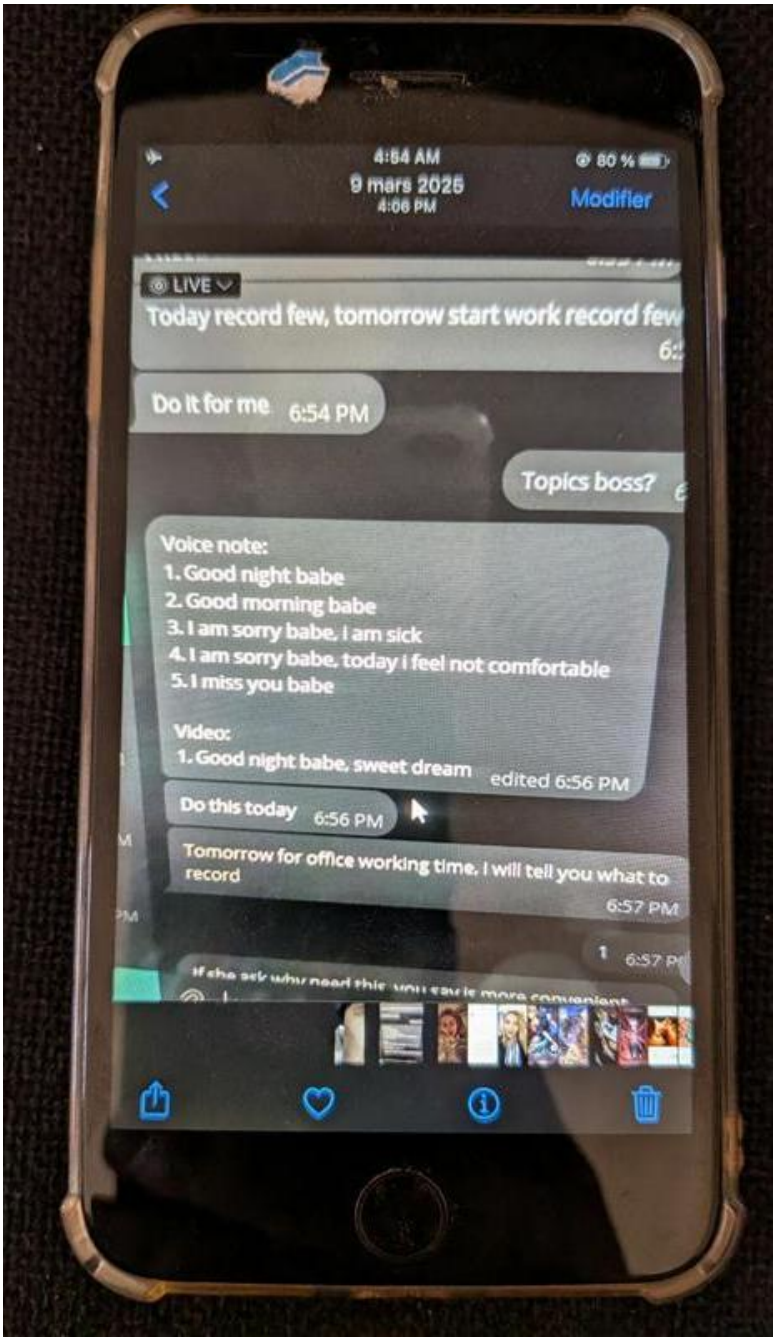


26. Further, at least one image was identified on Device 2 consistent with an apparent conversation between the scammer and a prospective victim, as follows.



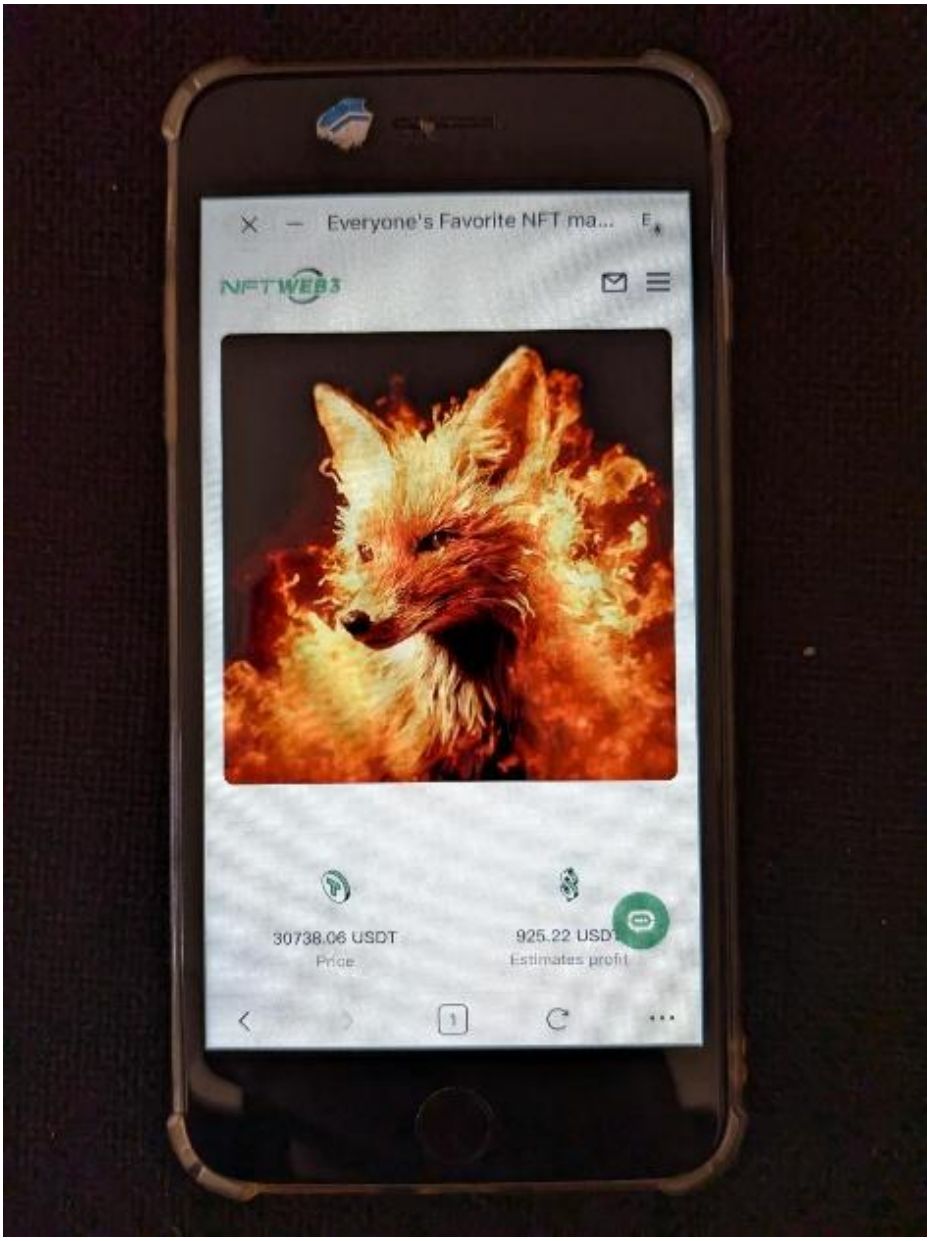
Use of Fake Personas

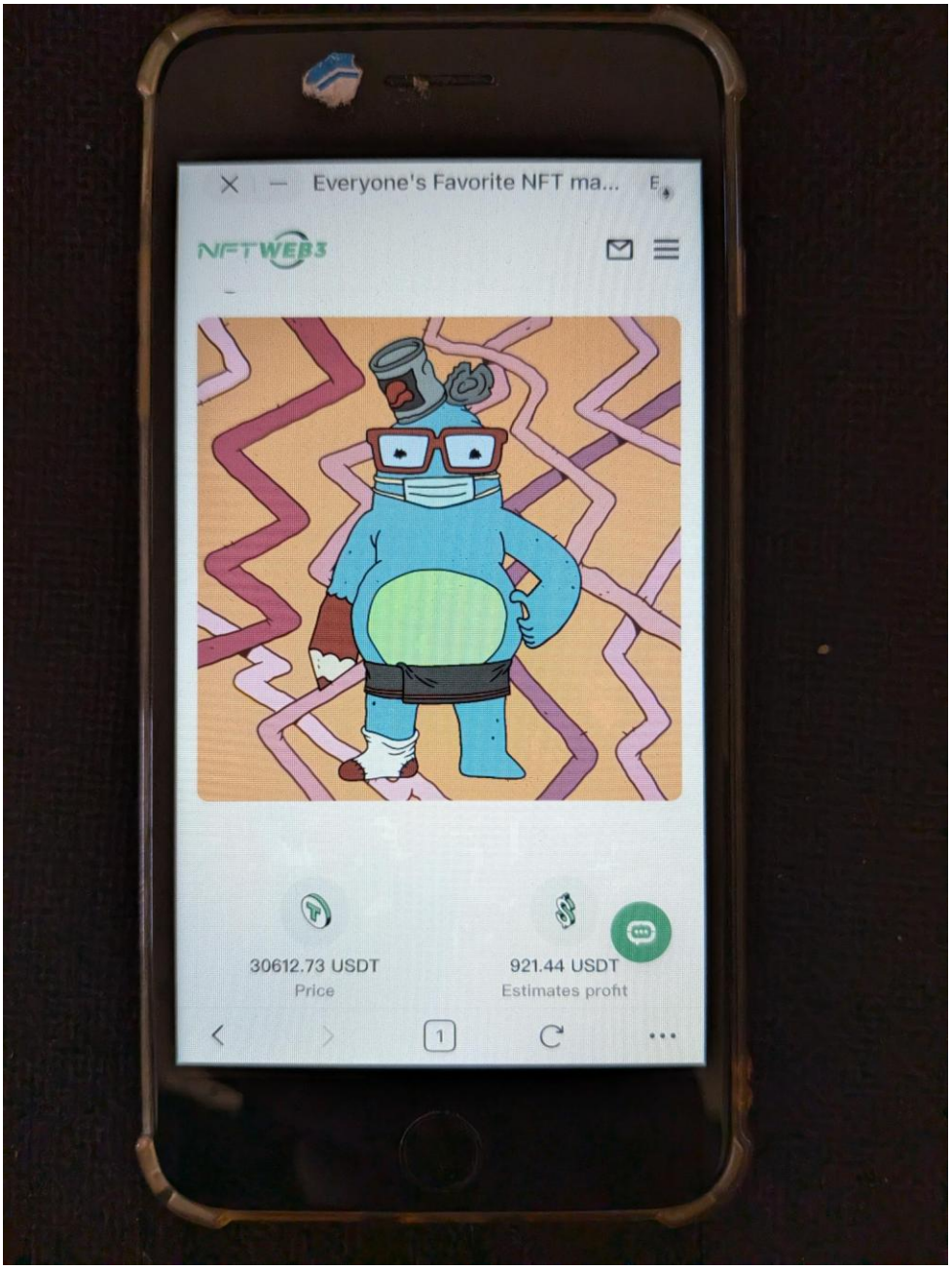
27. An image on Device 1 was located which appeared consistent with instructions provided to human models (i.e., fake personas of a real person) to perpetrate the scheme. Based on my training and experience, I know that oftentimes, these human models will create short video and/or audio clips to send to victims to increase the believability of the fraud scheme. An example follows.

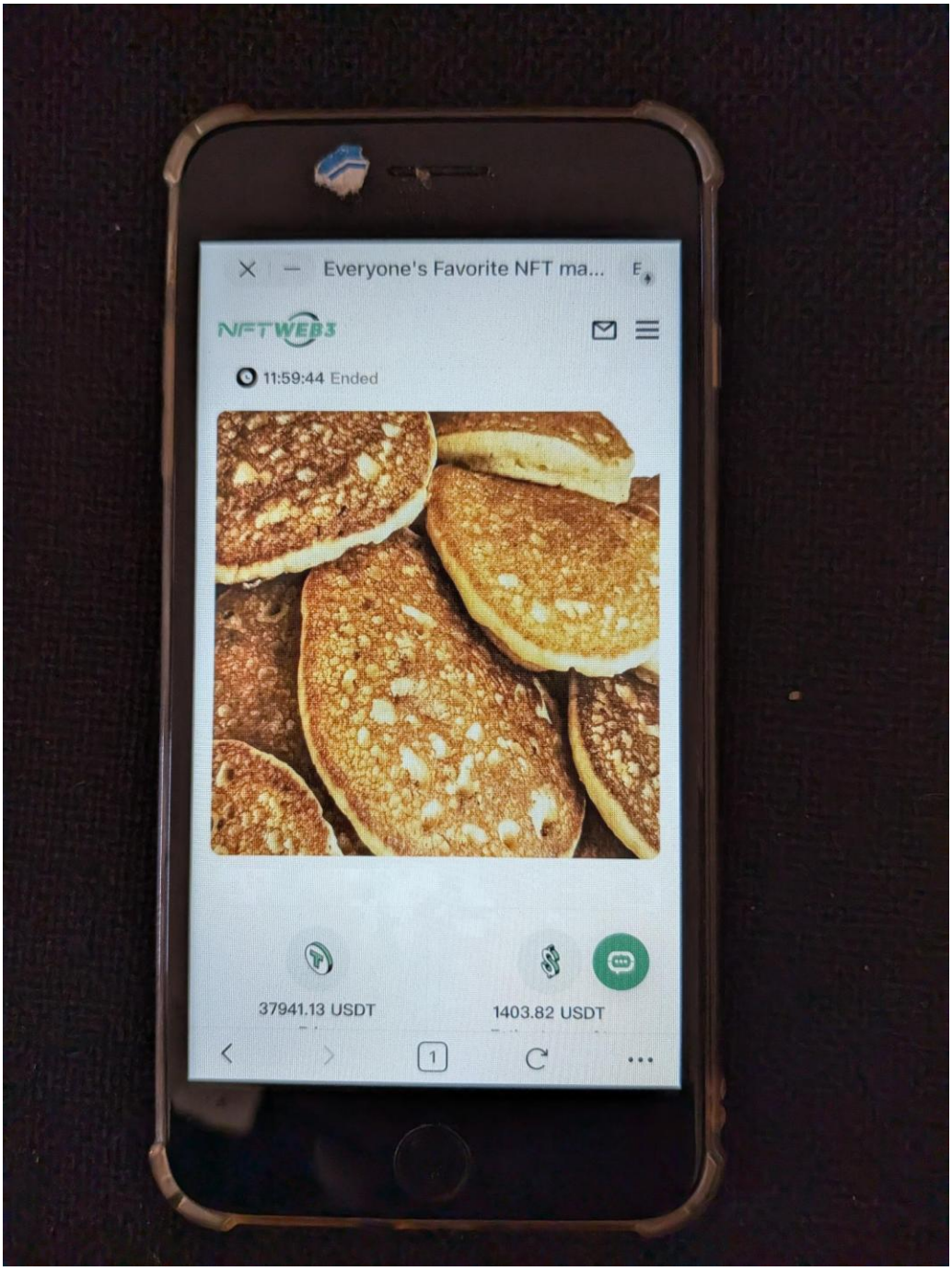


Use of Common Websites

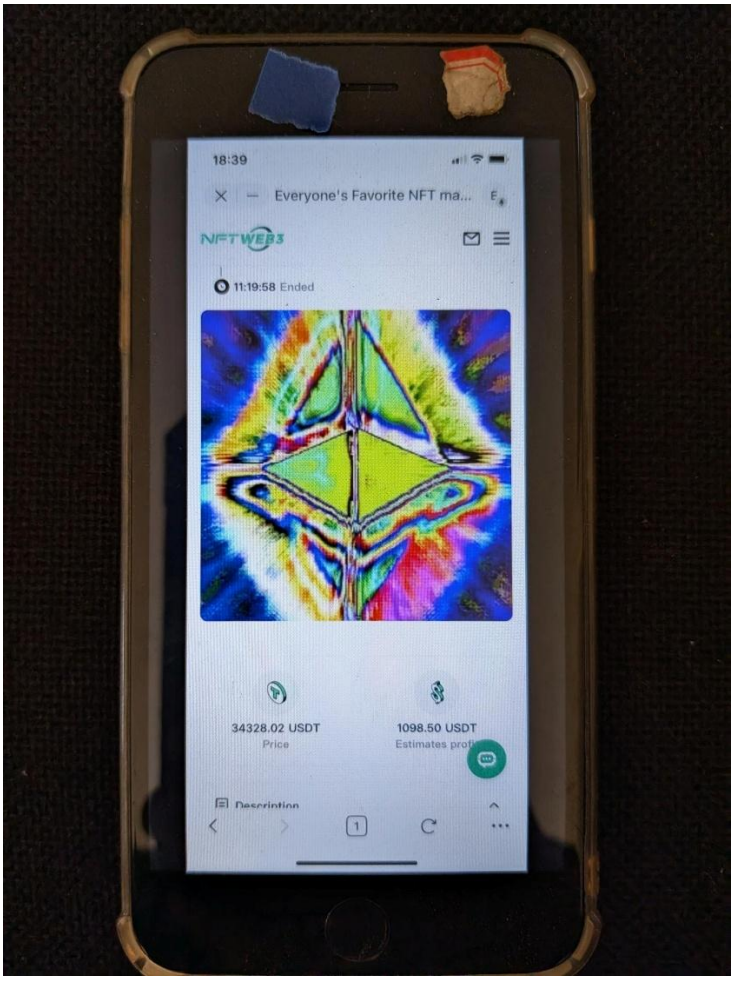
28. Through victim reporting, the FBI team had identified at least eight websites which appeared to be associated with the NFTWEB3 Scam (these websites were seized by prior order of this court, Case No. 26-sz-53, and incorporated here by reference). Found on Device 1 were at least three images were identified consistent with an apparent webpage which utilized the name "NFTWEB3," identified by multiple NFT Scheme victims, as follows.


Everyone's Favorite NFT ma...
NFTWEB3
30738.06 USDT
Price
925.22 USDT
Estimates profit


Everyone's Favorite NFT ma...
NFTWEB3
30612.73 USDT
Price
921.44 USDT
Estimates profit



29. Additionally, at least one image was identified on Device 2 consistent with an apparent webpage which utilized the name "NFTWEB3".

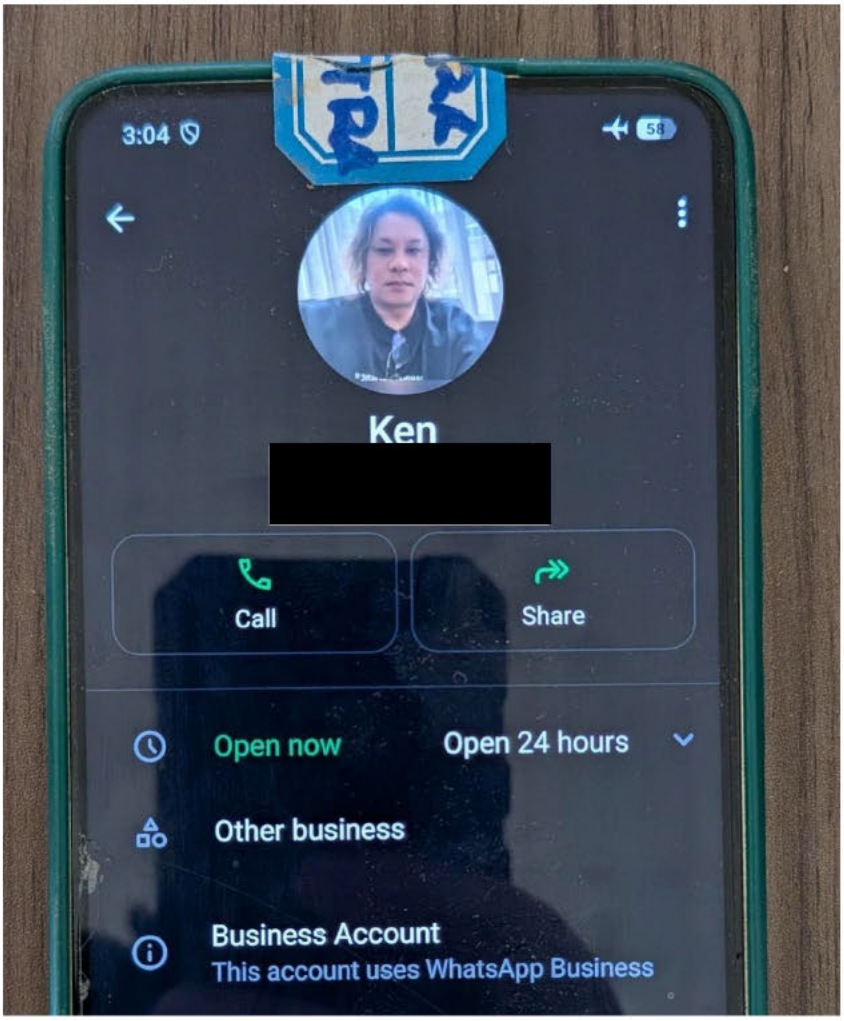


B. The Business Behind the NFTWEB3 Conspiracy

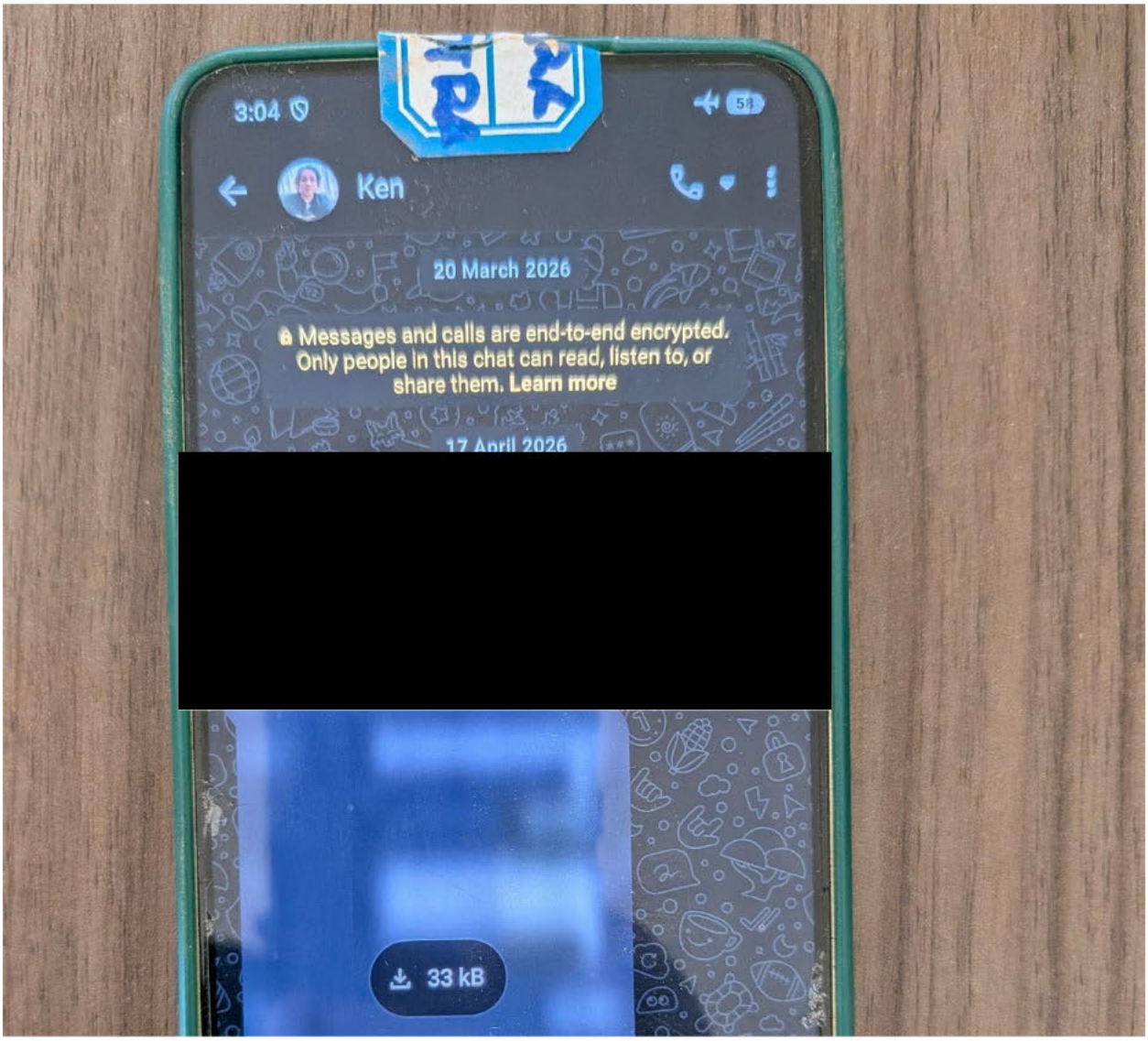
Identification of Defendant WA as a Leader and Boss

30. The MNP provided the FBI with two cellular devices, later attributed by your Affiant to a scam manager known as "Ken" (hereinafter, "KP1" (SN ending in FAG) and "KP2" (SN ending in FKX)).

31. Regarding KP1, the Google Drive application installed on KP1 had a pre-existing profile loaded for "Ken", email address [redacted] KP1 contained multiple WhatsApp messages to an account with a display name of "Ken", which was associated with telephone number [redacted] as shown below.



32. Also found on KP1 were multiple WhatsApp messages containing Tron Network cryptocurrency addresses, which were observed in the WhatsApp conversations between the WP1 phone and Ken. The first message appeared to have been sent around April 17, 2026, as shown below.



33. KP1's WhatsApp messages included the following Tron addresses sent and received with WP1:

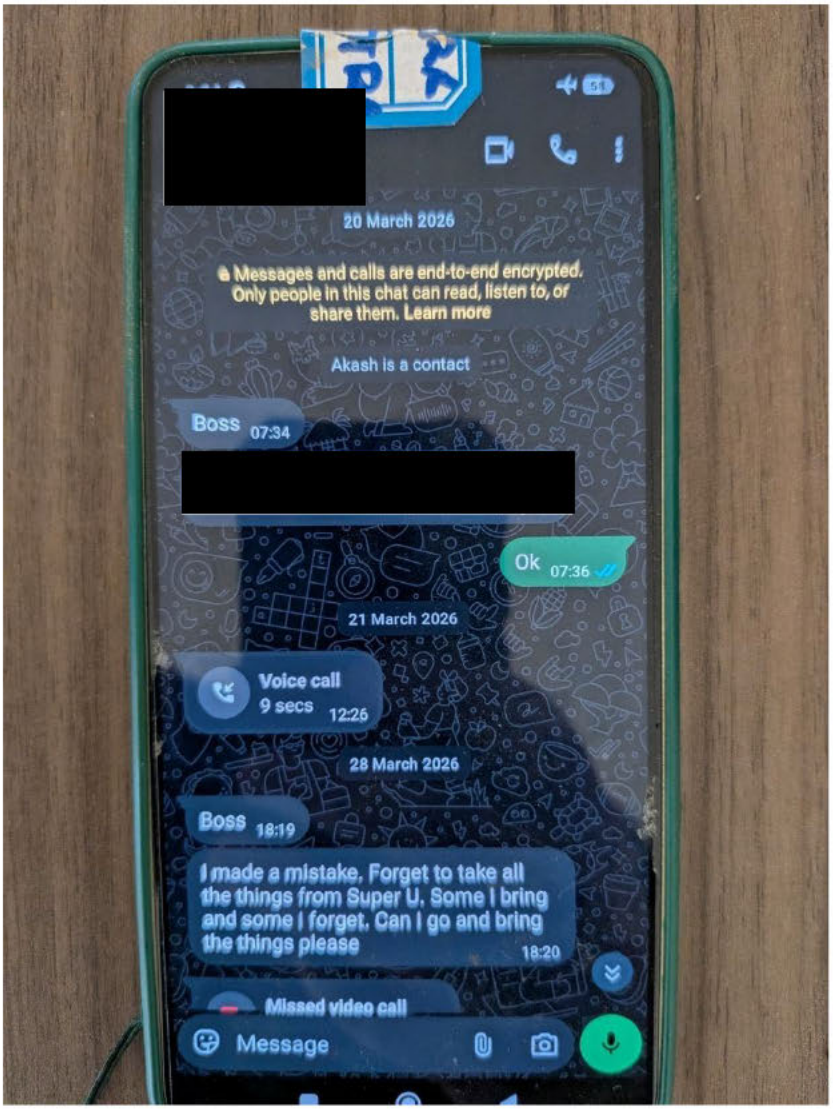
a. Sent by WP1 to "Ken"

[redacted]

b. Sent by "Ken" to WP1

[redacted]

34. Further, KP1's WhatsApp messages also included messages between Ken and an account with display name "Akash". Akash referred to the user of WhatsApp account on KP1 (presumably Ken) as "Boss" and sent a cryptocurrency addresses.



35. Open-source research of blockchain data revealed the cryptocurrency addresses provided by Akash, [redacted] received two transactions on March 20, 2026, the same day Akash sent the address. [redacted] received 339.85 USDt on 03/20/2026 05:09 UTC from an address attributed to

Binance.com. [redacted] then received 5,000 USDt on 03/20/2026 05:12 UTC from an address attributed to Binance.com.

36. Binance business records show that the aforementioned transactions to [redacted] on March 20, 2026 were sourced from Binance account [redacted] (hereinafter, "WA Binance Account 1"). WA Binance Account 1 contained the following basic information:

a. Name: CHUI KOK WA

b. Nationality: MY (Malaysia)

c. Email: [redacted]

d. Malaysia Identity Card

i. Number: [redacted]

ii. Address: [redacted]

37. Regarding KP2, it was identified as an iPhone 17 Pro Max (SN ending in FKX and telephone number [redacted] KP2 contained images consistent with the visual appearance of CHUI KOK WA.



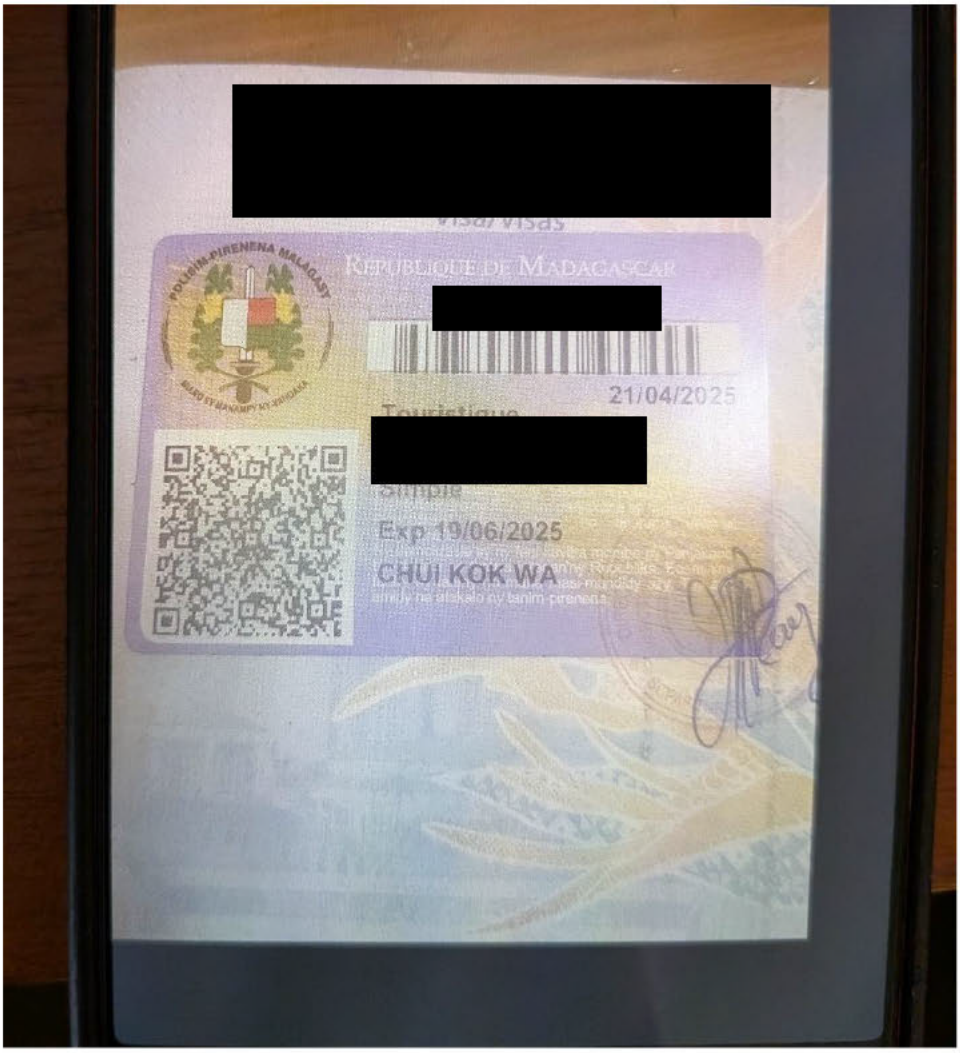
38. The browser history of KP2 contained multiple logs for Binance.com, Google.com, Facebook.com, and storibox.com. The Mail application on KP2 appeared to have been synced to the email address [redacted] the same email address associated with the Binance account registered to CHUI KOK WA.

39. In the device contacts for KP2, the contact card for the KP2 device was observed as "Ken K", and contained he following telephone numbers:

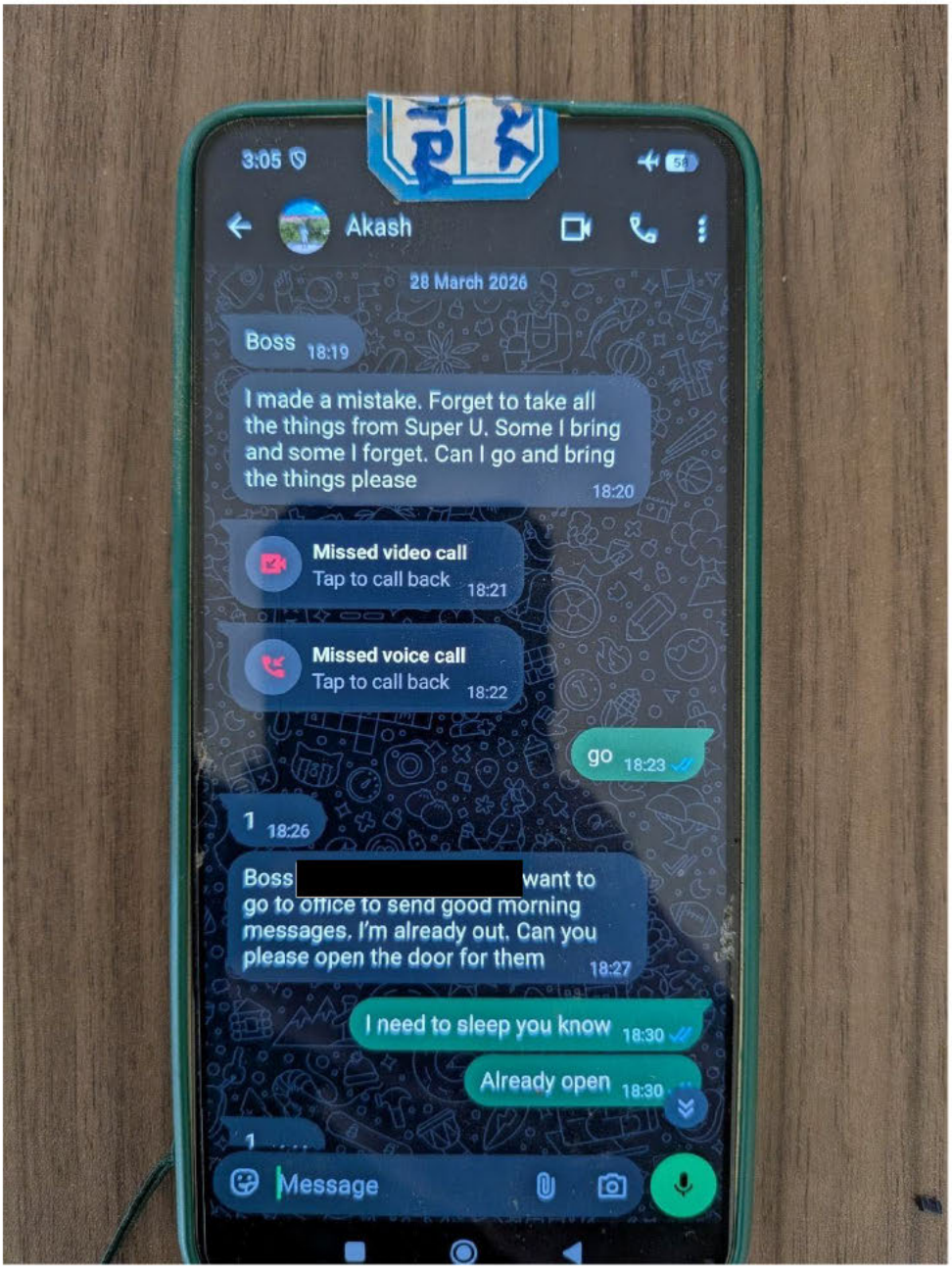
[redacted]

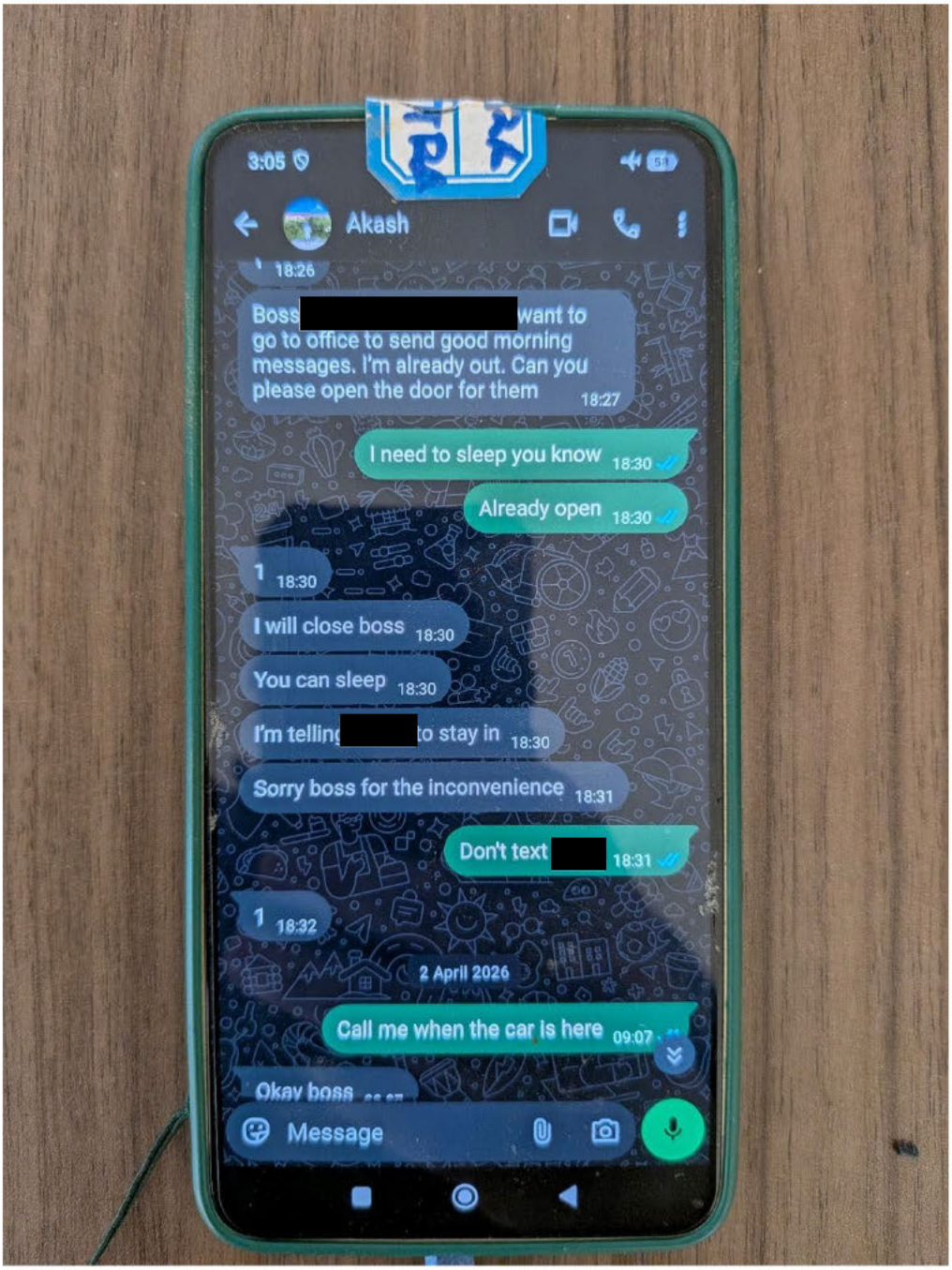
40. Photographs of travel documents for CHUI KOK WA were observed in the photo reel of KP2, to include a Malaysian Passport and Madagascar Visa:

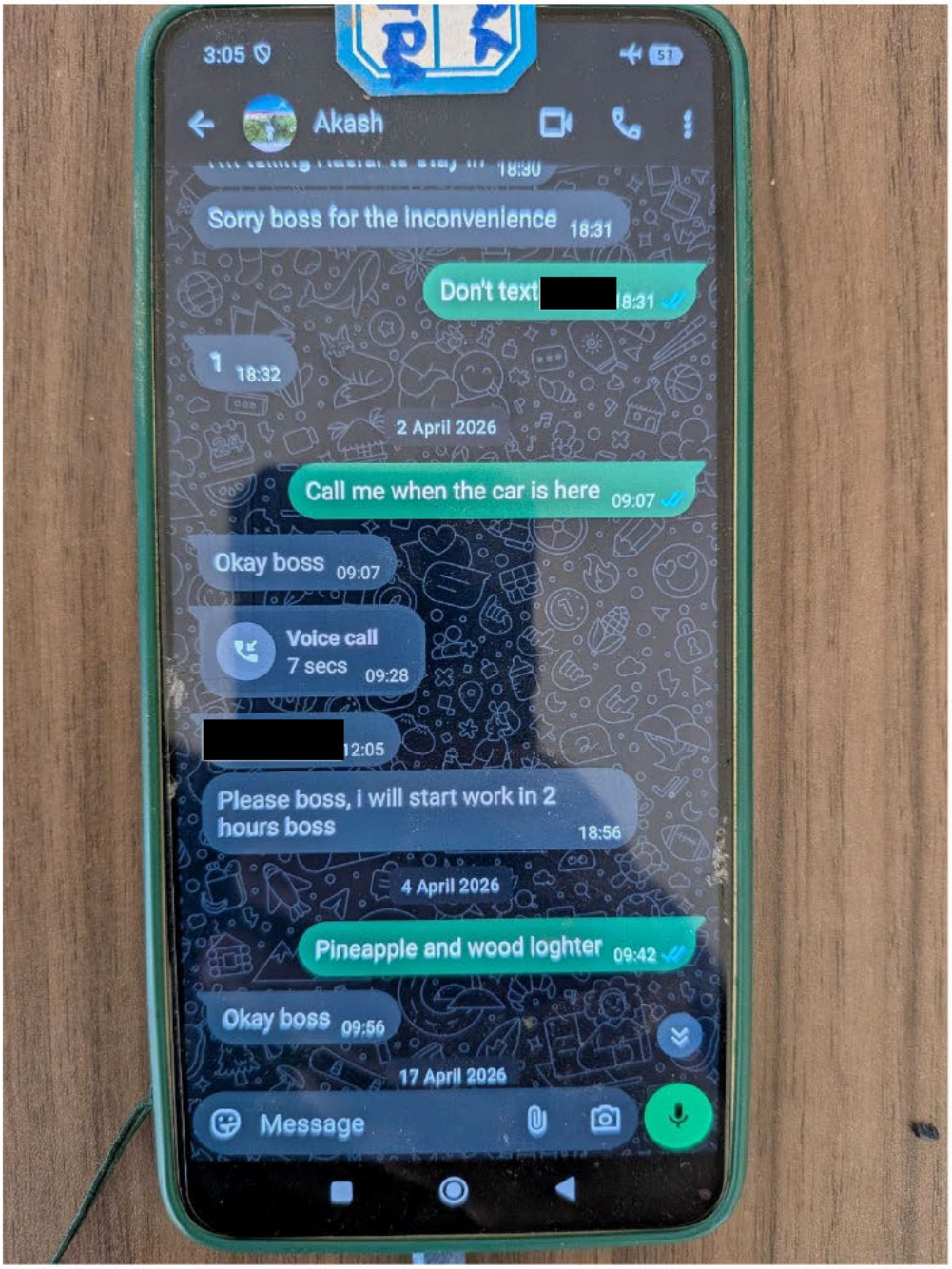

MALAYSIA
Pasport / Passport
Jenis / Type
P
Kod Negara / Country Code
MYS
[redacted]
Nama / Name
CHUI KOK WA
Warganegara / Nationality
MALAYSIA
[redacted]
No. Pengenalan / Identity No.
760112055295
[redacted]
Jantina / Sex
L-M
Tinggi / Height
173 cm
Tarikh Dikeluarkan / Date of Issue
10 MAY 2022
Tarikh Tamat / Date of Expiry
10 MAY 2027
Pejabat Pengeluar / Issuing Office
UTC KUALA LUMPUR
[redacted]
09:45
[Extended PB Secure

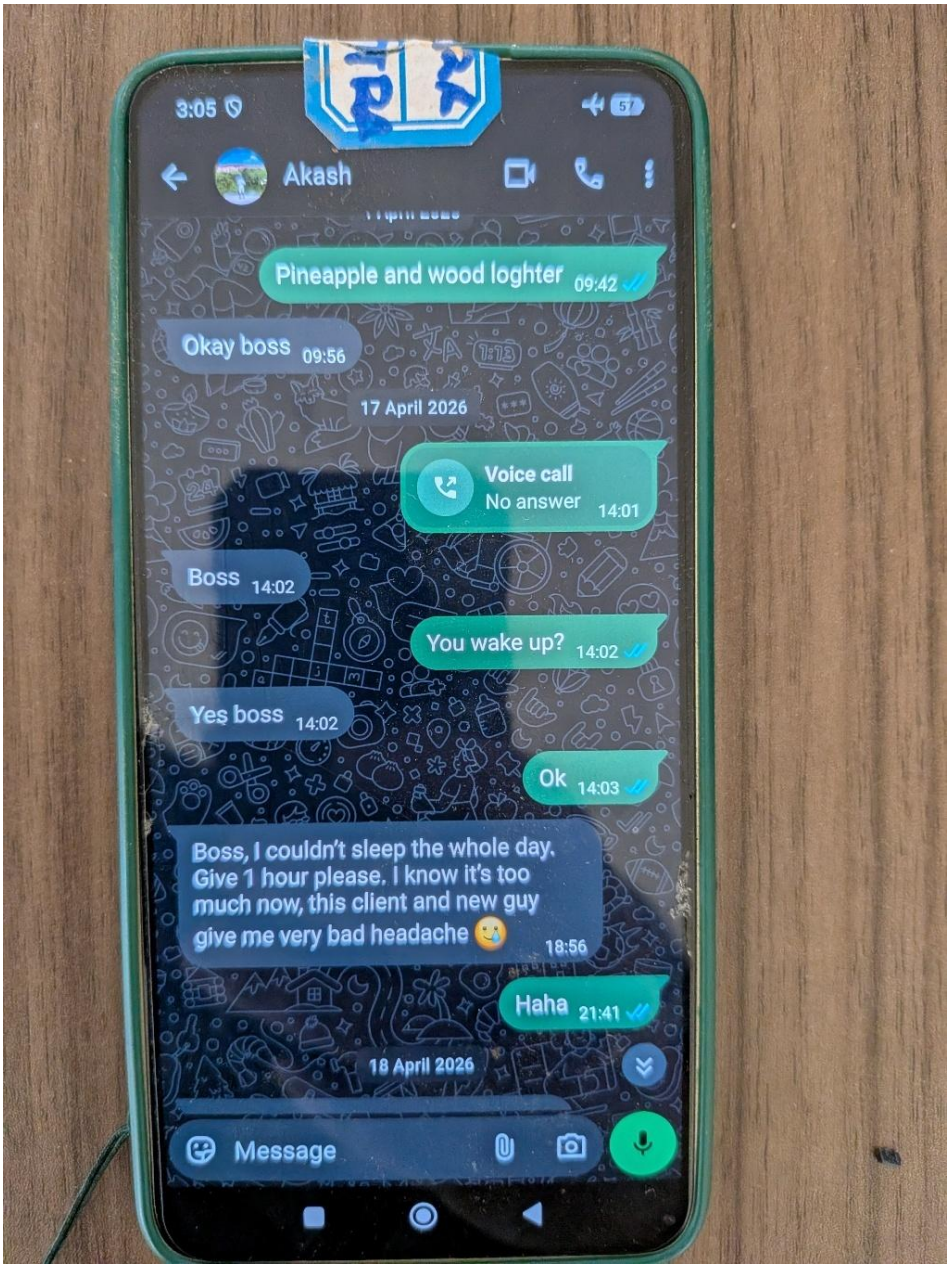


41. In addition to the above referenced use of the word "boss," messages between the WhatsApp account on KP1 (presumably Ken) and Akash indicate that Ken was in charge of an organization Akash was apart of, as shown in the following examples.


3:05
Akash
28 March 2026
Boss 18:19
I made a mistake. Forget to take all the things from Super U. Some I bring and some I forget. Can I go and bring the things please 18:20
Missed video call
Tap to call back 18:21
Missed voice call
Tap to call back 18:22
go 18:23
1 18:26
Boss [redacted] want to go to office to send good morning messages. I'm already out. Can you please open the door for them 18:27
I need to sleep you know 18:30
Already open 18:30
Message


3:05
Akash
18:26
Boss [redacted] want to go to office to send good morning messages. I'm already out. Can you please open the door for them 18:27
I need to sleep you know 18:30
Already open 18:30
1 18:30
I will close boss 18:30
You can sleep 18:30
I'm telling [redacted] to stay in 18:30
Sorry boss for the inconvenience 18:31
Don't text [redacted] 18:31
1 18:32
2 April 2026
Call me when the car is here 09:07
Okay boss
Message


3:05
Akash
Sorry boss for the inconvenience 18:31
Don't text [redacted] 8:31
1 18:32
2 April 2026
Call me when the car is here 09:07
Okay boss 09:07
Voice call
7 secs 09:28
[redacted] 12:05
Please boss, i will start work in 2 hours boss 18:56
4 April 2026
Pineapple and wood loghter 09:42
Okay boss 09:56
17 April 2026
Message



42. Finally, information within KP1 showed that Defendant WA was located in Madagascar during relevant time periods. For instance, a travel itinerary was identified on KP1, which indicated Defendant WA had scheduled a flight path initiating in Dubai and arriving in Antananarivo, Madagascar on December 27, 2024.

43. Additional business records of Binance showed access logs for WA Binance Account 1 indicated WA had login activity in the United Arab Emirates on/around December 25,

2024; as well as login activity in Antananarivo, Madagascar, on/around January 1, 2025, as follows:

Geolocation	Timestamp (UTC)	Real IP	Operation
Madagascar Antananarivo	2025-01-08 05:20:07	102.17.118.166	Renew login state
Madagascar Antananarivo	2025-01-08 05:19:54	102.17.118.166	Renew login state
Madagascar Antananarivo	2025-01-01 05:15:56	102.17.255.173	Renew login state
Madagascar Antananarivo	2025-01-01 05:15:46	102.17.255.173	Renew login state
Madagascar Antananarivo	2025-01-01 05:15:38	102.17.255.173	Renew login state
Madagascar Antananarivo	2025-01-01 05:15:19	102.17.255.173	Renew login state
United Arab Emirates Dubai	2024-12-25 14:22:38	5.31.183.112	User modifies settings
AE Dubai	2024-12-25 14:20:28	5.31.210.240	Withdrawal application
AE Dubai	2024-12-25 14:20:03	5.31.210.240	Withdrawal application
AE Dubai	2024-12-25 14:20:03	5.31.210.240	security check before withdraw
AE Dubai	2024-12-25 14:20:02	5.31.210.240	提现popup
AE Dubai	2024-12-25 14:19:16	5.31.210.240	Withdrawal risk control verification
AE Dubai	2024-12-25 14:19:04	5.31.210.240	User modifies settings

Organization and Management of the Conspiracy by Defendant WA

44. Information discovered on devices associated with Defendant WA (KP1 and KP2), show that WA was the leader and manager of approximately 20 or more workers who were involved in scamming related to the NFTWEB3 Scam.

45. First, KP1 included a version of a contract that, based on my training and experience, was a contract sent by Defendant WA to scam line operators.[8] A file named "员工薪

[8] I know based on my training and experience in this and other cases, and based on wide public reporting, that scam workers are often physically abused if they do not meet targets for scamming. In the FBI Team's review of Device 1, an image was located on the device which appeared consistent with the marks inflicted by an electric taser or electric cattle-prod device. The image appeared to have a creation date of March 6, 2025.

资Expatriate_Staff_Contract.docx" was found on KP1. (Based on a machine translation, 员工薪资 translates from Mandarin Chinese to "Employee Salaries" in English). Based on my technical background, I believe that the file path for the document is consistent with it being used in the Telegram application. When opened as a Microsoft word document, the file appeared to be an employment contract. Based on your Affiant's training and experience, the file is consistent with employment contracts presented to scam compound line workers. Multiple items consistent with scam line worker contracts are present, to include financial penalties for not acquiring new "client(s)" (victims), and providing the workers passport to the company for "temporary custody". Moreover, the hours of the contract are late day to overnight in Madagascar (7:00pm to 7:00am), and consistent with day-time to evening work in the United States (Madagascar is 7 or 8 hours ahead of the Eastern Time Zone of the United States, depending on daylight savings). Based on my training and experience in this and other cases, scammers typically work overnight hours to align with the time zones of their intended victims. An image of the contract follows.

Further, on or about October 22, 2026, FBI was made aware of a report authored by eight Madagascar attorneys (hereinafter, the "Attorney Report") in which the attorneys stated that they represented twenty-five African nationals in custody in Antananarivo, Madagascar. The Attorney Report claimed that the twenty-five individuals were employees of WA, and further that they had responded to employment advertisements on social media for work in Madagascar. The Attorney Report further stated that the individuals claimed that, after they arrived for these jobs, WA engaged in acts of abuse and intimidation, and refused to let them leave. The FBI has been unable to speak to any of WA's employees, held in Madagascar, despite requests to the Malagasy authorities, and has been unable to substantiate these claims. None of the 25 individuals are included as defendants in this or related affidavits.

However, your Affiant also notes that conduct of many of these individuals, of which your Affiant is aware, is potentially inconsistent with claims of duress. For instance, certain individuals traveled from Cambodia (rather than from their home countries) to Madagascar and engaged in prior conduct consistent with scam activity in Cambodia. Other individuals regularly and frequently checked their Binance accounts for status of their pay. All of WA's employees appear to have been paid through cryptocurrency wallets for which each employee had to register with Binance. Based on your Affiant's experience in other scam compound investigations, scam compound victims are not typically paid and are not permitted to maintain individual accounts with a virtual currency exchange.

Employment Contract

1. **Working hours**
Working hours: 19:00 p.m to 07:00 a.m daily, break time: 12:00 am to 01:00 am daily.

2. **Salary system**

The basic salary and commissions are based on the number of recharge clients and the recharge amount in a month (Based on the monthly deadline). Monthly salary and commissions will be paid on the 15th of the following month.

Commissions:
Monthly performance of 100,000 USDT and above earns a 6% commission.
Monthly performance between 50,000 USDT - 99,999 USDT earns a 5% commission.
Monthly performance between 30,000 USDT - 49,999 USDT earns a 4% commission.
Monthly performance between 15,000 USDT - 29,999 USDT earns a 3% commission.

Basic salary: 800 USD
I. To qualify for the 800 USD basic salary, you must either acquire at least 1 new client with a total recharge of 3,000 USDT and above within the month or acquire at least 2 new clients, each with a total recharge of 500 USDT and above within the month.

II. If you acquire only 1 new recharge client within the month and the recharge amount is less than 3,000 USDT, 100 USD will be deducted from the basic salary.

III. If you don't get any new recharge client within the month, 200 USD will be deducted from the basic salary.

IV. If you don't get any new recharge client for consecutive two months,, 500 USD will be deducted from the basic salary. The company might consider dismissing you. If company decided to dismiss you, the company won't bear the cost for you to leave the country (Including but not limited to flight ticket).

Monthly Bonus Rewards Program
i. For acquiring 3 recharge clients who each recharge 500 USDT and above within the month, you will receive a reward of 50 USD.

ii. For acquiring 4 recharge clients who each recharge 500 USDT and above within the month, you will receive a reward of 100 USD.

iii. For acquiring 6 recharge clients who each recharge 500 USDT and above within the month, you will receive a reward of 200 USD.

iv. For acquiring 8 recharge clients who each recharge 500 USDT and above within the month, you will receive a reward of 500 USD.

Note: Recharge client must meet the company's minimum qualification standards. Only new recharged clients who have accumulated recharge amount of 500 USDT and above within the month can be included in the monthly bonus reward program.

3. Resignation
I. If you wish to resign, you must give the company 30 days' notice. If you resign before the end of your contract, you must reimburse the company for the cost of your flight and visa.

II. After you submit resignation request, if you do not cooperate with the company during the period of stay, violating any of the company's rules and regulations, or having a negative attitude towards the work, company will have the right not to pay for your remaining salary & commissions of the month.

4. Off day
I. Every Sunday you have the first half of the day off and work the second half of the day. No payroll deduction for half days off.
II. The company will arrange a driver to pick up and drop off, you can't go out or come back alone, violator are directly dismissed.

5. Dismissal
I. The company does not cover the return airfare for those who are dismissed; the employee is responsible for that.

6. Contract duration
I. 1 year

7. Due to the nature of the work, the company reserves the right to inspect the contents of your personal mobile phone. Failure to cooperate will result in immediate dismissal, with all wages and bonuses forfeited.

I am willing to hand over my passport to the company for temporary custody on the period of working in the company.

Please read & understand all of the statements as above. By signing this contract, you are acknowledge and agree to all of the statements as above.

Passport Number:

Passport Name:

Contact Number:

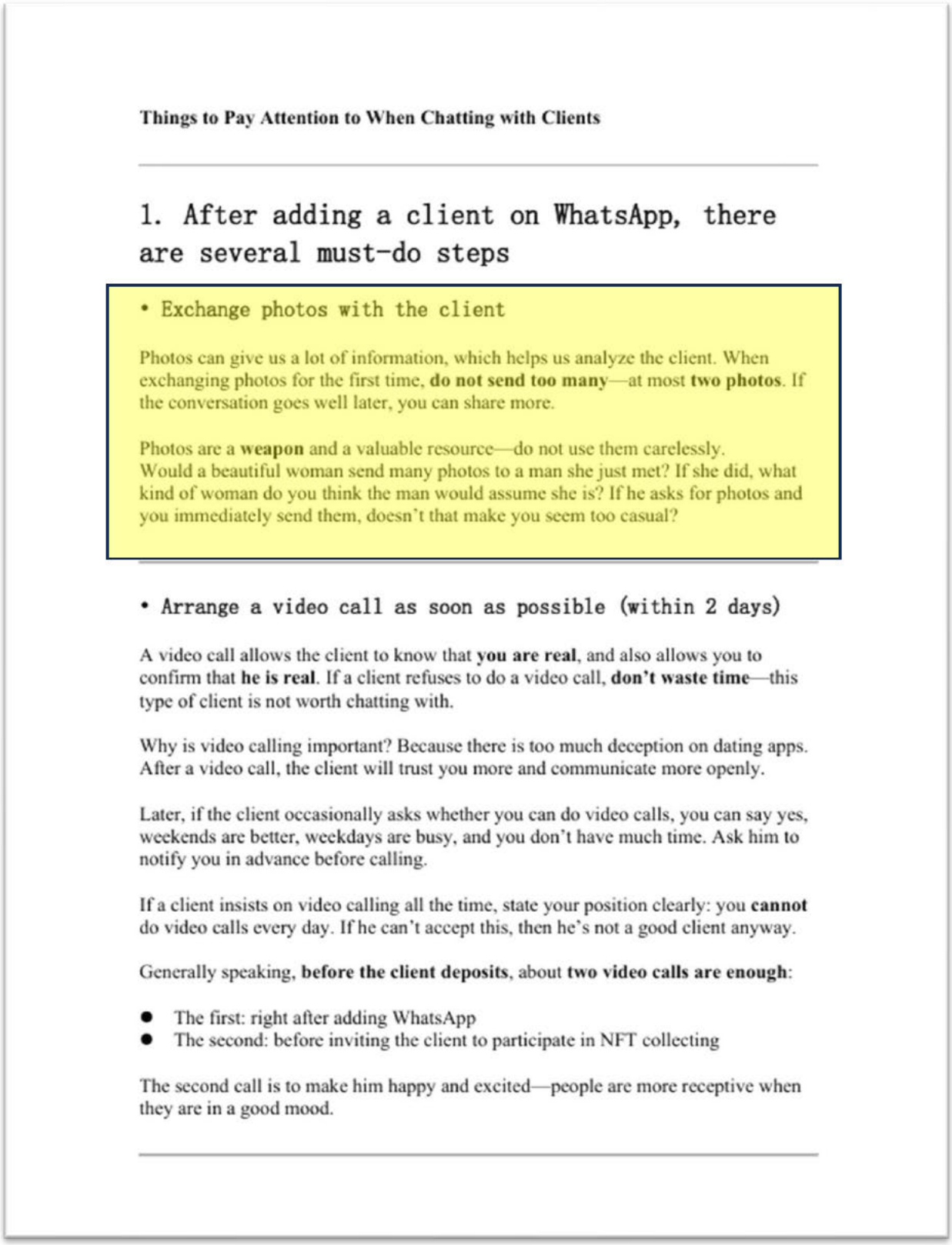
Date:

46. Based on my training and experience, word documents often contain valuable information in the underlying Extensible Markup Language (XML) files, which when combined, constitute many standard Microsoft Word file extensions, to include ".docx". Two XML files of investigative interest were identified relevant to the contract above, which showed that the file named "员工薪资Expatriate_Staff_Contract.docx" was originally created utilizing the WPS Office application, and the most recent modification occurred by a user named "Falla Dorothea".

47. A WhatsApp message sent by KP1 on March 22, 2026, to another WhatsApp user contained the email address [redacted]. The email address appears to be under the control of Defendant WA, as it was provided to assist the counterparty create a Telegram account, and the KP1 WhatsApp account provided a six-digit code to the counterparty shortly after sending the email address, indicating the KP1 WhatsApp account owner likely controlled the email address. A review of the chat history contained messages indicating the counterparty referred to the KP1 WhatsApp account as "boss", as well as chats pertaining to apparent strategy on scamming three separate likely victims named [redacted]

48. Second, KP1's devices contained documents consistent with direction scripts and advice about how to defraud victims. For instance, KP1 contained a document named "4_592937492391396103 6.doc," which appeared to your Affiant, based on training and experience, to contain a guide on how to socially engineer victims (described as "clients"). This file was found on KP1, with a file path which is consistent with the Telegram application. The file "4_592937492391396103 6.doc" was originally created utilizing the WPS Office application and was created and last modified by [redacted] A copy follows (with highlights added by the Affiant). As stated in the document below, the scammers were instructed to communicate with

their victims through WhatsApp, which is an encrypted messaging service owned and operated by Meta, a U.S. company.



Things to Pay Attention to When Chatting with Clients

1. After adding a client on WhatsApp, there are several must-do steps

• Exchange photos with the client

Photos can give us a lot of information, which helps us analyze the client. When exchanging photos for the first time, **do not send too many**—at most **two photos**. If the conversation goes well later, you can share more.

Photos are a **weapon** and a valuable resource—do not use them carelessly.
Would a beautiful woman send many photos to a man she just met? If she did, what kind of woman do you think the man would assume she is? If he asks for photos and you immediately send them, doesn't that make you seem too casual?

• Arrange a video call as soon as possible (within 2 days)

A video call allows the client to know that **you are real**, and also allows you to confirm that **he is real**. If a client refuses to do a video call, **don't waste time**—this type of client is not worth chatting with.

Why is video calling important? Because there is too much deception on dating apps. After a video call, the client will trust you more and communicate more openly.

Later, if the client occasionally asks whether you can do video calls, you can say yes, weekends are better, weekdays are busy, and you don't have much time. Ask him to notify you in advance before calling.

If a client insists on video calling all the time, state your position clearly: you **cannot** do video calls every day. If he can't accept this, then he's not a good client anyway.

Generally speaking, **before the client deposits**, about **two video calls are enough**:

- The first: right after adding WhatsApp
- The second: before inviting the client to participate in NFT collecting

The second call is to make him happy and excited—people are more receptive when they are in a good mood.

• Ask clearly what the client' s purpose is on the dating app

If his purpose doesn't match yours—for example, if he's only looking for a one-night stand—then there's no need to continue chatting.

Only when your goals align does it make sense to continue, because you're both looking for a **long-term, stable relationship**.
You may say that just being friends is also possible—if you believe that as friends you can still later persuade him to participate in NFT collecting, then you may try.

What we are doing is an **emotional scam**, using the client's feelings for us to get him to invest.

• Ask about the client' s experiences on dating apps

Even if you've already asked on the dating app, ask again on WhatsApp. You can ask whether he has met someone he liked, or whether he has encountered bad women.

If the client tells you he has been scammed before, don't panic. Ask what exactly happened. As long as the scam **was not related to NFTs**, you can still continue chatting.

If the client was scammed due to **cryptocurrency**, you should consider stopping. When you later bring up NFTs, these clients are usually very defensive and hard to convince.

Rather than spending more time and energy on such clients, it's better to focus on those who haven't been scammed. Also, knowing this early helps you decide whether to continue—otherwise, if you only find out at the deposit stage, you've wasted a lot of time.

---

2. Chats must feel real

If they don't, the client won't believe you. Don't naïvely assume clients are stupid.

Some clients notice when you say something wrong, send the wrong picture, repeat conversations, or resend the same photos—but they don't point it out. They're just observing what you'll do next and watching your performance.

How to increase authenticity:

- Don't avoid sensitive questions.
  For example, if a client asks why you're looking for a boyfriend in one city while working in New York, explain your real intention.

- Don't be afraid that the client might want to meet you in person. Just think of a reasonable excuse to deflect it.

• Use photos wisely during chats

Occasionally send photos—especially of food, cooking, or exercising. Learn to use photos, but don't send them randomly.

If a conversation is all text, isn't it tiring and boring?
When sending photos, pay attention to details:

- Dates shown in photos
- License plates
- Seasons (don't send a sweater photo in summer)

• Let the client understand your daily life

Talk about going to work, getting off work, weekends, and what you do after work.

Be specific and real.
For example, if the client asks what you're doing, say something like:
"I'm reading a book—*Atomic Habits*,"
not just:
"I'm not doing much, just relaxing."

• Remember what you talked about

This is one purpose of making reports. If you asked something yesterday and then ask the same question again the next day because you forgot, the client may think:

- You're chatting with many men at the same time
- You're not paying attention to what he says
- This makes him feel you're not taking him seriously.

---

3. Don' t keep asking questions nonstop

You're not a police officer or a journalist. Share your own experiences and feelings first, then ask questions.

Of course, we want more information from the client, but that should come from **patient conversation**, not constant questioning. Otherwise, the client will feel the chat is boring.

If a client chats well at the beginning but disappears after two or three days, it's usually because **your conversation is too boring**, and he has lost interest.

---

4. Use emojis and GIFs appropriately

They can make chats more fun, but don't overuse them. Don't let your entire chat history be full of emojis.

---

5. Progress from light topics to deeper ones

Make the client feel that chatting with you is interesting—that you are understanding, humorous, and thoughtful.

---

6. Do not engage in sexual topics

If the client starts talking about sex, stop him and clearly state your position. We do **not** use sexual topics to attract clients.

Even flirting should only happen **after confirming the relationship** or **after the client has deposited**, and only in moderation.



7. Go deep, don’ t stay on the surface

When chatting with clients, don’t just skim topics—learn to **extend and develop conversations**.
Refer to the document *“Topics You Can Chat About with Clients.”*

49. Additionally, a file named “emotional script.docx” was located on KP1. When opened as a word document, the file contained multiple paragraphs in English which appeared to be designed to illicit emotional responses, likely from prospective victims.

> ***‘When my husband was diagnosed with leukemia, it felt like my world shattered in an instant.*** *I still remember the look on his face when the doctor said the words.* ***He was trying to stay strong, but I could see the fear in his eyes.*** *In that moment, I made a silent promise to myself that I would do everything in my power to fight for him to fight for us, for our family.’*
>
> ***‘The next few months became a whirlwind of hospital visits, treatments, and sleepless nights.*** *We were honest with each other through it all our hopes, our fears, and even the possibility of losing.* ***He often told me how much he worried about leaving me and our daughter behind, and I would assure him that I would keep fighting, no matter what it took.’***

50. An additional file named “DAY 1-5 (51)First part Notes.docx” was located on KP1. When opened as a word document, the file contained a five-page document with multiple paragraphs in English which appeared to be a guide on initial victim interaction.

Purpose of day 5 - Share entrepreneurship experience

Brief a bit about entrepreneurship journey and how you approach business and investments. Talk about the import and export trading company. How tough it was and the hard work and dedication, to make the business eventually succeeded. Also ask for their entrepreneurship experiences so as to note thee customers weaknesses

Then talk about the Western restaurant how you invested in shares. The success of this venture demonstrated how careful planning and smart investments can pay off.

Talk about how the pandemic in 2020 was a test of resilience. How your import and export business went down, and how the stable income from cryptocurrency DeFi liquidity mining helped you stay afloat.

Brainwash customer in telling him how investment is important as compared to putting all eggs in one basket.

Ex: ''this taught me how important it is to have different ways to make money. From what I've learned, investing in various things—like stocks, real estate, restaurants, or cryptocurrencies—is essential. Don't put all your money into one place. Diversifying helps manage risk and can lead to more growth opportunities. I'm here to give advice and offer investment options, focusing on spreading out investments and making smart choices.

Also explain how knowledgeable you're in the field of business and cryptocurrency

Ex: ''Cryptocurrency DeFi not affected by any external forces like wars or pandemics''

51. Third, KP1's phone also contained a document that was indicative of an employment roster. The file was located in the recovery directory for an application called WPS Office[9], which is a free office suite application. The file, when opened as a spreadsheet, contained two tabs. The first tab contained columns such as Staff Name, Passport Name, Basic Salary, Discipline Fine, and Deduction for recharge customer not meeting target. The second tab was named "员工钱包地址", which was machine translated from Mandarin Chinese to "Employee

[9] https://www.wps.com/office/android/

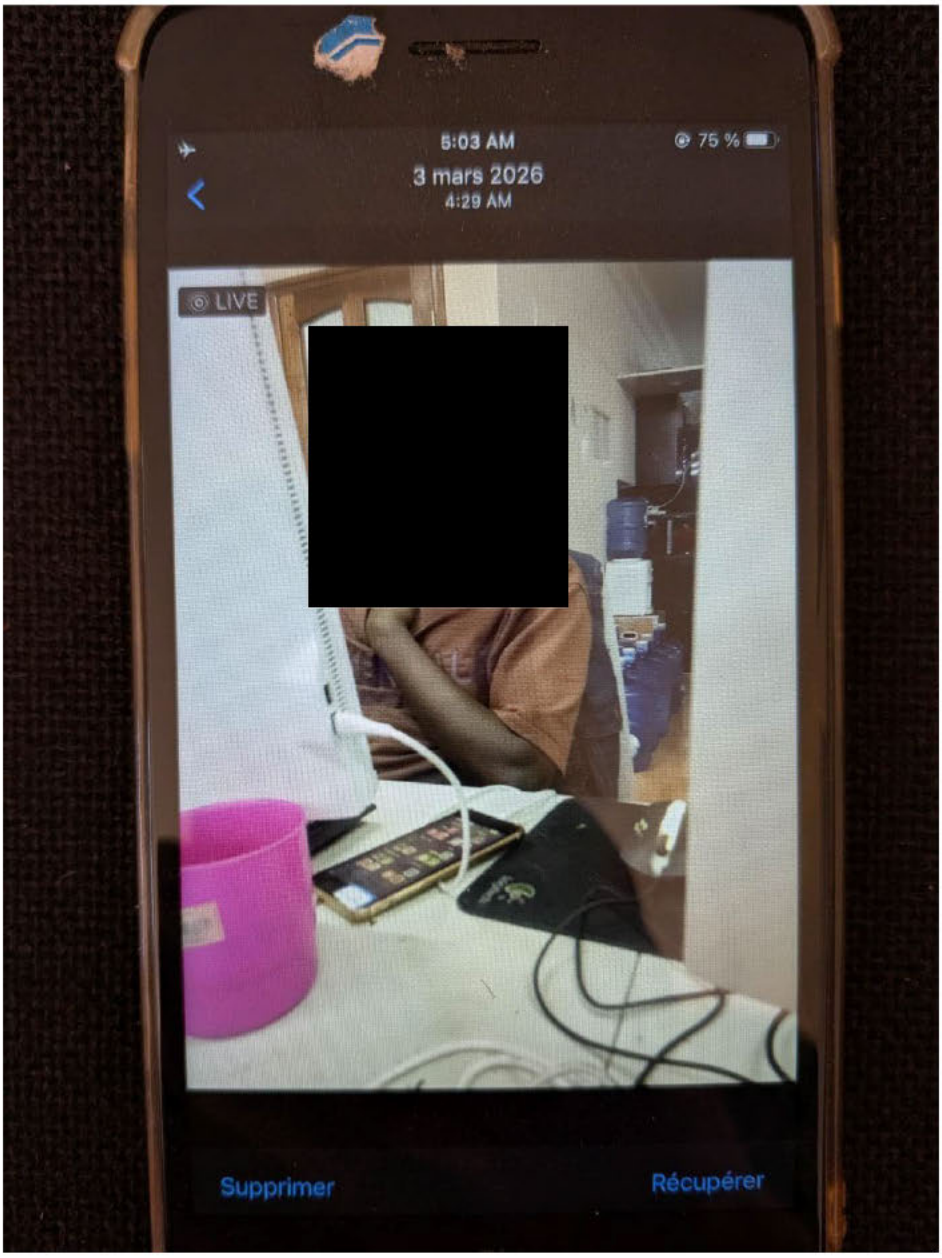
Salaries" in English. to English as "Employee wallet address" ,and contained columns with apparent names and cryptocurrency wallet addresses. As described further herein, the FBI team tied multiple entries on this employee roster to specific individuals who were further tied by to U.S. victims, who reported being defrauded by the NFTWEB3 Scam. The titles for each column were displayed in Mandarin Chinese.

No	员工名字	护照名字	基本薪资	工作天数	薪资净额	纪律罚款	充值客户数	充值客户数达标奖励	充值客户数未达标扣款
	Staff Name	Passport Name	Basic Salary	Working Days	Net Salary	Dicipline Fine	No Of Recharge	Reward For No Of Recharge	Deduction for recharge customer not meeting target
1	[redacted]		800	31	800.00	0.00	0	0.00	0.00
2			800	31	800.00	0.00	2	0.00	0.00
3			800	31	800.00	0.00	1	0.00	0.00
4			800	31	800.00	0.00	1	0.00	100.00
5			800	31	800.00	0.00	1	0.00	0.00
6			800	31	800.00	0.00	1	0.00	100.00
7			800	31	800.00	0.00	0	0.00	200.00
8			800	31	800.00	0.00	0	0.00	500.00
9			800	31	800.00	0.00	0	0.00	200.00
					7200.00	0.00	6	0.00	1100.00
10			800	31	800.00	0.00	0	0.00	0.00
11			800	31	800.00	0.00	0	0.00	200.00
12			800	31	800.00	0.00	0	0.00	200.00
13			800	31	800.00	0.00	1	0.00	0.00
14			800	31	800.00	0.00	0	0.00	200.00
15			800	31	800.00	0.00	1	0.00	100.00
16			800	31	800.00	0.00	0	0.00	200.00
17			800	31	800.00	0.00	0	0.00	200.00
18			800	29	748.39	0.00	0	0.00	200.00
					7148.39	0.00	2	0.00	1300.00
19			800	31	800.00	0.00	0	0.00	0.00
20			800	31	800.00	0.00	1	0.00	100.00
21			800	31	800.00	0.00	0	0.00	200.00
22			800	31	800.00	0.00	0	0.00	500.00
23			800	31	800.00	0.00	0	0.00	500.00
24			800	31	800.00	0.00	1	0.00	100.00
25			800	31	800.00	0.00	1	0.00	
26			800	31	800.00	0.00	0	0.00	200.00
27									
		sub total			6400.00	0.00	3	0.00	1600.00
		Total			20748.39	0.00	11	0.00	4000.00

充值业绩	业绩提成	预支/欠账	机票储备金	换取本地货币	总计	备注
Total Recharge Amount	Commissions	Advance/Debt	Air ticket reserve fund	Change local curreny	Total	Remarks
9338.66	0.00	0.00	100.00	0.00	700.00	Reserve Air Ticket Funds:400
4751.48	0.00	0.00	100.00	0.00	700.00	Reserve Air Ticket Funds:300
11272.02	0.00	0.00	100.00	30.00	670.00	Reserve Air Ticket Funds:300
558.37	0.00	0.00	100.00	0.00	600.00	Reserve Air Ticket Funds:300
57311.78	2865.59	0.00	100.00	0.00	3565.59	Reserve Air Ticket Funds:300
-8.17	0.00	0.00	100.00	0.00	600.00	Reserve Air Ticket Funds: 200
37825.68	1513.03	0.00	100.00	0.00	2013.03	Reserve Air Ticket Funds: 200
0.00	0.00	0.00	100.00	0.00	200.00	Reserve Air Ticket Funds: 200
0.00	0.00	0.00	100.00	0.00	500.00	Reserve Air Ticke Funds:200
121049.82	4378.62	0.00	900.00	30.00	9548.62	
0.00	0.00	0.00	100.00	0.00	700.00	Reserve Air Ticket Funds:400
1232.30	0.00	0.00	100.00	0.00	500.00	Reserve Air Ticket Funds:300
-18.31	0.00	0.00	100.00	0.00	500.00	Reserve Air Ticket Funds:200
18557.40	556.72	0.00	100.00	50.00	1206.72	Reserve Air Ticket Funds:300
1076.71	0.00	0.00	100.00	100.00	400.00	Reserve Air Ticket Funds:300
-309.21	0.00	0.00	100.00	0.00	600.00	Reserve Air Ticket Funds:300
0.00	0.00	0.00	100.00	0.00	500.00	Reserve Air Ticke Funds: 200
0.00	0.00	0.00	100.00	0.00	500.00	Reserve Air Ticke Funds:200
0.00	0.00	13.98	100.00	150.00	284.41	Reserve Air Ticket Funds: 100
20538.89	556.72	13.98	900.00	300.00	5191.13	
0.00	0.00	0.00	100.00	100.00	600.00	Reserve Air Ticket Funds:400
624.23	0.00	0.00	100.00	0.00	600.00	Reserve Air Ticket Funds:200
0.00	0.00	0.00	100.00	50.00	450.00	Reserve Air Ticket Funds: 100
13755.55	0.00	0.00	100.00	0.00	200.00	Reserve Air Ticket Funds:300
0.00	0.00	0.00	100.00	0.00	200.00	Reserve Air Ticket Funds:300
-9.82	0.00	0.00	100.00	50.00	550.00	Reserve Air Ticket Funds:200
-8.17	0.00	0.00	100.00	100.00	600.00	Reserve Air Ticket Funds:100
0.00	0.00	0.00	100.00	0.00	500.00	Reserve Air Ticke Funds: 100
					0.00	
14361.78	0.00	0.00	800.00	300.00	3700.00	
155950.50	4935.34	13.98	2600.00	630.00	18439.75	

		TRC	ERC
1	[redacted]	[redacted]	[redacted]
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			

52. Fourth, images located on Device 1 appeared to show an unknown individual sitting at a table. The individual is sitting in front of what appears to be a white colored, all-in-one style computer. The computer seen in the image is consistent with hundreds of similar computers which were observed by the FBI Team as part of the devices seized by the MNP, as well as the information described herein that numerous African-origin individuals were employed by Defendant WA as part of the NFTWEB3 Scam.



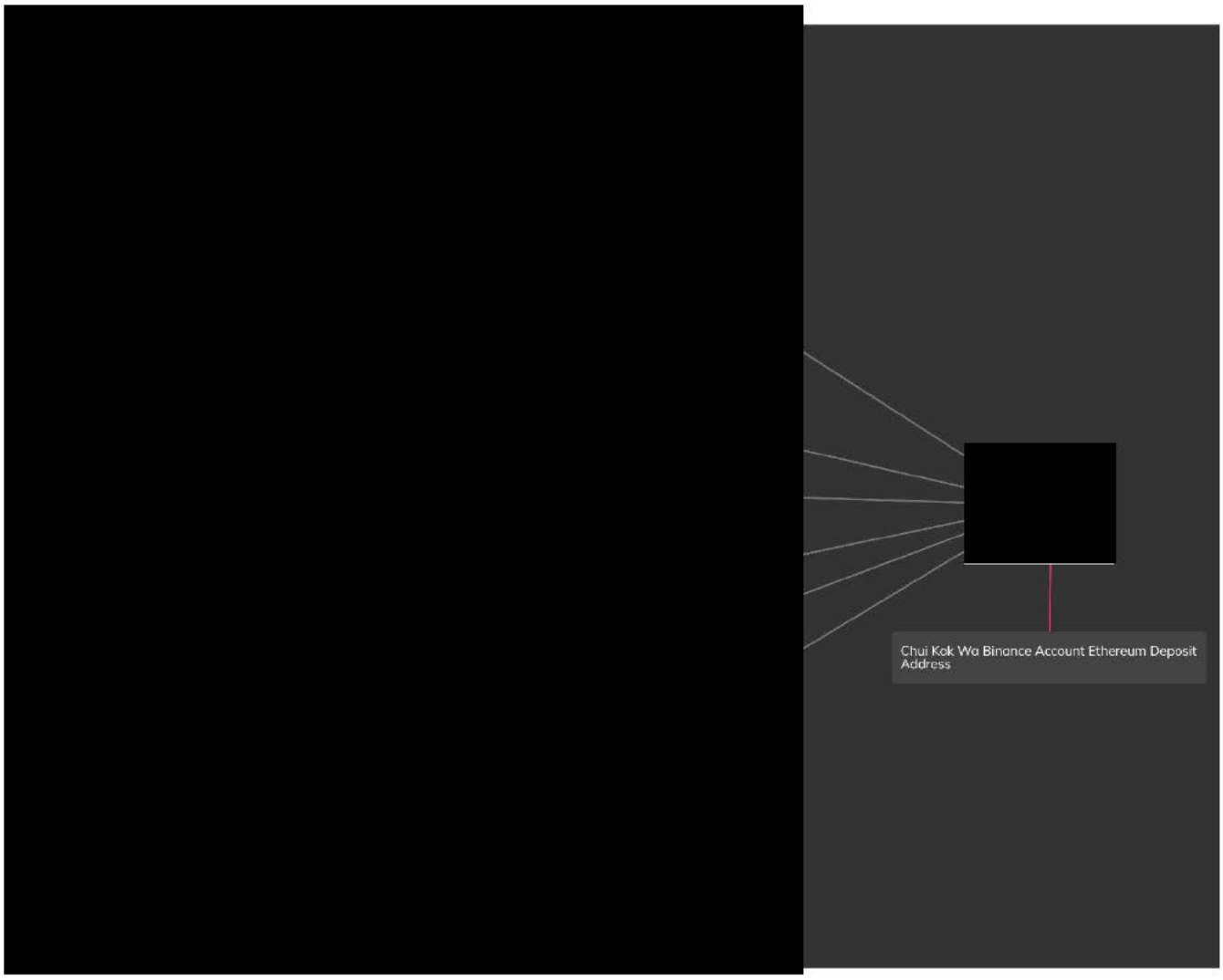
Defendant WA's Cryptocurrency Accounts

53. Defendant WA used cryptocurrency wallets both to receive funds stolen in the NFTWEB3 Scheme and to pay his employees' salaries. Relevant here, through business records of Binance and information in the KP1 phone, FBI investigators have identified the three primary means of such transfers as the Defendant WA's Binance Account 1, Tron Address 1, and Ethereum Address 1.

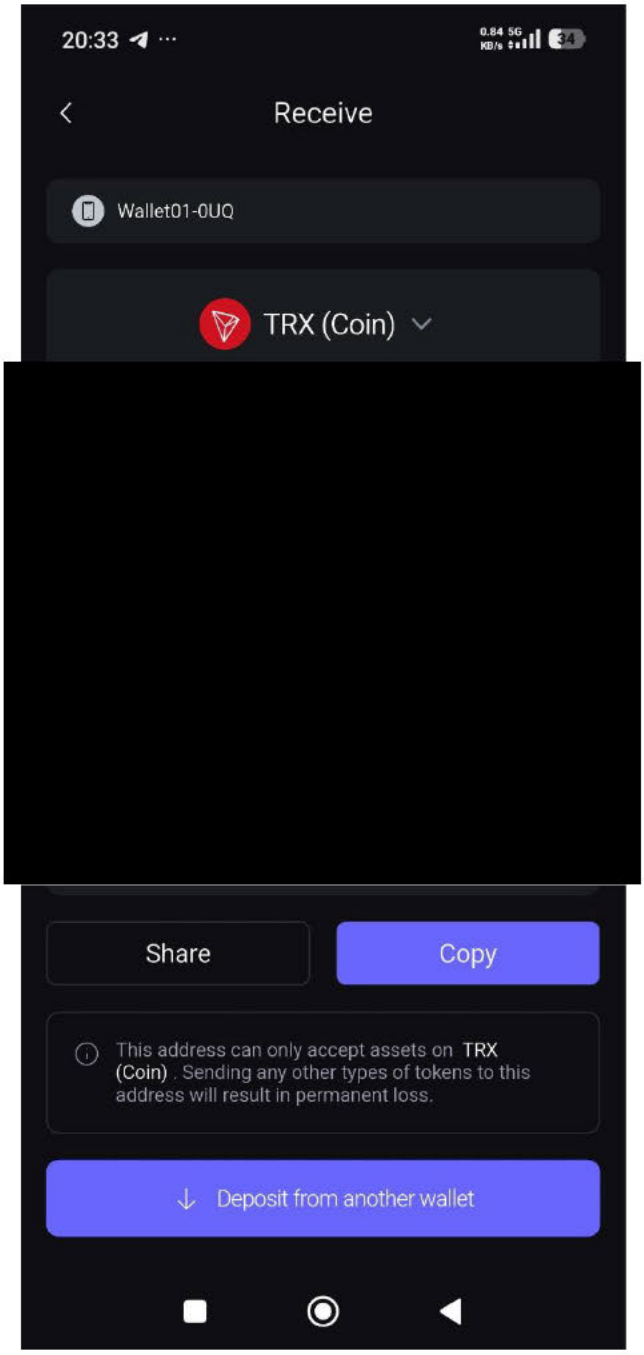
54. Related to the WA Binance Account 1, as explained further herein, during the NFTWeb3 Scam, the scammer would convince the victim to invest in NFT's and then have the victim link their cryptocurrency wallet to a specific Web3 site. Once linked, the scammer could then control the wallet and pull money without the consent of the victim. As shown in the following paragraphs, Defendant WA's Binance Account 1 was repeatedly used (a) to receive victim funds and (b) to pay the employees working for WA in the scheme.

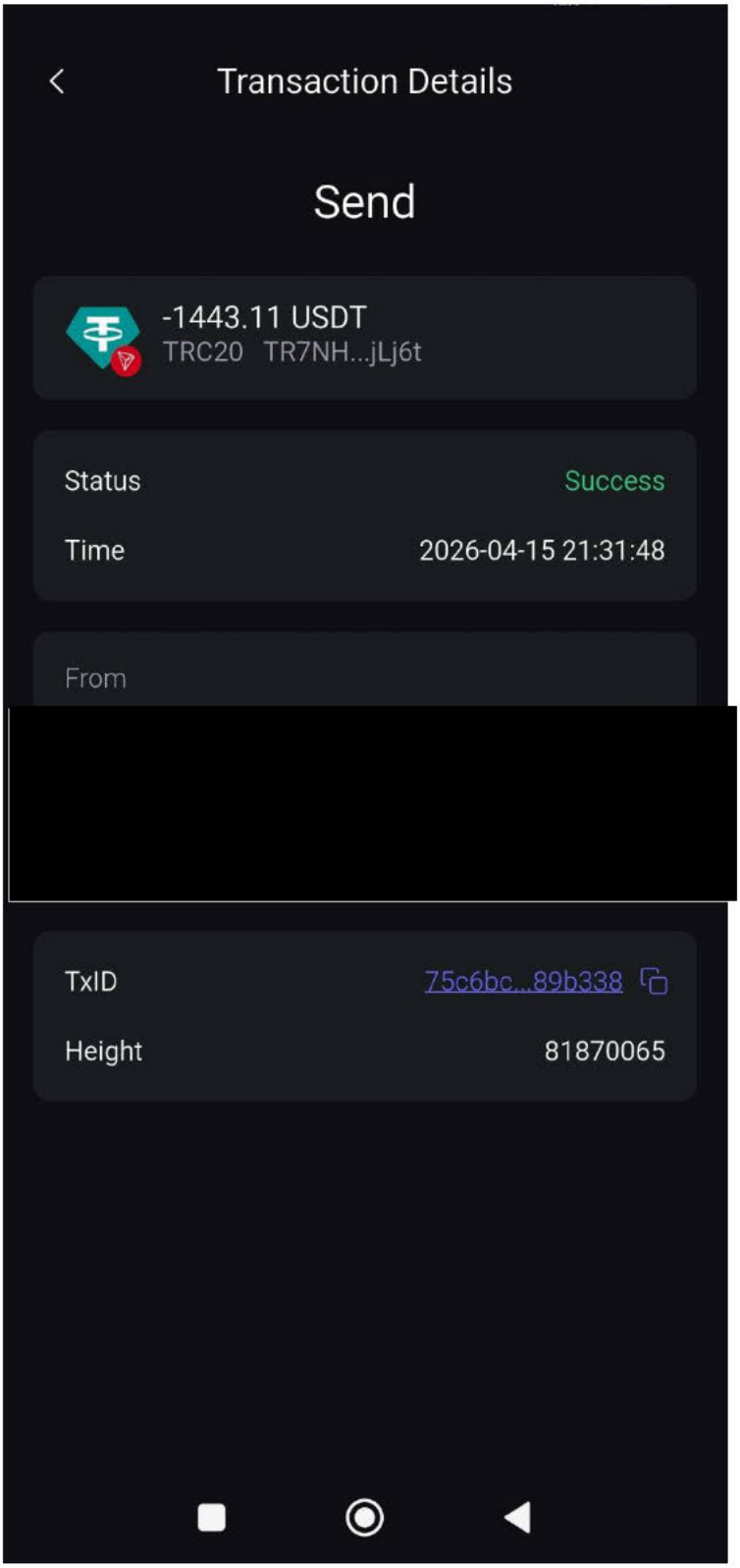
55. According to business records of Binance, WA Binance Account 1 had an Ethereum deposit address of [redacted]. The FBI conducted analysis of incoming transactions to [redacted], and identified at least five counterparty wallets that sent funds to [redacted] all of which had IC3 reports filed indicating those wallets had received money from the victim as part of the NFT Web3 Scam activity. An additional counterparty wallet, [redacted], was blacklisted by Tether on/around March 26, 2026, which according to information provided by the United States Secret Service (USSS) was due to a request of the USSS because that wallet appeared to engaged in malicious Ethereum token approve functions.[10] A visual aid follows.

[10] Ethereum contains a function called "approve()", which when called, allows Wallet A to spend a set amount of a designated token from Wallet B. The number of tokens which can be allocated to an approve() function is unlimited. See also supra ¶ 19.d.



56. Related to the WA Binance Account 1, multiple screenshots were identified on KP1 indicating a SafePal Wallet was installed on KP1. Additionally, the android package "io.safepal.wallet" was installed on KP1. One of the Tron Network addresses identified within the SafePal Wallet was [redacted] (hereinafter, "WA Tron Address 1").

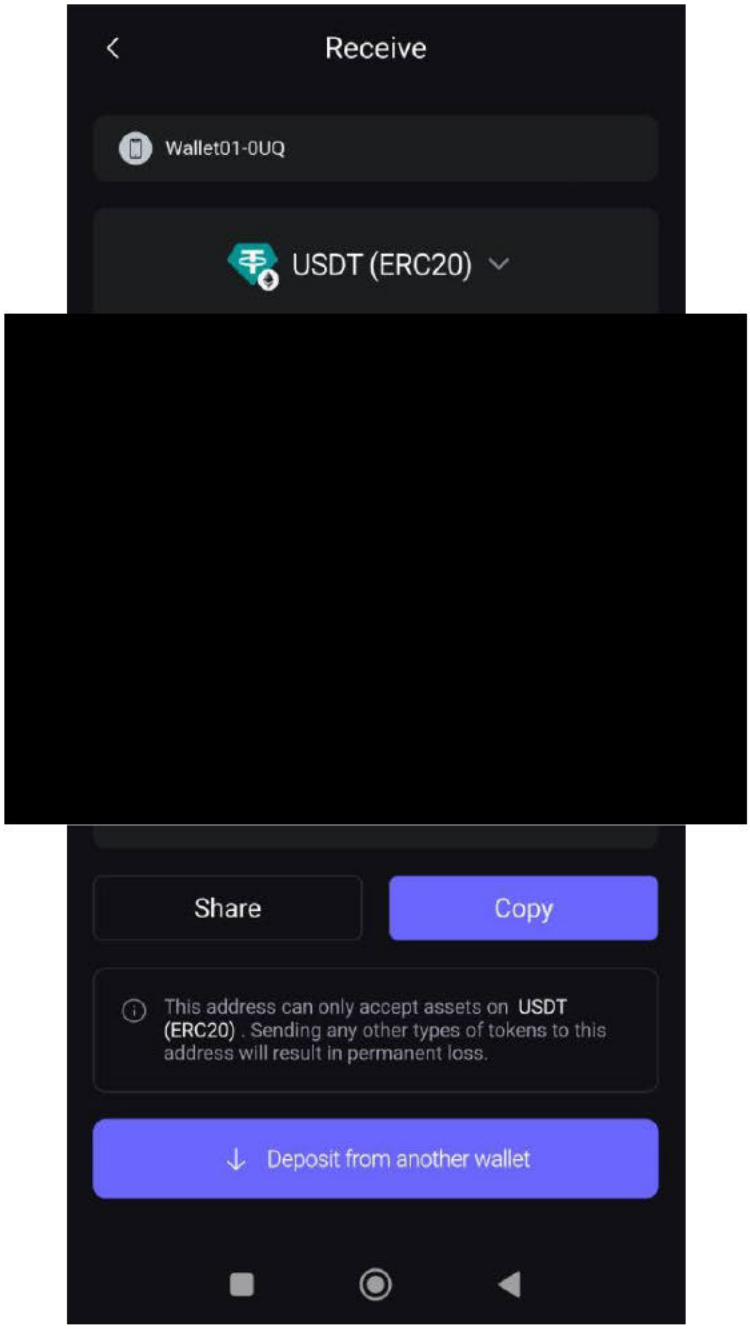

20:33
Receive
Wallet01-0UQ
TRX (Coin)
Share
Copy
This address can only accept assets on TRX (Coin) . Sending any other types of tokens to this address will result in permanent loss.
Deposit from another wallet

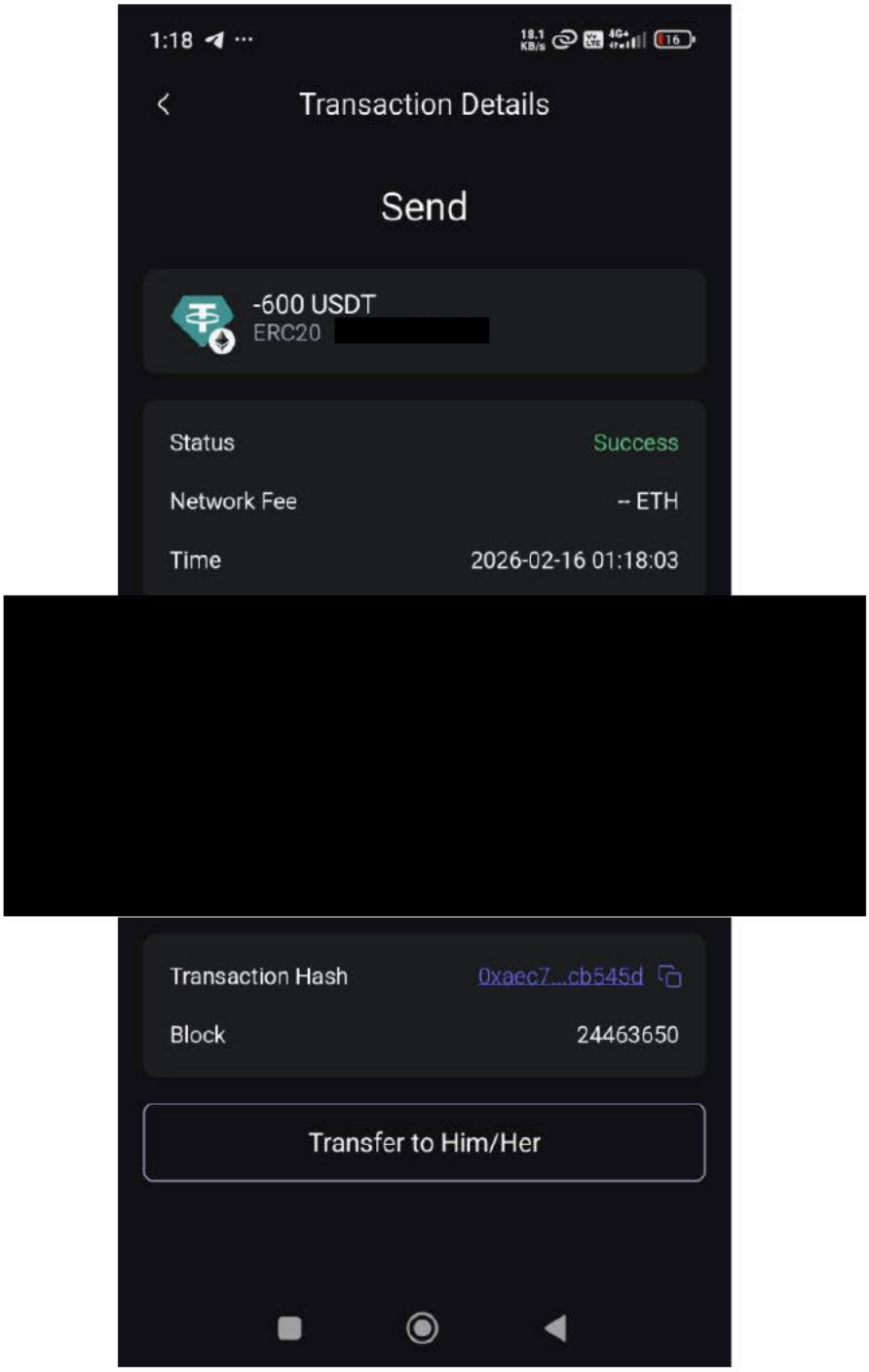


(File Name: Screenshot_2026-04-15-21-34-21-849_io.safepal.wallet-edit.jpg)

57. As an example, the file on KP1 called "Screenshot_2026-04-15-21-34-21-849_io.safepal.wallet-edit.jpg" pertained to a transfer of USDt from WA Tron Address 1 to [redacted] which is an address attributed to Binance.com. Binance business records showed that the account associated with [redacted] is registered by an individual listed as employee number 4 of the first tab of the employee roster .

58. In addition, files located on KP1 indicate defendant WA likely controls Ethereum (a Blockchain network) address [redacted] (hereinafter, "WA Ethereum Address 1"), which sent cryptocurrency payments to at least eight co-conspirators.


Receive
Wallet01-0UQ
USDT (ERC20)
Share
Copy
This address can only accept assets on USDT (ERC20) . Sending any other types of tokens to this address will result in permanent loss.
Deposit from another wallet



Example of Use of Cryptocurrency Consolidation Addresses

59. A victim in Las Vegas, Nevada (hereinafter, "the Las Vegas-Victim"), reported a loss of $618 to an NFT scam. The Las Vegas-Victim reported an unauthorized transaction had occurred from their wallet [redacted] when 618.2 USDt was transferred to [redacted]

60. The Las Vegas-Victim's wallet [redacted] received one initial USDt funding transaction of 593.937874 USDt from an address attributed to Kraken.com on 08/25/2026 21:43. This was the first incoming transaction of any asset type to [redacted]. Nine minutes later, at 08/25/2026 21:54, [redacted] received 0.00025 ETH from [redacted]. Eighteen minutes later, at 08/25/2026 22:12, [redacted] signed an approve function transactions which allowed unlimited USDt to transferred from [redacted] address was the same addresses which was involved in the approve function transactions for both the Portland-Victim and the Greenbelt-Victim.

61. The Las Vegas-Victim received three incoming USDt transactions from [redacted] between 08/27/2026 22:22 and 08/31/2026 22:29, for a cumulative amount of 24.7 USDt. These three transactions are consistent with hook payments to victims which are designed to generate a false sense of trust in a fraudulent platform. On 09/03/2026 00:41, [redacted] transferred all 618.62 USDt from the Las Vegas-Victim's wallet to [redacted]

[redacted]

62. Additionally, [redacted], the addresses which received the Las Vegas-Victim's stolen USDt, had transaction activity occur between Aug 29, 2026 - Sep 5, 2026. During this time, [redacted] received 9971.78 USDt, and sent approximately 53% of all received USDt to addresses attributed to the crypto exchanges Binance.com and OKX.com.

Connection of Cryptocurrency Wallets Used in the Scheme to Chinese Users

63. A review of publicly-available blockchain data related to reports from U.S. victims showed that the victims' stolen funds often were siphoned into cryptocurrency wallets controlled by Chinese individuals.

64. The NFTWEB3 Scheme utilizes multiple Ethereum addresses to initiate malicious transactions to steal USDt tokens from their victims.

a. One of the most prominent Ethereum addresses used by the conspiracy is [redacted]

Utilizing publicly-available blockchain date, the FBI identified at least 74 unique Ethereum addresses which had signed unlimited USDt approve transactions which listed [redacted] as the approve address spender. In practicality, this means [redacted], could at any time, transfer an unlimited amount of USDt tokens from the Ethereum addresses which signed the transaction. The FBI identified a total of 127 separate transactions initiating from the 74 unique Ethereum addresses, with a total estimated loss of 516,695.46 USDt.

b. The FBI identified at least four Ethereum addresses which had signed USDt approve transactions involving [redacted] had exposure to [redacted], an address attributed to okx.com. Records from okx.com showed that the

registered user of the wallet was Individual 1, who reported that they resided in China and provided Chinese identity documents as a basis for identity verification.

c. The FBI conducted analysis of six Ethereum addresses which sent USDt to [redacted] between 08/13/2026 and 10/09/2026. Five of the six analyzed addresses received USDt from addresses which had signed USDt approve transactions involving [redacted]

d. One of the addresses which sent USDt to [redacted] was [redacted] In total, [redacted] **sent** 18,855.55 USDt to [redacted] between 08/13/2026 and 08/27/2026:

   i. 4,366 USDt on 08/13/2026 17:52

   ii. 300 USDt on 08/15/2026 01:19

   iii. 102.66 USDt on 08/17/2026 23:51

   iv. 3,130 USDt on 08/19/2026 01:13

   v. 1,448 USDt on 08/19/2026 09:18

   vi. 5,700 USDt on 08/21/2026 01:42

   vii. 3,000 USDt on 08/26/2026 06:00

   viii. 808.89 USDt on 08/27/2026 15:11

e. [redacted] received two incoming USDt transaction from [redacted] between [redacted]

   i. 2,858.49 USDt on 08/24/2026 23:22

   ii. 9,067.64 USDt on 08/25/2026 19:54

As previously discussed, [redacted] is an address controlled by the Greenbelt-Victim (see supra ¶19.a).

65. One of the six addresses analyzed by the FBI was [redacted] sent 2,757 USDt to [redacted] on 10/09/2026. [redacted] has received one sole incoming USDt transaction of 6,267.55 USDt on 10/09/2026 from [redacted]. The FBI identified an IC3 report filed by an individual in Philadelphia (hereinafter, the "Philadelphia-Victim") relevant to [redacted] The Philadelphia-Victim filed an IC3 report on 10/13/2026 containing allegations of NFT fraud and an unauthorized transfer of USDt from their wallet, which was identified as [redacted] The FBI identified [redacted] signed a USDt approve function on [redacted] which allowed [redacted] transfer an unlimited amount of USDt from [redacted].

66. According to business records of OKX, an OKX Account registered to Individual 1 had four unique login events in 2026, all of which originated from IP addresses which resolved to China Mobile Communications Corporation.

Login Time (+0800)	**Login IP**	**IP Network**
2026-08-09 00:17:22	111.55.168.252	China Mobile Communications Corporation
2026-05-28 12:57:45	39.144.251.139	China Mobile Communications Corporation
2026-05-04 23:04:27	39.144.251.206	China Mobile Communications Corporation
2026-03-04 15:10:19	112.48.77.23	China Mobile Communications Corporation

67. The OKX Account registered to Individual 1 did not conduct any on-chain cryptocurrency withdrawals in 2026; however, it did conduct 59 internal transactions converting USDt to Chinese Yuan Renminbi (CNY). All 59 conversion transactions converted USDt to CNY,

and were sent to AliPay account ending in *354. In total, approximately 268,779 USDt was converted to CNY. Records produced by OKX contained the following information:



(Visual aid showing USDt flow into OKX account

68. Additionally, the FBI identified a consolidation address, which received funds from at least two individuals who filed IC3 reports, which between Nov 30, 2025 - Mar 28, 2026, received 980,166.22 USDt.

69. An individual from Kalamazoo, Michigan (hereinafter, "the Kalamazoo-Victim"), filed an IC3 report on 07/03/2026 pertaining to an allegation of a NFT scam perpetrated by inftnexus.com, to include unauthorized transfers of USDt. The Kalamazoo-Victim controlled Ethereum address which signed a USDt approve transaction involving on 02/18/2026. On

03/10/2026, 1,603.27 USDt was transferred from [redacted] In total, the Kalamazoo-Victim lost approximately 6,708.62 USDt.

70. An individual from Ben Lomond, California (hereinafter, "the Ben Lomond-Victim"), filed an IC3 report on 03/13/2026 pertaining to an allegation of a NFT scam perpetrated by inftx.pro. The Ben Lomond-Victim controlled [redacted] which signed a USDt approve transaction involving [redacted] on 02/18/2026. The following two transactions occurred wherein USDt was transferred from [redacted] both transactions were initiated by [redacted]

a. 8,242.11 USDt on 02/28/2026 17:30

b. 20,600 USDt on 03/10/2026 13:25

71. The FBI identified that [redacted] sent approximately 3,000 USDt to [redacted] an address attributed to okx.com. According to business records of okx.com, [redacted] was associated with Individual 2, who reported to OKX that they were a resident of China.

72. The same OKX Account had nine unique login events, five of which occurred from IP addresses attributed to telecommunications and/or internet service providers in Madagascar:

Login Time (+0800)	Login IP	IP Network
2026-07-25 00:08:43	203.160.68.197	China Unicom (Hong Kong) Operations Limited
2026-06-22 18:21:20	41.74.210.194	ORANGE_MADAGASCAR
2026-05-30 09:47:57	129.222.109.53	STARLINK.COM
2026-03-14 06:28:38	102.16.71.140	Telecom Malagasy
2026-03-10 21:41:16	102.16.71.140	Telecom Malagasy
2026-03-07 21:08:00	102.16.71.140	Telecom Malagasy
2026-02-05 23:40:27	102.17.104.191	Telecom Malagasy
2025-11-15 05:55:04	171.236.136.211	VIETTEL-VN
2025-10-16 12:39:32	14.249.65.140	VNPT-VN

73. The same OKX Account only conducted one on-chain cryptocurrency withdrawal from their account on/around 03/09/2026 of 0.004935 ETH. However, it did conduct 16 internal transactions converting USDt to Chinese Yuan Renminbi (CNY). All 16 conversion transactions converted USDt to CNY, and were sent to either AliPay account ending in *222 or WeChat Pay account ending in *7222. In total, approximately 41,570 USDt was converted to CNY. Records produced by OKX associated the account with a Chinese user.



(Visual aid showing USDt flow into OKX account [redacted])

74. Further, the FBI identified an IC3 report filed by an individual from Douglas, Massachusetts (hereinafter, "the Douglas-Victim"), which contained allegations of an NFT scam purported by "inftpulse.com". The FBI identified the Douglas-Victim had signed a USDt approve function on 2/26/2026 which allowed [redacted] to transfer an unlimited amount of USDt from the Douglas-Victim's wallet.

75. On 3/27/2026, [redacted] transferred 8,917.76 USDt from the Douglas-Victim's wallet to [redacted] The FBI examined four of the largest USDt funders of [redacted] and identified all four funders had

signed unlimited USDt approve function transactions. Three of the funders had signed USDt approve function transactions with [redacted] and one had signed a USDt approve function transaction with [redacted]. The four analyzed USDt funders of [redacted] had tokens sent between 03/24/2026 to 03/28/2026.

76. Between 03/24/2026 to 04/02/2026, [redacted] received 111,901 USDt. [redacted] sent three outbound USDt transactions between 03/30/2026 to 03/31/2026 to [redacted] an address attributed to okx.com

a. 10,000 USDt on 03/30/2026 14:50

b. 10,000 USDt on 03/30/2026 15:28

c. 15,000 USDt on 03/31/2026 04:09

[redacted]

77. Records from okx.com related to the account associated with [redacted] identified an account (ending in *584) and associated with a Chinese user. Further OKX account records for the same account showed that the account had one sole login event in 2026, which occurred from IP address 27.154.193.7. The login IP address was resolved to CHINANET FUJIAN PROVINCE NETWORK. A review of historical login events between 2021 and 2025 for the OKX account ending in *584 identified multiple IP addresses resolving to providers in China, Vietnam, Malaysia, and the United Arab Emirates.

78. Records of Binance further show that all USDt received in 2026 by OKX account ending in *584 was sold for Chinese Yuan Renminbi (CNY). Three USDT to CNY transactions (cumulatively 35,100 USDt) occurred between 3/30/2026 – 03/31/2026 to AliPay account ending in *833, which was listed as a payment instrument for OKX account [redacted]

IV. Identification Employees of WA and Members of the Conspiracy

79. Your Affiant analyzed the documents located on KP1 (i.e., the chart of employees and their wallet addresses) with other documents in the case. Specifically, business records of Binance.com showed payments from WA's Binance Account 1 to the Binance accounts of his employees, who were listed on the employee roster. Further, Binance records included the national IDs of WA's employees, and corresponding to the employee roster. Binance records also showed payments made by WA to each employee's wallet associated with their Binance account. Finally, blockchain tracing, when compared and analyzed with iC3 records, showed that many of the employees received victim funds into wallets associated with their Binance accounts and several also received payments from Defendant WA's Tron Address 1. The following chart summarizes that pertinent information for ease of the Court, and shows the scope and organization of WA's business.

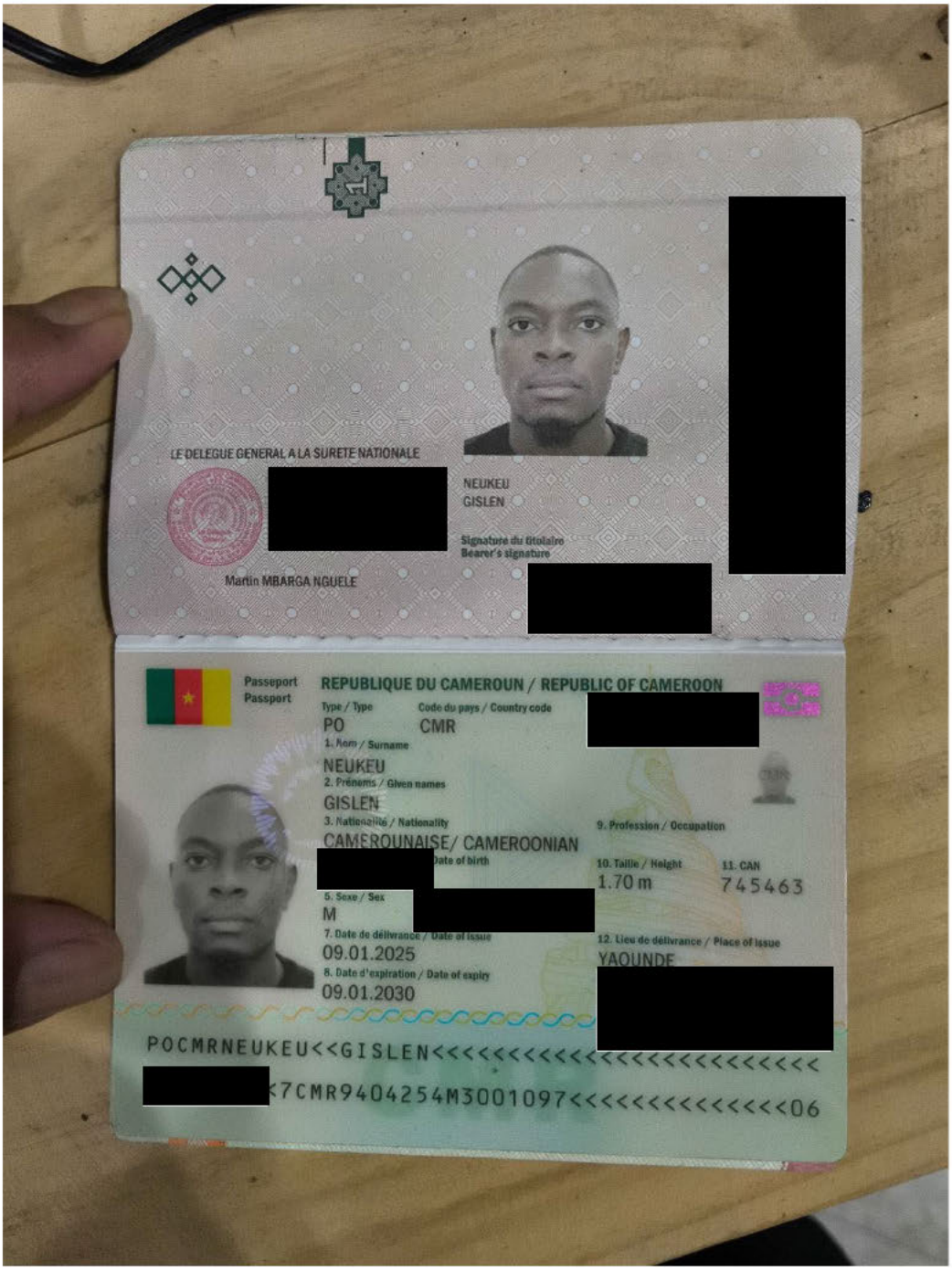
Employee Roster		*Binance Records*				*Blockchain Tracing*	
Employee Number on Roster (Tab 2)	**Wallet on Roster**	**Nationality**	**Wallet ID**	**IP Login Location**	**IP Log In Dates**	**Total Payments from CHUI Tron Address 1 (USDt)**	**Victim Funds / Infrastructure Funds Receieved (USDt)**
10	[redacted]	Kenya	[redacted]	Antananarivo, Madagascar	2025-04-08 to 2026-05-14	2,065.22	N/A
13	[redacted]	Rwanda		Antananarivo, Madagascar	2025-12-02 to 2026-05-13	200	N/A
14	[redacted]	Zimbabwe		Antananarivo, Madagascar	2025-08-16 to 2026-05-12	200	N/A
15	0[redacted]	Kenya		Antananarivo, Madagascar	2025-12-02 to 2026-05-05	500	N/A
22	[redacted]	Zimbabwe		Antananarivo, Madagascar	2025-07-21 to 2026-05-14	88.46	N/A
24	[redacted]	Ghana		Antananarivo, Madagascar	2025-12-05 to 2026-05-14	1,934.50	N/A
11	[redacted]	Rwanda		Antananarivo, Madagascar	2025-04-20 to 2026-05-15	600	N/A
9	[redacted]	Zimbabwe		Antananarivo, Madagascar	2026-01-15 to 2026-04-20	670	N/A
8	[redacted]	Zimbabwe		Antananarivo, Madagascar	2026-01-13 to 2026-04-23	500	N/A
5	[redacted]	Zimbabwe		Antananarivo, Madagascar	2025-08-12 to 2026-04-20	994.14	N/A
2	[redacted]	Zimbabwe		Antananarivo, Madagascar	2025-08-08 to 2026-05-14	600	7,726.65
2	[redacted]	Kenya		Antananarivo, Madagascar	2025-11-30 to 2026-05-01	1443.11	972.84

80. Through a review of the aforementioned evidence, your affiant identified Defendant NEUKEU as an employee of Coconspirator 1, WA engaged in the conspiracy.

81. KP1 contained in image, titled "raw.jpg" that appeared to be a photograph taken of a Republic of Cameroon Passport belonging to the following individual:

Name: GISLEN NEUKEU

Passport Number: [redacted]



("raw.jpg" [md5 hash: c969638f9fd57c82fc401476a9084c18])

82. Binance records showed that the following Binance account associated with GISLEN NEUKEU (and included a different passport with the same identifying information):

Binance User ID: [redacted]

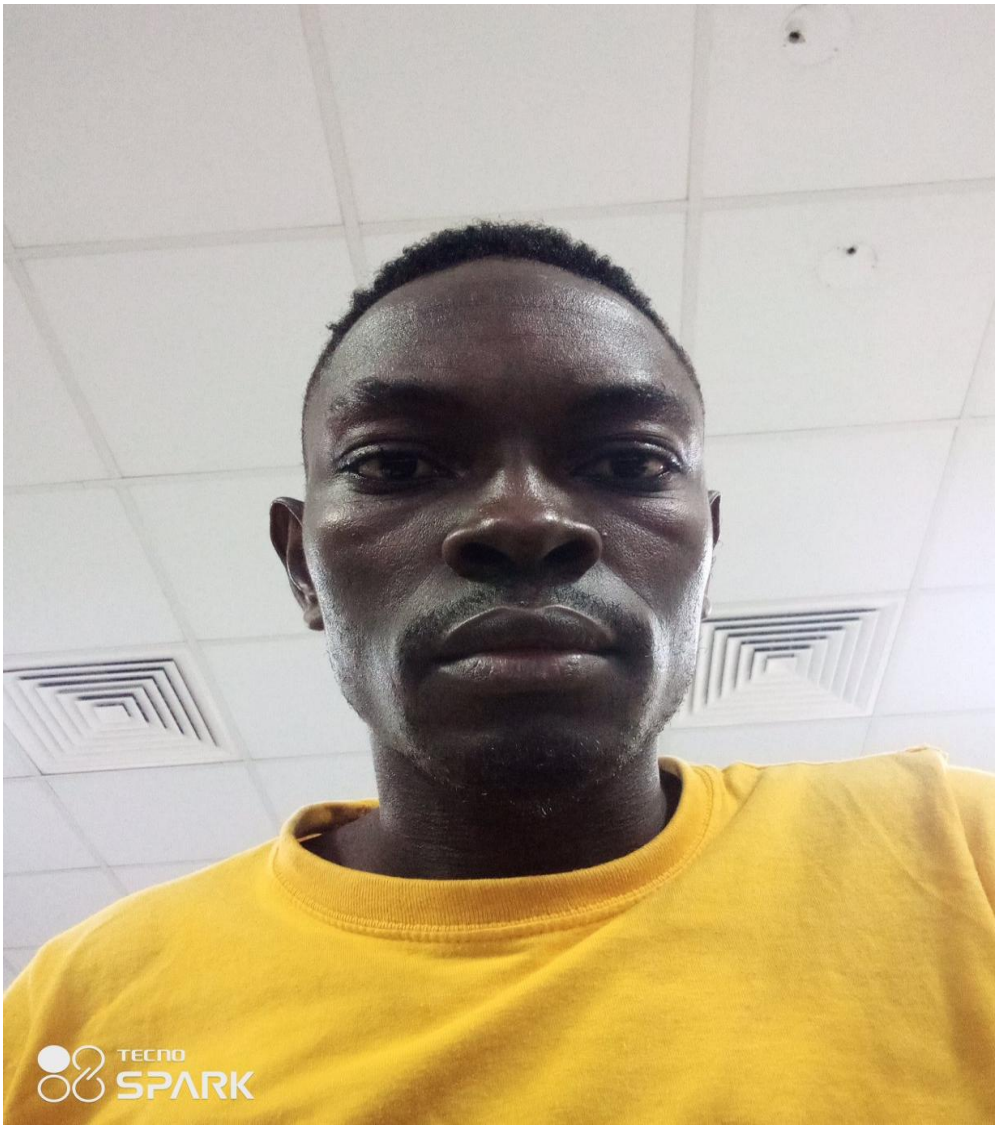
Name: GISLEN NEUKEU

ID Document: Republic of Cameroon Passport

ID Number: [redacted]



(Binance KYC document)



(Binance KYC document)

83. A review of access logs for Binance account [redacted] revealed 592 unique logs between 2025-04-17 04:04:46 to 2026-05-31 05:58:02 which had IP addresses geolocate to Antananarivo, Madagascar.

84. Defendant NEUKEU was also connected with a victim of the NFTWEB3 Scheme. An individual from Eagan, Minnesota (hereinafter referred to as the Eagan-Victim) filed an IC3 report on 09/21/2026. The report contained allegations of cryptocurrency fraud and theft by the website "inftvault.com". The Eagan-Victim had a reported loss of approximately $31,343.88.

85. An Eagan-Victim identified cryptocurrency address [redacted] as an address in a wallet controlled by the Eagan-Victim. The FBI identified on 7/1/2026, [redacted] signed a transaction which contained an approve function delegation for all USDt to [redacted] (also related to the Greenbelt, Portland, and Las Vegas victims).

86. Blockchain analysis indicated the Eagan-Victim had USDt taken from [redacted] and sent to the following two addresses:

a. [redacted]

i. 15,888.04 USDt on 07/14/2026 22:55

ii. 1,866.91 USDt on 07/15/2026 21:55

iii. 2,712.05 USDt on 07/22/2026 14:17

b. 0x1e3C530E34b59f6B967fDBD7991b41Afde7022F3 (**0x1e…22F3**)

i. 4,366 USDt on 08/13/2026 15:51

87. 6,540 USDt on 08/20/2026 18:00Both [redacted] and [redacted] sent USDt to [redacted], which is an address attributed to Binance account [redacted] (the account associated with Defendant NEUKEU):

a. 36 USDt on 08/19/2026 14:47 from [redacted]

b. 36 USDt on 08/20/2026 13:52 from

c. 36 USDt on 08/21/2026 15:27 from

d. 36 USDt on 08/22/2026 15:44 from

e. 550 USDt on 08/01/2026 11:56 from

f. 90 USDt on 08/01/2026 16:35 from

g. 18 USDt on 08/05/2026 15:38 from

h. 36 USDt on 08/06/2026 14:40 from

i. 36 USDt on 08/07/2026 15:12 from [redacted]

j. 36 USDt on 08/08/2026 14:58 from

k. 36 USDt on 08/09/2026 21:23 from

l. 36 USDt on 08/10/2026 15:45 from

m. 36 USDt on 08/11/2026 15:43 from

88. Based on the entirety of the evidence, there is probable cause to believe that Defendant was working as an employee of WA and under a contract with WA to scam individuals through the U.S. wires.

89. Through a review of the aforementioned evidence, your affiant identified Defendant NINSIIMA as an employee of WA engaged in the conspiracy.

90. KP1 contained in image, titled "raw.jpg" that appeared to be a photograph taken of a Republic of Cameroon Passport belonging to Coconspirator 2, NEUKEU, (CC2).

91. Binance records showed that the following Binance account associated with CC2 (and included a different passport with the same identifying information):

Binance User ID: [redacted]

92. A review of access logs for Binance account [redacted] revealed 592 unique logs between 2025-04-17 04:04:46 to 2026-05-31 05:58:02 which had IP addresses geolocate to Antananarivo, Madagascar.

93. CC2 was also connected with a victim of the NFTWEB3 Scheme. An individual from Eagan, Minnesota (hereinafter referred to as the Eagan-Victim) filed an IC3 report on 09/21/2026. The report contained allegations of cryptocurrency fraud and theft by the website "inftvault.com". The Eagan-Victim had a reported loss of approximately $31,343.88.

94. An Eagan-Victim identified cryptocurrency address [redacted] as an address in a wallet

controlled by the Eagan-Victim. The FBI identified on 7/1/2026, [redacted] signed a transaction which contained an approve function delegation for all USDt to [redacted] (also related to the Greenbelt, Portland, and Las Vegas victims).

95. Blockchain analysis indicated the Eagan-Victim had USDt taken from [redacted] and sent to the following two addresses:

c. [redacted]

i. 15,888.04 USDt on 07/14/2026 22:55

ii. 1,866.91 USDt on 07/15/2026 21:55

iii. 2,712.05 USDt on 07/22/2026 14:17

d. [redacted]

i. 4,366 USDt on 08/13/2026 15:51

ii. 6,540 USDt on 08/20/2026 18:00

96. Both [redacted] and [redacted] sent USDt to [redacted] which is an address attributed to Binance account [redacted] (associated with CC2):

n. 36 USDt on 08/19/2026 14:47 from [redacted]

o. 36 USDt on 08/20/2026 13:52 from

p. 36 USDt on 08/21/2026 15:27 from

q. 36 USDt on 08/22/2026 15:44 from

r. 550 USDt on 08/01/2026 11:56 fro

s. 90 USDt on 08/01/2026 16:35 from

t. 18 USDt on 08/05/2026 15:38 from

u. 36 USDt on 08/06/2026 14:40 from

v. 36 USDt on 08/07/2026 15:12 from

w. 36 USDt on 08/08/2026 14:58 from [redacted]

x. 36 USDt on 08/09/2026 21:23 from

y. 36 USDt on 08/10/2026 15:45 from

z. 36 USDt on 08/11/2026 15:43 from

97. As stated, the Eagan-Victim's funds were stolen and deposited into [redacted] and [redacted] Further, both [redacted] and [redacted] sent USDt to [redacted] which is an address attributed to Binance.com:

a. 180 USDt on 07/16/2026 09:20 fro [redacted]

b. 50 USDt on 07/30/2026 09:02 from

c. 18 USDt on 08/19/2026 14:53 from

d. 18 USDt on 08/19/2026 from **0x1e**

e. 18 USDt on 08/19/2026 from **0x1e**

f. 18 USDt on 08/19/2026 from **0x1e**

[redacted]

(Visual aid showing connections between the Eagan-Victim and Binance account [redacted]

98. Records from Binance for [redacted] identified the following Binance account:

Binance User ID: [redacted]

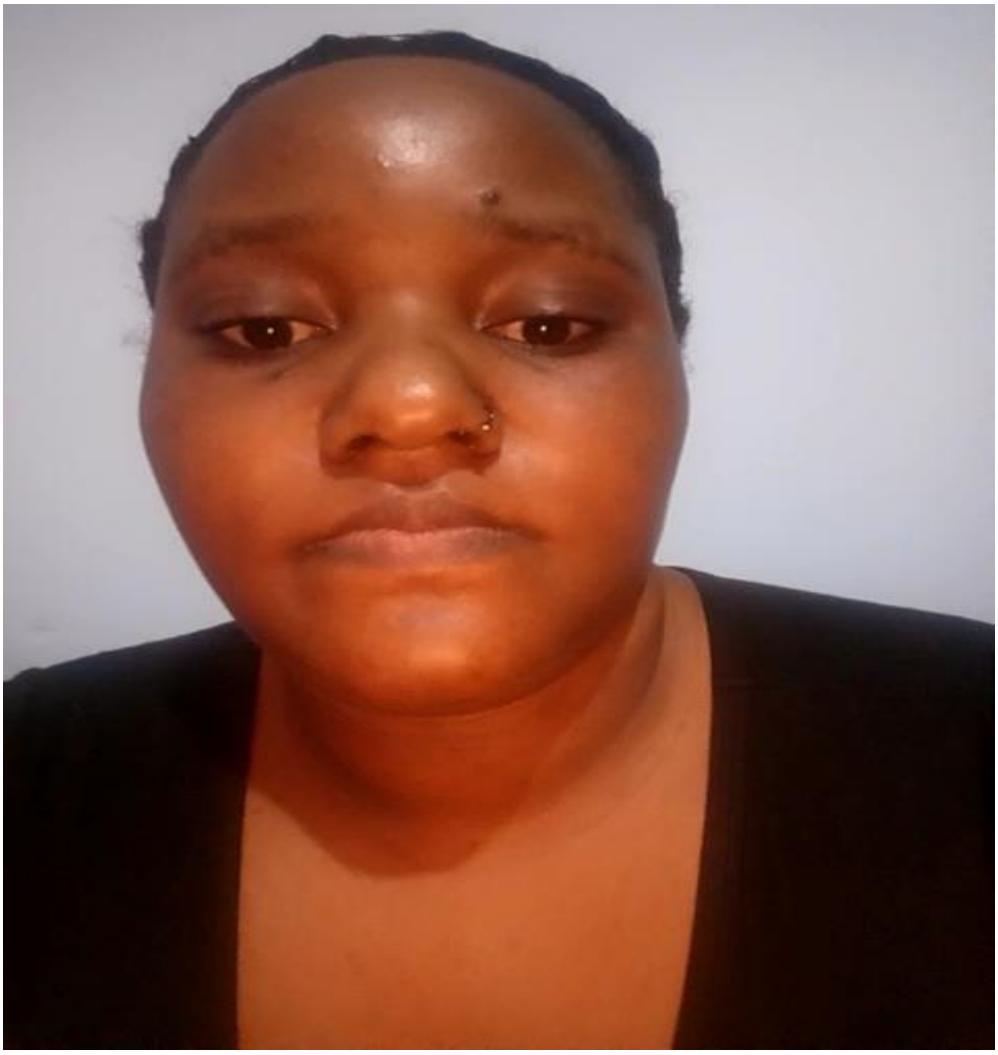
Name: SHAMUSA NINSIIMA

ID Document: Republic of Uganda National ID Card

ID Number: [redacted]



(Binance KYC document)



(Binance KYC document)

99. A review of access logs for Binance account [redacted] revealed 68 unique logs between 2026-02-14 04:46:03 to 2026-07-22 22:15:11 which had IP addresses geolocate to Antananarivo, Madagascar.

100. Based on the entirety of the evidence, there is probable cause to believe that Defendant NINSIIMA was working as an employee of WA and under a contract with WA to scam individuals through the U.S. wires.

101. Through a review of the aforementioned evidence, your affiant identified Defendant MUGIRANEZA as an employee of WA engaged in the conspiracy.

102. KP1 contained in image, titled that appeared to be a photograph taken of a Republic of Rwanda Passport belonging to the following individual:

Name: CLEMENT MUGIRANEZA

Passport Number: [redacted]



("raw.jpg" [md5 hash: b93a09b122174c92c993c3f6631be3aa])

103. Binance business records showed following Binance account associated with CLEMENT MUGIRANEZA:

Binance User ID: [redacted]

Name: CLEMENT MUGIRANEZA

ID Document: Republic of Rwanda Passport

ID Number: [redacted]



(Binance KYC document)



(Binance KYC document)

104. A review of access logs for Binance account [redacted] revealed 582 unique logs between 2025-03-18 03:09:36 to 2025-10-26 13:55:58, which had IP addresses geolocate to Antananarivo, Madagascar.

105. The following two Binance deposit addresses were attributed to Binance account 971340770:

[redacted] received three incoming transactions of USDt from [redacted] between 3/17/2025 and 04/17/2025 [redacted] also funded 7 other co-conspirators' Binance accounts), which your

affiant believes to be a payment account associated with the conspiracy (hereinafter, "Conspirator Payment Wallet 1"):

[redacted]

106. Approximately 82% of all USDt received by Conspirator Payment Wallet 1 to date was sent by [redacted] The FBI identified five separate IC3 reports, from four separate victims, which all contained narratives of being victimized by a fake NFT trading operation. All five reports listed [redacted] as an address where stolen funds were sent to. The five reports were filed between 03/06/2025 and 04/09/2026.

[redacted]

(Visual aid showing funds to Binance Account [redacted]

107. Based on the entirety of the evidence, there is probable cause to believe that Defendant was working as an employee of WA and under a contract with WA to scam individuals through the U.S. wires.

108. Through a review of the aforementioned evidence, your affiant identified Defendant MERVEILLE as an employee of WA engaged in the conspiracy.

109. WA's Tron Address 1, sent 200 USDt on 4/16/2026 to [redacted] a Tron addresses attributed

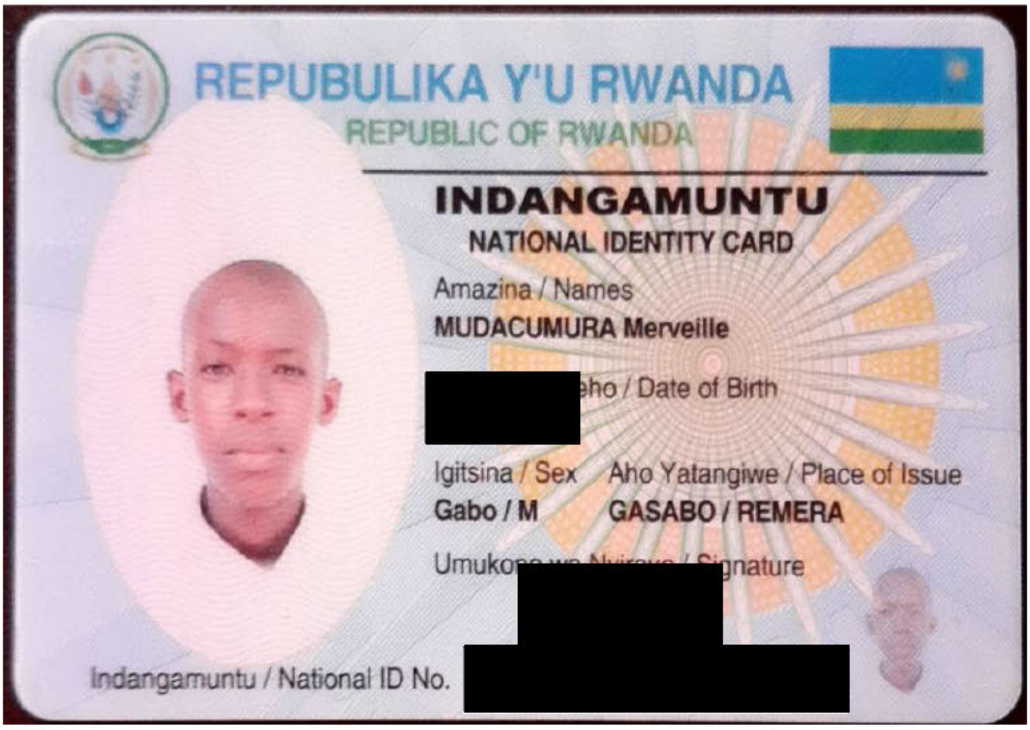
to Binance.com. The FBI requested and received records from Binance, which revealed the following Binance account associated with [redacted]

Binance User ID: [redacted]

Name: MERVEILLE MUDACUMURA

ID Document: Republic of Rwanda National Identity Card

ID Number: [redacted]



(Binance KYC Document)



(Binance KYC Document)

110. A file named "[redacted]" was recovered from KP1. When opened as a spreadsheet, the file contained two tabs. The first tab had a name of "2", and is an apparent employee roster to include columns for staff name, basic salary, working days, discipline fine, commissions, and air ticket reserve fund. On Tab 1, Employee number 26 is "Herve", who had an associated basic salary entry of "800". The second tab had a name of "员工钱包地址", which machine translates to "Employee wallet address". Employee number 26 on Tab 2 is "Herve". Employee 26 had a listed cryptocurrency address of [redacted] which is a deposit addresses associated with Binance User ID [redacted]

111. On 3/16/2026, [redacted] received 500 USDt from [redacted] On 2/15/2026, [redacted] received 63.89 USDt from [redacted]



(Visual aid showing connections between Binance account [redacted] and [redacted]

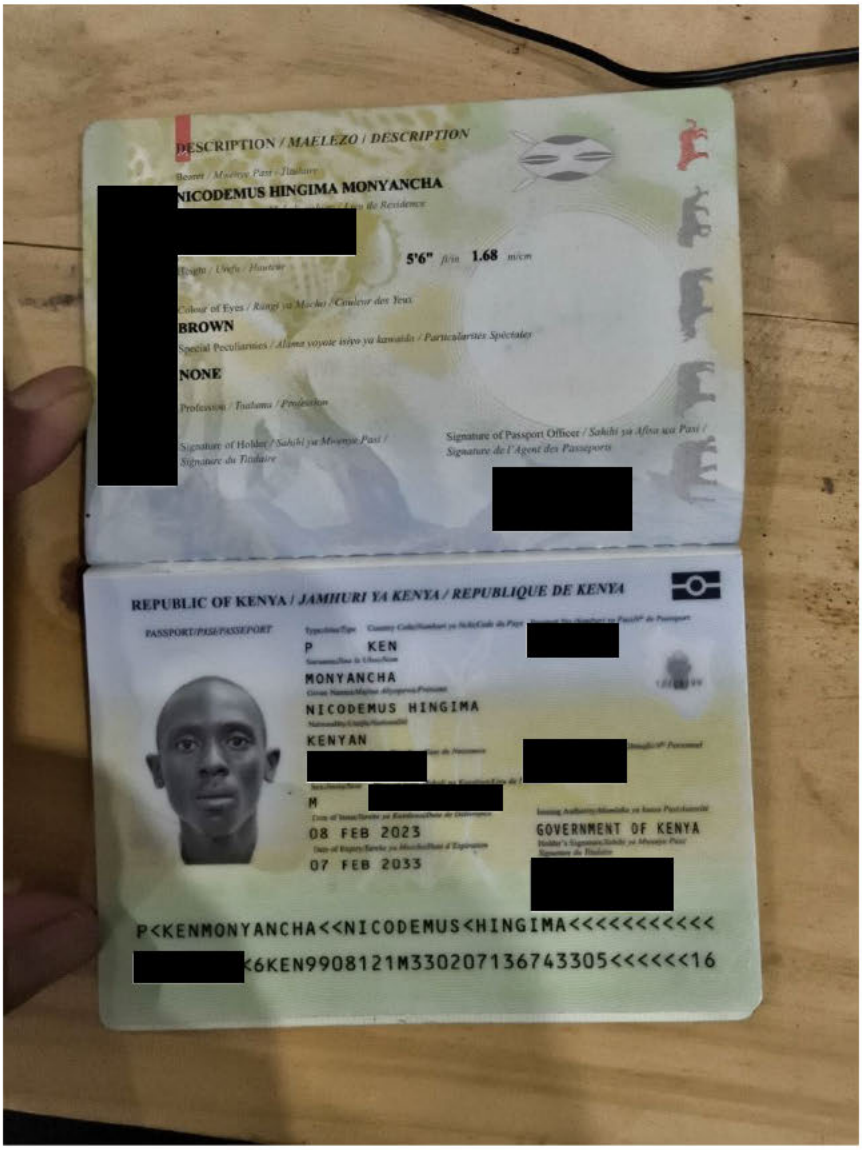
112. Based on the entirety of the evidence, there is probable cause to believe that Defendant was working as an employee of WA and under a contract with WA to scam individuals through the U.S. wires.

113. Through a review of the aforementioned evidence, your affiant identified Defendant MONYANCHA as an employee of WA engaged in the conspiracy.

114. KP1 contained in image, titled "raw.jpg" that appeared to be a photograph taken of a Republic of Kenya Passport belonging to the following individual:

Name: NICODEMUS HINGIMA MONYANCHA

Passport Number: [redacted]



(raw.jpg [md5 hash:1ca6bb21530bcb2d61e4a92d64a55064])

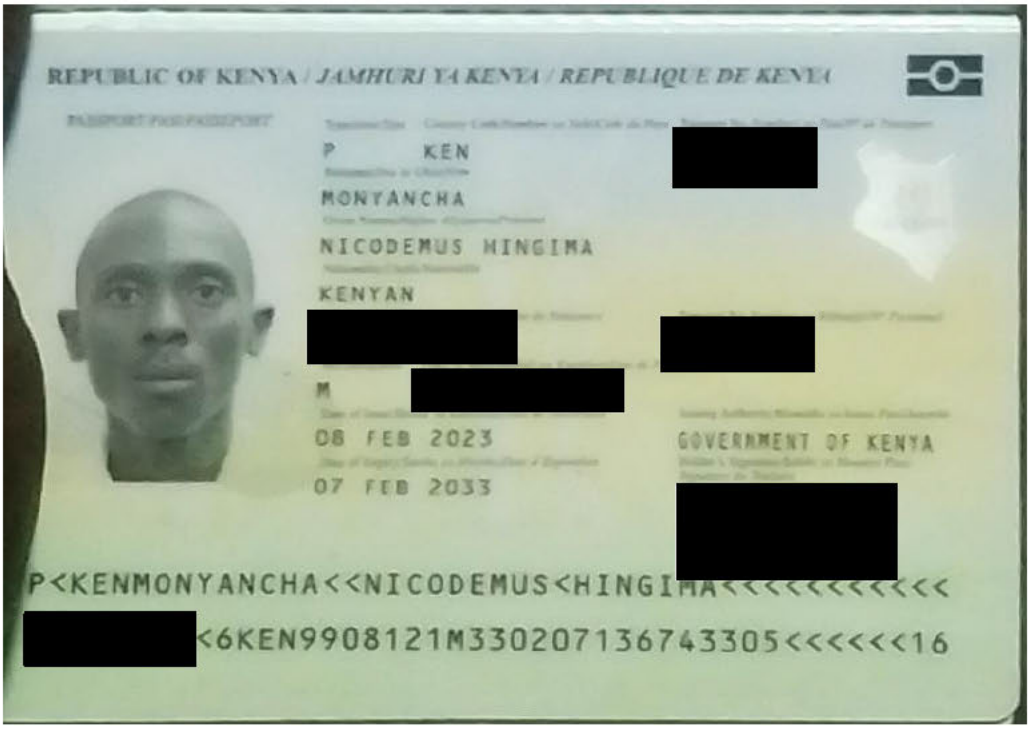
115. Binance records showed the following Binance account associated with NICODEMUS HINGIMA MONYANCHA:

Binance User ID: [redacted]

Name: NICODEMUS HINGIMA MONYANCHA

ID Document: Republic of Kenya Passport

ID Number: [redacted]



(Binance KYC document)



(Binance KYC document)

116. A review of access logs for Binance account [redacted] revealed 208 unique logs between 2025-04-08 04:10:49 to 2025-11-27 07:37:40 which had IP addresses geolocate to Antananarivo, Madagascar.

117. The following two Binance deposit addresses were attributed to Binance account [redacted]

[redacted]

118. The wallet [redacted] received two incoming transactions of USDt from [redacted] also funded 7 other co-conspirators' Binance accounts), which your affiant believes to be a payment account associated with the conspiracy (hereinafter, "Conspirator Payment Wallet 1"), on 03/31/2025 and 04/17/2025:

a. 213 USDt on 03/31/2025 17:38

b. 450 USDt on 04/17/2025 04:28

119. Approximately 82% of all USDt received by Conspirator Payment Wallet 1 to date was sent by [redacted] The FBI identified five separate IC3 reports, from four separate victims, which all contained narratives of being victimized by a fake NFT trading operation. All five reports listed [redacted] as an address where stolen funds were sent to. The five reports were filed between 03/06/2025 and 04/09/2026.

120. Based on the entirety of the evidence, there is probable cause to believe that Defendant was working as an employee of WA and under a contract with WA to scam individuals through the U.S. wires.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

121. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Affidavit and accompanying request for the issuance of a complaint and arrest warrant. I submit that Assistant U.S. Attorney Karen P. Seifert, an attorney for the United States, is capable of identifying our voices and telephone numbers for the Court.

CONCLUSION

122. Based on the forgoing factual allegations, there is probable cause to believe that the Defendants have committed violations of 18 U.S.C. §§ 1343, 1349 (Wire fraud conspiracy), and I respectfully request that the Court issue the complaint and an arrest warrant in this matter.

[redacted]

Special Agent, Federal Bureau of Investigation

Subscribed and sworn telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on October 23, 2026.

HONORABLE ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE