

UNITED STATES DISTRICT COURT
for the
District of Columbia

In the Matter of the Seizure of
(Briefly describe the property to be seized)

ONE TELEGRAM CHANNEL FOR
VIOLATIONS OF 18 U.S.C. §§ 1349, 1956

)
)
)
)
)

Case No. 26-sz-32

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under

18 U.S.C. §§ 981(a)(1)(A), 982(a)(1), 1343, 1349, and 1956(a)(1)(B)(i) & (h) and 28 U.S.C. § 2461(c)

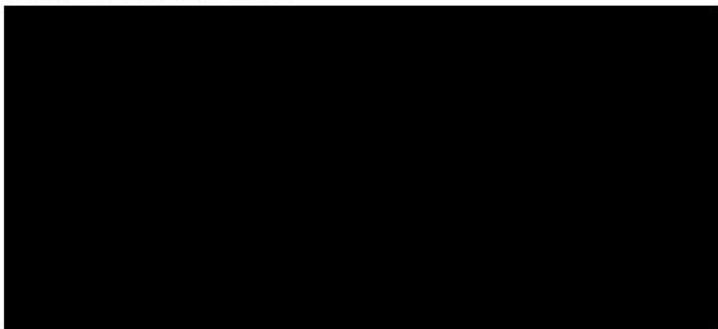
(describe the property):

ONE TELEGRAM CHANNEL, OPERATED BY TELEGRAM MESSENGER INC., Commerce House,
Wickhams Cay 1, PO Box 3140, Road Town, Tortola, British Virgin Islands VG1110

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, HEREBY INCORPORATED BY REFERENCE.

Continued on the attached sheet.



Attested to by the applicant in according with the requirements of Fed. R. Crim. P. 41 by telephone.

Date: 04/22/2026

Judge's signature

City and state: District of Columbia

Matthew J. Sharbaugh, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEIZURE OF
ONE TELEGRAM CHANNEL FOR
VIOLATIONS OF 18 U.S.C. §§ 1349, 1956

CASE NO. 26-SZ-32
FILED UNDER SEAL

Reference: USAO No. 2026R00309; Target Account: t.me/pogojobhiring2023

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

[REDACTED]

[REDACTED]

1. I make this affidavit in support of an application for a seizure warrant for the Telegram Channel associated with the invite link t.me/pogojobhiring2023¹ (**TARGET PROPERTY**). The **TARGET PROPERTY** to be seized is described in the following paragraphs and in Attachment A.

2. A search of publicly available information for the **TARGET PROPERTY** shows that the property is hosted by **TELEGRAM**, a cloud-based, cross-platform social media and instant messaging (IM) service, registered in the British Virgin Islands (BVI) with a legal address for correspondence usually listed as Conyers Trust Company (BVI) Limited, Commerce House, Wickhams Cay 1, P.O. Box 3140, Road Town, Tortola, VG1110, British Virgin Islands.

¹ According to Telegram's website, a Telegram channel is a tool for broadcasting one-way messages to unlimited subscribers, functioning as a public or private feed rather than a conversational group. It allows creators to send text, media, or large files (up to 2GB) to a large audience, with features like silent notifications, post-view counts, and optional linked discussion groups. Each Channel has an "owner," who can "broadcast messages, delete any messages, add subscribers (the first 200 only), remove subscribers, change the Channel's name, profile image and link, as well as delete the Channel completely. Any user can find and join a public channel, which has its own username.

3.

[REDACTED]

4.

[REDACTED]

PURPOSE OF AFFIDAVIT

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1343, 1349 (Fraud by wire, radio, or television, and conspiracy), and 18 U.S.C. § 1956(a)(1)(B)(i) & (h) (Laundering monetary instruments and conspiracy) have been committed by numerous unknown individuals operating out of a Cambodia-

based scam compound and their co-conspirators. There is also probable cause to seize the **TARGET PROPERTY** described in Attachment A as property subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1), and 28 U.S.C. § 2461(c).

6. The United States, through its agencies the FBI and the U.S. Secret Service (USSS), is investigating international criminal organizations operating fraud scams out of southeast Asia. Numerous schemes are run out of industrial-scale scam compounds in Cambodia. The criminal syndicates behind these compounds often lure unsuspecting persons to travel to Cambodia on the offer of high paying jobs. However, many of these persons instead have their identification documents seized and are forced to work in these scam compounds. Within these compounds, these trafficked persons, themselves victims, are forced to work long hours to conduct fraud schemes against victims from the United States and other countries.

7. According to victim reporting, discussed in more depth below, law enforcement is investigating a compound in the Anlong Veng district of Oddar Meanchey Province in northern Cambodia, near the Thai border. The compound is across the street from a large casino. Also according to victim reporting, trafficked persons brought to work at the compound have been subject to torture, abuse, and extortion. The compound is reportedly run through a mix of Chinese criminal actors.

STATUTES, JURISDICTION, AND VENUE

8. Title 18, United States Code, Section 1343 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.” Title 18, United

States Code, Section 1349 criminalizes the conspiracy to commit wire fraud, as defined in Section 1343.

9. Title 18, United States Code, Section 1956(a)(1)(B)(i) criminalizes “knowingly” “conducting or attempting to conduct a financial transaction which involves the proceeds of specified unlawful activity” where the defendant knows “that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.” Violations of 18 U.S.C. §§ 1343, 1349 qualify as specified unlawful activity under the statute. Title 18, United States Code, Section 1956(h) criminalize the conspiracy to commit money laundering, as defined in Section 1956(a).

10. This Court has jurisdiction to issue the requested warrant. Section 853(f) of Title 21 of the U.S. Code authorizes the government to obtain a seizure warrant from the court in the same manner as a search warrant under Federal Rule of Criminal Procedure 41. Further, Section 853(l) provides that a federal court has “jurisdiction to enter orders as provided in this section *without regard to the location of any property which may be subject to forfeiture*” (emphasis added). Section 853(f) provides that a court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **TARGET PROPERTY** for forfeiture. By seizing the **TARGET PROPERTY**, the government will prevent third parties from controlling or acquiring **TARGET PROPERTY** and using it to commit additional violations of 18 U.S.C. §§ 1343, 1349, and 1956.

11. This court has the authority to issue seizure warrants for assets located in a foreign jurisdiction pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that a seizure warrant

may be issued by a “judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C.] section 1355(b), and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement” (emphasis added).² Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts or omissions giving rise to the forfeiture occurred, even as to property located in a foreign jurisdiction. Further, 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.

12. This affidavit also is being submitted in support of a civil seizure warrant for the property pursuant to 18 U.S.C. § 981(b)(2). Such a warrant requires a finding of probable cause and may be obtained on an *ex parte* basis. Section 981(b) applies to all property subject to civil forfeiture under section 981(a). Under section 981(a)(1)(A), property subject to forfeiture to the United States includes “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of [18 U.S.C. §1956].” As discussed below, there is probable cause to believe that violations of 18 U.S.C. §§ 1343, 1349, and 1956 have been committed by numerous

² Notwithstanding the provisions of Rule 41(a), a seizure warrant may be “transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.” Here, however, Telegram has generally agreed to accept service of law enforcement process through its web portal. The United States will first attempt to serve Telegram through its web portal.

unknown individuals operating out of the Cambodia-based scam compound and the individuals responsible for the use of **TARGET PROPERTY**.

PROBABLE CAUSE

I. Background on Scam Compounds in Cambodia

13. Based on my training and experience in this and other investigations, I know that numerous cryptocurrency investment fraud (CIF) schemes are operated from industrial-scale scam compounds in Cambodia. The criminal syndicates behind these compounds often lure unsuspecting persons to Cambodia or neighboring Thailand with the offer of high-paying jobs. Upon arrival, however, many of these persons instead have their identification documents seized and are trafficked to scam compounds. Within these compounds, the trafficked persons, themselves victims, sometimes joined by willing scam workers, are forced to work long hours to conduct CIF schemes against victims from the United States and other countries.

14. According to public reporting, one of the original goals of these compounds was to host gambling operations, both online and in-person, for Chinese customers—an activity that is illegal in China. After the COVID-19 pandemic disrupted business plans for gambling centers, Chinese criminal organizations in these zones turned to fraud schemes, especially CIF, as a new source of revenue. And as lockdowns and border controls meant Chinese workers could not travel to Cambodia, these organizations began trafficking workers from around the world.³ A U.S. government funded study reported that beginning in 2021 “criminal trafficking networks” began to “lure a new multinational labor force into scamming enclaves in Cambodia, Myanmar, Laos,

³ United States Institute of Peace (USIP), Senior Study Group Final Report May 2024, *Transnational Crime in Southeast Asia A Growing Threat to Global Peace and Security*, at 8, available at https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.

and elsewhere with promises of well-paid, high-tech jobs. Today, there are an estimated 300,000 cyber scammers in the Mekong region, many of whom are held captive in prisonlike conditions and forced to spend long hours scamming unsuspecting targets”⁴

15. According to public reporting, Cambodia has been a hub of scamming activity for over the last ten years. “Between 2014 to 2019, . . . the number of casinos in Cambodia increased by 163 per cent: from 57 in 2014 to 150 in 2019.”⁵ “The Office of the United Nations High Commissioner for Human Rights estimates that criminal gangs are holding at least 220,000 people from more than 40 countries at scam centers in just Cambodia and Myanmar. . . . Though there are no official figures, the return on cyber scamming in Cambodia is estimated—by multiplying a conservative estimate of 100,000 laborers thought to raise an average of \$350 per person per day times the number of days in a year—to exceed \$12.5 billion annually, which is equivalent to nearly *half* the country’s formal GDP.”⁶

II. The Compound

A. Location

16. Anlong Veng district of Oddar Meanchey Province in northern Cambodia is located near the Thai border. The below map (Fig. 1) shows the location in Cambodia.

17. According to trafficking victims, described further herein, there is a compound located on Cambodia’s National Road 67, directly across from a casino, which is holding trafficking victims against their will and forcing them to commit scams (hereinafter “Anlong

⁴ *Id.* at 18.

⁵ Office of the High Commissioner for Human Rights, *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia* (Aug. 2023), at 6, available at <https://bangkok.ohchr.org/sites/default/files/documents/2025-01/online-scam-operations-2582023.pdf> (last accessed March 5, 2026).

⁶ *A Growing Threat* (May 2024) at 19 (emphasis added).

Compound”). Based on information provided by a trafficking victim (TV-1), law enforcement identified the location of the Anlong Compound. The approximate location of the Anlong Compound is 14.342082740033003, 104.0568921576074. Aerial of the location and street imagery of the location, as identified by a trafficking victim, follow (see Fig. 2).

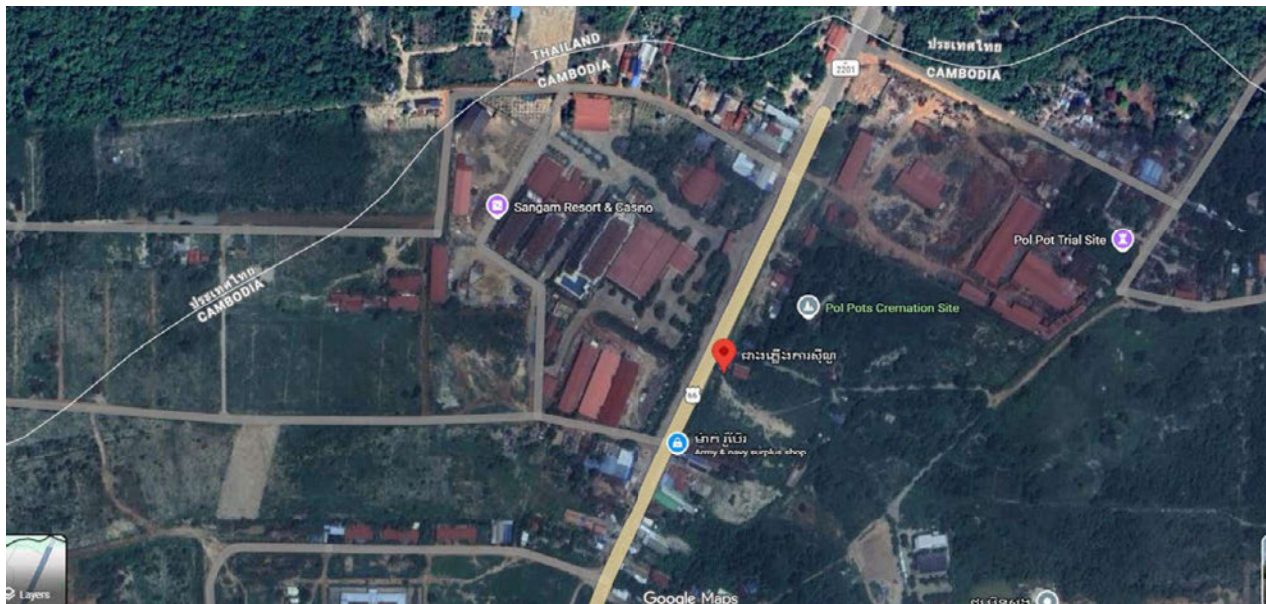


Figure 1 - Aerial Map of Anlong Compound

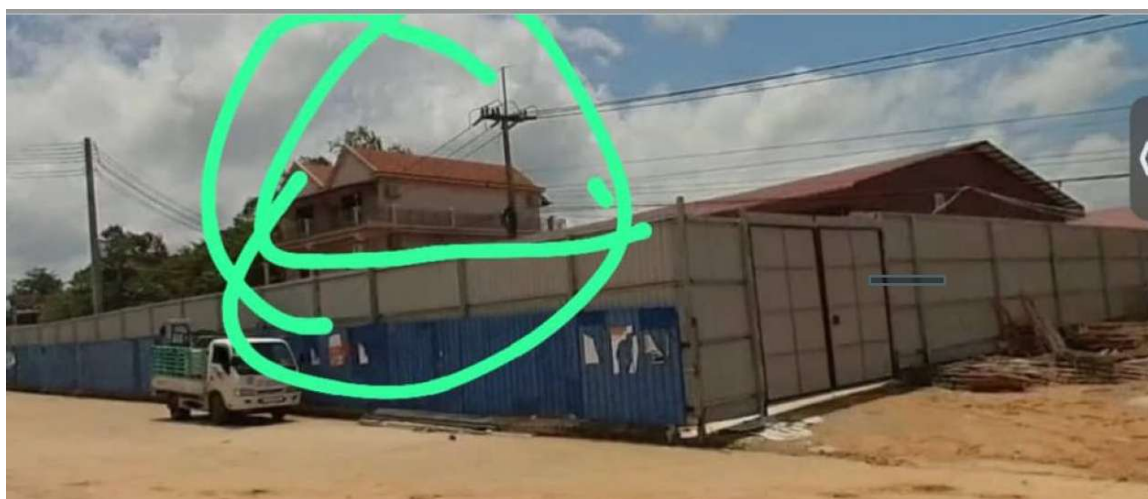


Figure 2 - Street View Identification of Anlong Compound by TV-1

18. In addition to TV-1, records of a U.S. Internet Service Provider (U.S. Provider 1) indicated scam activity coming from the same location. Specifically, U.S. Provider 1 records

showed ACCOUNT 1 and ACCOUNT 2 were identified according to location data as operating at the same location, and records of activity for ACCOUNT 1 and ACCOUNT 2 suggest that the accounts were involved in contacting unsuspecting victims located in the United States. Users of ACCOUNT 1 and ACCOUNT 2 engaged in unsolicited communications with users located in the United States and asked personal questions regarding their employment and investment accounts. Additionally, as is common in these schemes, the users of ACCOUNT 1 and ACCOUNT 2 suggested maintaining contact through mobile encrypted communication applications such as WhatsApp or Microsoft Teams. U.S. ISP 1 identified at least an additional 35 accounts conducting similar activity at the same location.

B. Trafficking Victim 1

19. Between March 18, 2026 and March 25, 2026, TV-1 was interviewed by law enforcement in the United States [REDACTED] During these interviews and communications with TV-1, TV-1 provided detailed information regarding recruitment, transportation, and working conditions at the Anlong Compound.

20. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] TV-1 reported there

were several individuals overseeing the compound who exercised control over workers, restricted

⁷ TV-1 contacted the Department of Justice on their own volition in order to report this conduct. TV-1 has not been compensated and has not asked for any benefits from the Department of Justice.

their movement, and closely monitored their activities. TV-1 further reported that there were approximately 20 employees at the scam center and the employees were required to work 12-hour shifts. Workers at the compound were not permitted to leave the compound without authorization.

21. TV-1 further described conditions consistent with coercion and stated that compound leaders confiscated TV-1's identification documents, money, and personal belongings, limiting TV-1's ability to independently leave the compound. Additionally, TV-1 observed that individuals who attempted or failed to comply with directives were subjected to threats and physical abuse. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

22. TV-1 reported the compound housed multiple foreign nationals, including Filipino workers, many of whom stated that they had been recruited under similar false pretenses. TV-1 indicated some individuals appeared unaware of the true nature of the work prior to arrival, consistent with the pattern of deceptive recruitment.

23. TV-1 reported that TV-1 was required to engage in scam activities directed by individuals overseeing the compound. This included the use of scripted communications with unsuspecting victims, including victims in the United States. These activities were supervised by the managers of the compound, all of whom were Chinese nationals, and performance-driven work and compliance were enforced through monitoring, correction, and punishment. According to TV-1, supervisors and project leaders directed and monitored the scamming communications to ensure adherence to the scripts. TV-1 identified three individuals by name involved in managing the

operations, and provided law enforcement with the names those individuals used. TV-1 further stated that an interpreter was used by the Chinese bosses to translate instructions and ensure that all workers understood and properly executed the scripted communications.

24. [REDACTED]

[REDACTED] Based on TV-1's statements, the conditions described are consistent with forced labor, fraud, and coercion that is typical to the CIF scam compounds described in publicly available reporting.

C. The Scheme

25. According to TV-1, individuals operating within the compound engaged in a coordinated scheme to defraud victims through the use of structured and scripted communications.

26. TV-1 stated workers in the compound were required to initiate and maintain contact with potential victims using designated communication platforms, specifically WhatsApp or Microsoft Teams, both of which are run by U.S. Internet Service Providers and use wires in interstate and foreign commerce to run the platforms. These interactions involved written scripts, which workers were required to follow. These scripts were designed to manipulate victims and induce compliance with financial or other demands.

27. TV-1 described that the scheme occurred in several stages. TV-1 stated that each successive stage increased the level of pressure on the victim and was intended to escalate the situation in order to induce the victim to comply with demands. The scam workers initiated contact, usually by telephone based on a list of U.S. persons, their phone numbers, and their Social Security Numbers, which was provided by the Chinese bosses. The scam workers were given a script and told to establish communication using the scripted language.

- a. Phase One: The scam worker poses as a bank employee, usually JP Morgan Chase, a U.S. financial institution, and tells the victim that a credit card issued in their name had purchased firearms and that the bank had flagged the transaction. The scam worker alleges that the victim's information was used to purchase firearms via the website of an actual U.S. firearm vendor (Firearm Vendor 1) and that such information needs to be provided to law enforcement. A copy of the script follows:

JP MORGAN SCRIPT

JP MORGAN CHASE BANK FRAUD ANALYSIS DEPARTMENT
ADDRESS: 383 MADISON AVE. NEW YORK, NY 10017
PHONE NUMBER: 212-270-6000

NEW YORK POLICE DEPARTMENT
ADDRESS: 2207 AMSTERDAM AVE. NEW YORK, NY 10032
PHONE NUMBER: 212-927-3200

This is JP Morgan Fraud Analyst, my name is __ May I speak with __

We are calling in regards with the transaction that was flagged on our system with your PLATINUM VISA CARD Ending in 9484. The card was used to purchase 4 FIRE ARMS with the amount of \$2,900.61.

We wanna verify if you authorized this transaction?

(If client answers NO: Thanks for letting us know, that's what we thought as it is shows as suspicious transaction on our end)

Let me validate this call first to know if I'm not mistaken.
I'm speaking with Ms/Mr/hase 4 FIRE ARM Last 4 digits of SSN __

(Client confirmed)

Thanks for confirming that I'm speaking with the correct person.

If you didn't authorized this transaction can you double check if you have the card on your possession?

(Client will mention that they don't recognize this card)

This could be a problem as it shows that this card was just recently issued to you here at JP Morgan Chase Bank New York last August 29 using your name and information that I used to validate this call.

Originally we contacted to know if you authorized the transaction but what you're telling me right now is you don't own a card ending in 9484.

I may need to inform our legal team about this and by the way this call is being monitored and recorded for security purposes.

We need to figure out how there was a card that was open without your knowledge.

Is there anyone else you've authorized to use your financial information who may have opened an account on your behalf?

(Thanks for letting us know, I'll make sure that it's properly documented)

Have you checked your credit report recently, and did you notice any accounts or inquiries that you did not approve.

Have you recently been notified by your bank or any company about a possible data breach involving your personal information?

Have you shared personal information recently (e.g., online forms, job applications, social media) that could have been accessed by someone else?

Have you lost your wallet, ID, or important documents in the past few months?

Based on your statement, it looks like this might involve identity theft. I will review the process to be sure as we rarely encounter this to make sure that I'm following the most up to date guidelines.

Can I place the call on hold for a few seconds?

Thanks for patiently waiting, the identity theft process begins with restricting the card to prevent any further transactions.

Next, we will require an official document or police certificate confirming that you are a victim of identity theft in order to proceed with the card cancellation.

Since someone used your personal information to buy weapons, there is a real risk that they could use those items for criminal activities.

And because the card and the purchase are all under your name any investigation could lead back to you unless you report it and you have an official report on file showing you are a victim of Identity theft.

The sooner you report it, the sooner you remove any connection to the illegal activities they might do. Reporting this protect both your financial security and legal standing.

I can share with you the details of the fraudulent card and the transaction made today, which you can provide to the police department as a basis for the report when you file it later.

Card Details:

Type of Card: Platinum Visa Card
Card Number: 4025-3330-5572-9484
Issuer Bank: JP Morgan Chase Bank
Address: 383 Madison Ave, NY NY 10017

Transaction Details:

Purchase: 4 Fire arms
Merchant: [REDACTED]
(online purchase)
Reference Number of this Call: 357382

Kindly record my name as well ___ as the one who informed you and I'm one of the Fraud Analyst of JP Morgan Chase Bank.

Please request for a Police Certificate that will serve as a proof that you are a victim and not the person responsible for this fraud.

And once our department receives the police certificate, that's the time we will

cancel the fraudulent card, remove your name from the system and ensure that no legal action is pursued against you regarding the illegal firearm purchases made using your information.

We will guarantee that our legal team provides the police certificate to the merchant so that the illegal firearms are not shipped.

And in addition to that, since the purchase and credit card was issued here in New York and you believe that your identity has been stolen, we recommend reporting this to the New York Police Department as the incident is linked here. This will help ensure the case is formally documented within the jurisdiction that has proper authority over the matter. I can share with you their address so you can go there personally.

(If client informed they're from a different state: Even though you're living on a different state, you can still file a report remotely)

I can check with our Legal Team to see if they can arrange a phone connection with the NYPD for you. You just have to make sure that you are in a quiet environment when speaking with them as that's part of their protocol for virtual assistance.

While waiting for an update from our legal team, do you have any other questions for me so I can address them properly?

- b. Phase Two: The scam worker notifies the victim that they need to be transferred to law enforcement, usually the New York Police Department. The scam worker transfers the call to another scam worker, who uses a “law enforcement script.” The scam worker convinces the victim to file a police report and elicits personal details from the victim. The scam worker tells the victim that their account has been linked to a known criminal organization and asks for a video call on Microsoft Teams or WhatsApp, both run by U.S. Internet Service Providers, to verify the victims’ identity. A copy of the script provided by TV-1 follows.

New York Police Department 33rd precinct
2207 Amsterdam Avenue NY , NY 10032
+1 212 927 3200

INTRO

- * New York police department , officer _____ , How may I help ?
- * Can you please tell me more about this matter in details please .
- * Aside from the report that you are filing today , have you legally purchased any firearms in the past ? Do you have any firearms license or permit ?

QUESTIONS

- * As you mention the card was issued in NEW YORK , do you have any family or relatives living in NEW YORK?
- * Is there anything you can recall that might help explain how your name ended up on this card?
- * Do you usually connect your phone to public WiFi , for example in the airport , restaurants , coffee shops ?
- * Did you had any conflict or arguments with someone that may motivate them to steal your information to use in this kind of fraudulent activities ?

Police Report

- * So you want to filed a police report regarding in this matter right ?
- * Before we proceed on filing a police report , may I ask for your Full name please
- * If you want to file a police report , you need to file a report to our department , once its completed we will issue a police clearance certificate , this will shows that you don't have any involvement in purchasing the firearms and you didn't authorize the card as well
- * Its actually best if you can come to our station so I can help you personally in completing the report , without your presence and completed report we cannot proceed with the investigation
- * Are you able to come to our station ?
- * Alright let me see what I can do here just give me a moment. Since you cannot come to our station I can request a special case for you so that we can handle this over the phone , is that okay with you ?
- * This phone call work same as filing a police report in person , so what I am going to say is very important , so I need your cooperation and follow my instruction can you do that ?
- * This phone call must be one on one , with only your voice and mine if anyone else interrupted our conversation the transcript will lost its legal effect , understand ?
- * So may I ask where are you currently at ? Are you at home or at work? Is there anyone else with you there ? Can you go to a quiet place or in a separate room so we can proceed with the transcript.
- * Please be advised that this call is being recorded for legal purposes ,under the

law everything you say in this transcript can be use as an evidence so you must tell us honestly and completely , Understand ?

TRANSCRIPT

The transcript is now officially begin today is (Month/Date/Year). This case involve the unauthorized use of an individual personal information . Where the name (Client Name) was fraudulently use for illegal activities , I am Officer Ashley Rodriguez , Badge No. 5271 of New york police department. I am creating an official record for the reporting party , For the transcript please state your full name and your date of birth

Now please take any of your ID or If you have a driver license that will be better , Tell me the ID number three digit at a time so the recording system can capture them clearly , this is only to confirm that it is you making an online report to the NYPD , you may begin when you are ready.

Thank you , Now can you please explain again what happen and why you decide to report this incident to us today , please explain clearly and provide all the relevant details that you have.

FAMILY AND WORK

Now I will be asking about your personal background to see if there are circumstances that could link you to the card in question,

- * Do you currently live with any of your family member?
- * Do you have any conflict or dispute with any of your family member , friends or relatives ?
- * Does anyone in your household have an access with your personal documents , Bank account , passport and other financial information ?
- * May I ask what is your current occupation ?
- * How long have you been employed there ?
- * Do you have any conflict or Dispute with you colleagues or boss ?

I hope you understand that giving false information that may lead to further legal consequences , Do you confirm that the answer you provided to me are true and complete to the best of your knowledge ?

Please stay on the line , I will give a heads up call to the headquarter to see if they have any additional information about you.

WALKIE TALKIE

OFFICER 01 : 01 calling headquarters , 01 here please respond over!

OFFICER 02: Headquarters received , 01 go ahead over!

OFFICER 01 : I need help verifying the identification of the citizen ID type is ____ ID number ____ . Over

OFFICER 02: Headquarters received , The ID type is ____ ID number ____ has been verified

OFFICER 01 : Returning to headquarter , This individual name appeared in connection with the illegal purchased of firearms through the online platform called [REDACTED] the citizen stated that he/she has no knowledge of this activities and that the card used was not belong to he/him. Please gather any additional related information . Over!

OFFICER 02: Headquarters received 01 , we are checking please wait
WAIT FOR 2 MINUTES

OFFICER 02 : Headquarters here , please respond to home call 01 , This is an emergency 01 , Over!

OFFICER 01 : 01 here , go ahead headquarters

OFFICER 02 : Back to 01 , The Citizen full name is ____ , ID number ____ is linked to a CITIBANK account ending in 3065 , opened on March 28 , 2025. This account is linked to CHEN HAO International drug and money laundering case involving up to \$250 ,000. This account is flagged as a suspicious. Treat is a warning account 01.

OFFICER 01 : 01 Copy , Please send all documents and evidence about this person immediately Over!

OFFICER 02 : Headquarters copy , we will send it immediately.

TEAMS/WHATSAPP

While waiting for the documents from the headquarters , may I ask if you have Microsoft Teams ? Because the information that I received from the headquarters is confidential , I need to conduct a video call to verify if I am speaking with the right person in the ID number that you provided to me.

WHILE ON VIDEO CALL

Can you please show me the ID that you provided to me a while ago , hold the idea and move backward.

Take a photo of this ID front and back then send it to me so I can attached it with your case file.

Thank you , Now we will proceed with the discussion.

CHEN HAO

I already have the documents and evidence from the headquarters , Let me read it to you .

From the documents that I receive , it says here that there is a CITIBANK account that registered under your name , the account ends in 3065 and it was open last March of 2025. The phone number that linked to this account is the one that you are using right now.

- c. Phase Three: The scam worker has a call with the victim on Microsoft Teams or WhatsApp. During that call, the scam worker tells the victim that a bank account,

with another bank (often Citibank) in their name has been linked to a money laundering investigation, purportedly being conducted by Homeland Security Investigations. During this portion of the scam, the scam worker also elicits from the victim (under the guise of cooperating with an investigation) the victim's personal bank account information. A copy of the script provided by TV-1 follows.

This card was linked to an ongoing investigation involving Chen Hao. The investigation concern serious crimes of money laundering and human trafficking. I need to know what is your connection with this account and what is your connection with Chen Hao as well , Do you know someone name Chen Hao ? I will send you his picture , take a look at it and think carefully if you already encounter this person.

Do you have any CITIBANK account except for this account ending in 3065?

Chen Hao is a previous Manager in CITIBANK , that is why I am asking if you have any other CITIBANK account.

The account under your name is currently under investigation of HSI (Homeland Security Investigation) and the prosecutor handling Chen Hao case.

This case considered highly confidential. You are not allowed to share any details of this case to anyone. Breaking this law could lead to severe legal consequences.

Our record shows that the account that register under your name have \$250,000 that linked to Money laundering activities , HSI is investigating any connection you might have with Chen Hao who is the primary suspect.

Chen Hao used to work as a bank manager , giving him access to financial system. He is now identified as a leader in a criminal organization involved on Money Laundering and Human Trafficking.

Right now we are still investigating the situation , An arrest warrant has been prepared in case evidence show you are strongly work with Chen Hao , but it has not been signed yet so you still have the chance to explain yourself and gather more evidence that may prove that you are not connected with Chen Hao.

Your cooperation is essential , it will help us determine whether your are a victim of an identity theft or if you have a deeper connection with the main suspect.

In our recent raid we found money , drugs , fake passports and more than 200 bank card that linked to a money laundering activities .

This is a very serious situation , The evidence against you is significant and we need your cooperation to clear your name as of now we have 3 main pieces of evidence against you.

PHYSICAL EVIDENCE - A bank card under your name was found use by CHEN HAO for illegal activities

FACTUAL EVIDENCE - Your account received ransom money in a child abduction case , which has been disappeared. NYPD'S HIS and the prosecutor are investigating.

THIRD PARTY EVIDENCE - 32 Victims submitted remittance slip showing CHEN HAO instructed them to transfer money into your account.

Because of the seriousness of this case , we need to confirm your involvement as quickly as possible , cooperation now gives you the best chance to clear your name

On our recent investigation , we found out that some of CHEN HAO accomplices are Bank Managers , Teller , Security Guards , Some government official and even high ranking police are involve in manipulating the transaction inside the bank. So we need to be extra cautious because we are not sure what are those criminal are capable of .

I will give you a call tomorrow to provide an update on this case.
You might received some random calls , massages and emails from unknown individuals please don't answer any of it , in this stage of investigation some of other suspect might try to gather some more information about you , once they find out that we are investigation they might find way to destroyed all the evidence that we have to clear your name. Be more exercise cautious.
Agsin , This is officer Ashley Rodriguez , NYPD Division .

I will send you the confidential order , I need you to sign it and then send it back to me . You also need to do a hand written statement to clear out your name with this matter take a picture of the written statement and then send it to me via TEAMS / WHATSAPP

Because of that we have two government order has been issued :
THOROUGH INVESTIGATION ORDER - Everyone connected to this case including you will be fully investigated
CONFIDENTIALITY ORDER - You cannot share any information about this case with anyone including your FAMILY , FRIENDS or CO-WORKERS , breaking this law could result in immediate arrest and prosecution.

If you are really innocent then you should cooperate with us to clear out your name , providing what authorities required you will be a big help to close this case as soon as possible.

BANKING DETAILS

Now I will be needing to ask for your bank details as part of the official investigation . Because there is a money laundering activities involve the New York State Department of Financial Service will review your account to verify your account activity and determine which account was opened by you and which account was opened by Chen Hao , also to check for any unauthorized transaction and determine whether your name was use for illegal activities , providing these details help us clarify your involvement and gather evidence to resolve this case accurately.

- * How many bank account do you have ?
- * In which bank are this account under ?
- * How far is this bank from your home ?
- * Do you have an online access with this bank ?
- * Provide me the last 4 digits of this accounts
- * What are the purpose of this accounts ? why did you open this ?
- * Have you notice any unusual transaction in your account recently ?
- * Do you deal with Virtual Currency ?
- * Do you have any Mutual Funds ?
- * Except to you , is there anyone have an access with your bank ?

Once the New York State Department of Financial Service completes the investigation, if your bank was cleared the findings will support your case and help resolve this matter as soon as possible.

ENDING

Our conversation will continue tomorrow , you must fully cooperate as you are still considered as a suspect , you will need to report via TEAMS/WHATSAPP
Please confirm what time are you available tomorrow ?

d. Phase Four: the scam worker transfers the victim to an alleged court facility, sometimes referred to as the Supreme Court of New York. TV-1 did not have access to the script for this phase; however, as described further herein, several U.S. victims reported to the FBI that they were told they needed to pay fines to “cooperate” and avoid any criminal charges.

28. TV-1 reported that workers were evaluated based on their ability to effectively implement the scripts and communication with victims. According to TV-1, individuals with stronger English-language skills, particularly those able to speak fluent American English, were preferred for certain roles within the operation.

29. TV-1 further stated that workers’ activities were monitored and controlled and that failure to comply with directives or meet performance expectations could result in punishment.

30. Based on TV-1’s statements, the operation utilized scripted misrepresentations and impersonation tactics to induce victims to provide money or other things of value, consistent with a coordinated CIF scheme.

D. Trafficking Victim 1 Identifies TARGET PROPERTY

31. On or about March 18, 2026, and several times thereafter, TV-1 reported that **TARGET PROPERTY** was used by the compound to recruit other trafficking victims to work in the compound. The **TARGET PROPERTY** has an invitation link and associated domain address of t.me/pogojobhiring2023. The group name is **POGO JOB HIRING 2023!!!!**, and the group has 6,564 members.

32. A display of the publicly available website for the **TARGET PROPERTY** shows as follows:

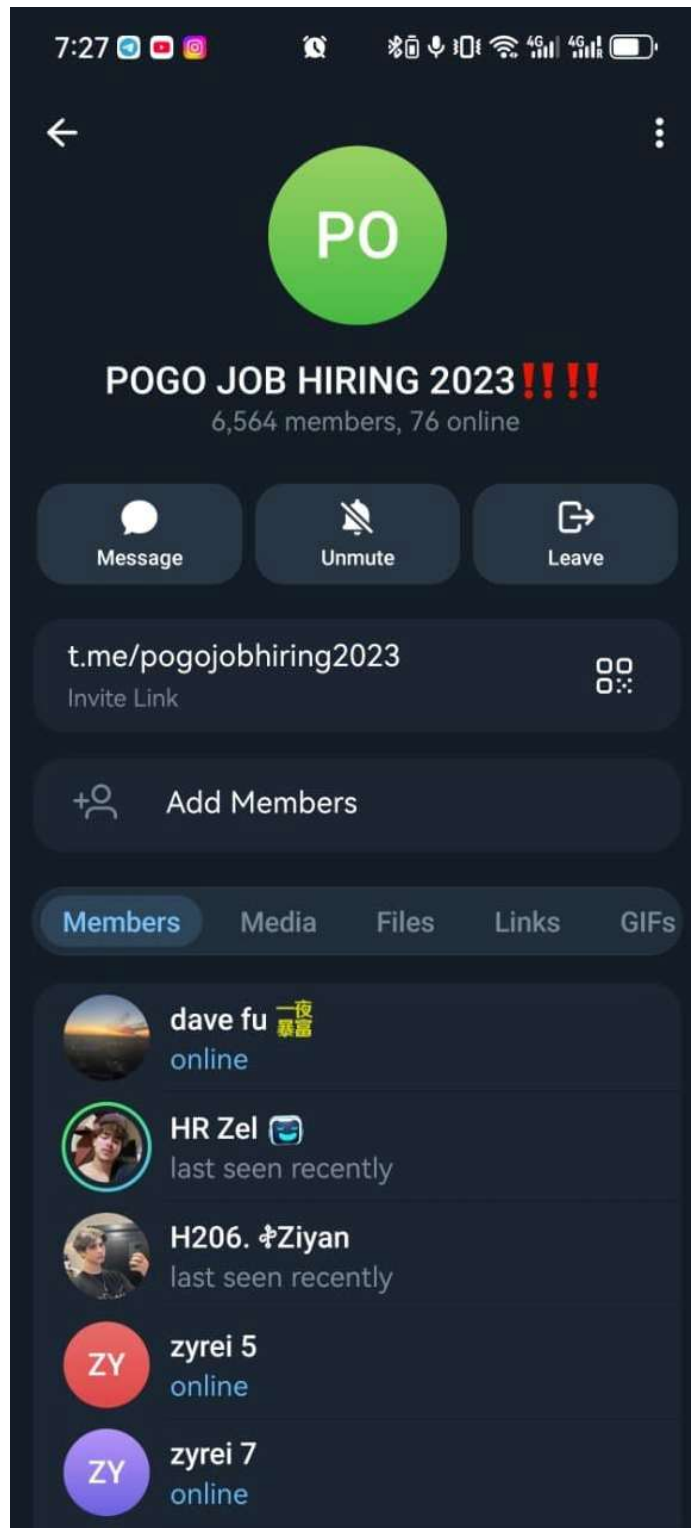


Figure 3 - Landing Page for TARGET PROPERTY

Louisa
 🤗 WE ARE HIRING 🤗

★ Female
 ★ 21-25 years old

📍 Working location : Cagayan Valley, The Philippines 📍

DEALER
 Nationality: Filipino
Salary: 30k-50k PHP + Performance
 Height must be at least 5'1 ft (155cm) and up
 No marks or tattoo on visible parts of the body
 No sweaty hands
 Please remove braces when applying.

Interested Applicants. please send your SET-CARD to:
 @tmejown
 Thank you so much!

10:24 AM

Figure 4 - Job Post Solicitation from member in TARGET PROPERTY

Haonan Network Co., Ltd
 Open to citizens of: Indonesia, Malaysia, Vietnam, **Philippine**, Myanmar, Laos, Taiwan, Philippines

📍 Location: Yerevan ,Armenia 🇦🇲

Position Available:

- ◆ Customer Service Operations – 1500–2100 USD
- ◆ Operations Team Leader / Supervisor – 2000–4000 USD
- ◆ General Management Department Supervisor – 2500–4000 USD
- ◆ General Manager Assistant – 1800–2500 USD
- ◆ New Media Operations Specialist – 12,000–16,000
- ◆ Overseas Social Media Advertising Specialist / Manager – negotiable
- ◆ Golang Engineer – negotiable
- ◆ H5 Engineer – negotiable
- ◆ Unity Game Developer – negotiable
- ◆ (HR) recruiter (Malaysia, Vietnam) - no need chinese language
- ◆ Customer Service WFH

Job Requirements:

- ◆ Proficient in Chinese

Benefit:

- ◆ Monthly allowance
- ◆ Performance bonus
- ◆ Free meal + accomodation
- ◆ 2 Day off per Month

Contact Information:
 Whatsapp : +855 963437548
 Telegram : @HrBaozi
 Telegram channel : @Loker_Armenia

Figure 5 - Job Post Solicitation from member in TARGET PROPERTY


FEMALE TELEMARKETING STAFF

- Full-time | Onsite | Pasay
- With Telemarketing/Telesales experience (BPO/Telco required)
- Team Leader experience is a plus
- Handles outbound calls, meets targets, supports & guides team
- Can work under pressure and start ASAP

Offer: Competitive salary, incentives & career growth

APPLY NOW:
 sophiamarie04042016@gmail.com
 Telegram: @MxSM0404 **WE ARE HIRING – PASAY CITY**

Multiple Open Positions Available

HR Ly 
WE ARE HIRING

WE'RE HIRING – START ASAP!

ONE-DAY APPLICATION PROCESS ONLY!

WORK FROM HOME
 POSITION: TELEMARKETING / CASINO AGENT

EARNINGS & PAYOUT:

- ✓ ₱100 per FTD
- ✓ Load Budget
- ✓ Monthly Bonus
- ✓ Weekly payouts
- ✓ Leads Provided
- ✓ Cut-off Period: Monday - Sunday
- ✓ Salary release: Monday-Tuesday

Comfortable to work in a commission based set up (Per FTD)

APPLY NA AGAD!
https://t.me/HR_Sam01

Figures 6 & 7 - Job Post Solicitation from members in TARGET PROPERTY

Urgent Hiring in Cambodia
 Direct company hiring.

- Need only Those people are already in Cambodia.
- Nationality- Pakistani, Indian, Nepali, Bangladeshi, Phillipines, African speak American accent

Night Shift – 10 PM to 10 AM
Salary up to \$1,100 + 3.5% Commission
 Indian & Pakistani & Chinese Meals Provided

Requirements:

- Hindi: Excellent
- English: 60-80%
- Age: 20-40 (flexible for experienced and fresher)
- Call center experience (advantage)

Salary Tiers:

- Line 1: \$800+200/month (with attendance) + 3.5% commission
- Line 2: \$800+200(with attendance)\$1,000 + 3.5% commission
- Line 3: \$1,100/month + 200% + 3.5% commission
- Monthly 2 days off
- Company will provide full safety for employees.
- Work contract 1 year.
- Without passport and visa also accepted

• Agents are welcome for cooperate agent money 1000\$ without passport 500\$, Phillipino nationality 1500\$

Responsibilities:
 Handle calls, provide support, meet targets, maintain records, and deliver quality service.

Figure 8 - Job Post Solicitation from members in TARGET PROPERTY

33. I have reviewed the **TARGET PROPERTY**, and it is consistent with that account provided by TV-1. Generally the activity in the **TARGET PROPERTY** demonstrates that members “post” what appear to be lucrative job opportunities in customer service, telemarketing, casino agents, and other opportunities at various purported locations such as Malaysia, Philippines, and Cambodia among other countries. Many of the job opportunities advertised on the **TARGET PROPERTY** purport to offer attractive salaries, commissions, travel expenses, and meals. Additionally, some of the job opportunities advertised request that the applicant meet certain physical characteristics such as no visible tattoos, marks, or braces.

34. Based on my training and experience, I know that individuals engaged in fraudulent schemes often use messaging platforms such as Telegram to advertise purported job opportunities that are misleading or entirely fictitious. Legitimate and reputable companies do not typically rely on Telegram as a primary means of recruiting applicants, making such postings indicative of potential fraud.

35. Additionally, based on my training and experience, I know that in the commission of the fraud scheme, the individuals recruited to work in these compounds are often required to have video and telephone conferences with unsuspecting victims. Therefore, the job opportunities posted on the **TARGET PROPERTY** request applicants with specific physical appearances or language abilities in order to meet their specific illicit objective.

D. Identification of Fraud Victims

36. Your Affiant queried the FBI Internet Crimes Complaint Center (ic3.gov) for any reports by victims who identified being defrauded via the scheme, specifically involving the

firearms sale website listed in the script above (WEBSITE 1).⁸ Your Affiant identified approximately 267 victims who filed reports consistent with the scheme, as described above.

37. Each ic3.gov complaint includes a narrative in which the fraud victim describes the scheme by which they were defrauded. Your affiant has reviewed these narratives and the corresponding reported information, all of which appear consistent with the information provided by TV-1 about the manner in which the scam campaigns were conducted by the co-conspirators. Examples follow.

U.S. Fraud Victim 1

38. One such U.S. fraud victim, Fraud Victim 1 (FV-1), located in La Jolla, California, was a victim of the scheme described above. FV-1 reported to the FBI that in or around August 2025, FV-1 received a phone call from an unknown caller posing as an American Express representative. This unknown caller told FV-1 that a credit card account was opened in FV-1's name and was used to purchase firearms on WEBSITE 1. FV-1 believed FV-1 was the victim of identity theft. Sometime later in or around November 2025, FV-1 received a phone call from someone posing as a Citibank representative. The unknown caller claimed a credit card account was opened in FV-1's name and was used to conduct fraudulent activity. The unknown caller posing as the bank representative claimed that FV-1 needed to report this incident to law enforcement. Believing that the prior phone call from in or around August was related, FV-1 agreed to be connected telephonically to whom FV-1 believed was law enforcement. This second unknown caller told FV-1 that FV-1's account was linked to criminal activity and that FV-1's status could change from "suspect" to "victim" only through full cooperation with the unknown caller.

⁸ Your affiant has made multiple (unsuccessful) attempts to contact the owner of WEBSITE 1, a resident of Florida.

FV-1 was later told by an unknown caller posing as a “prosecutor” that a “manual review” needed to be conducted of FV-1’s investment funds and demanded that FV-1 cash out FV-1’s 401k investments.

39. FV-1 was fraudulently induced by the coconspirators to send the following amounts from FV-1’s U.S. financial institution (USFI) to several accounts held at different financial institutions. Each of these wire transfers was to a different company, the details of which and the account numbers were provided by an unknown caller posing as a “prosecutor”. Based on my training and experience in this and other investigations, they appear to be “shell companies” used to move funds in a money laundering scheme.⁹

	DATE	TYPE	FACILITY	AMOUNT	BENEFICIARY
a.	12/01/2025	Wire Transfer	USFI 1	\$595,000	Shell Company 1
b.	12/18/2025	Wire Transfer	USFI 1	\$589,000	Shell Company 2
c.	1/2/2026	Wire Transfer	USFI 1	\$414,000	Shell Company 2
d.	2/3/2026	Wire Transfer	USFI 1	\$100,369.36	Shell Company 3

U.S. Fraud Victim 2

40. Fraud Victim 2 (FV-2), located in Sugarland, Texas, was a victim of the scheme described above. FV-2 reported to the FBI that in or around September 2025, FV-2 received a call from an unknown caller posing as a Wells Fargo Bank representative. The unknown caller falsely and fraudulently told FV-2 that an account was opened in FV-2’s name and was used to purchase multiple firearms on WEBSITE 1. The unknown caller posing as a bank representative told FV-2

⁹ For the purposes of this affidavit, a “shell company” is a corporate entity that does not have an online or physical presence and does not appear to conduct business beyond the movement of funds.

that FV-2 needed to report this identity theft to the FBI and transferred the call to a second caller posing as a law enforcement officer with the FBI in New York. The second caller posing as a law enforcement officer told FV-2 that FV-2 in fact was the suspect of a money laundering investigation and would be arrested and “taken from [FV-2’s] family”.

41. FV-2 was fraudulently induced by the coconspirators to send the following amounts from FV-2’s USFI to several accounts held at different financial institutions. Each of these wire transfers was to the same shell company, the details of which and the account number was provided by an unknown caller posing as a “prosecutor”.

	DATE	TYPE	FACILITY	AMOUNT	BENEFICIARY
a.	11/25/2025	Wire Transfer	USFI 2	\$50,000	Shell Company 4
b.	11/26/2025	Wire Transfer	USFI 2	\$120,000	Shell Company 4
c.	12/09/2025	Wire Transfer	USFI 2	\$121,000	Shell Company 4

U.S. Fraud Victim 3

42. Fraud Victim 3 (FV-3), located in Pompano Beach, Florida, was a victim of the scheme described above. FV-3 reported to the FBI that in or around November 2025, FV-3 received a phone call from someone posing as a representative from the JP Morgan Chase fraud department. The unknown caller posing as a bank representative told FV-3 that an account was opened in FV-3’s name and was used to purchase firearms on WEBSITE 1. The caller told FV-3 that FV-3 was the victim of fraud and needed to report this incident to the New York Police Department (NYPD). The second caller posing as a detective with the NYPD told FV-3 that the matter was confidential and later transferred FV-3 to a separate unknown caller posing as a “prosecutor”. FV-3 was instructed to send funds to an “FBI Account” for verification.

43. FV-3 was fraudulently induced by the coconspirators to send the following amount from FV-3's USFI to another likely shell company account at a financial institution; the account number was provided by an unknown caller posing as a "prosecutor".

	DATE	TYPE	FACILITY	AMOUNT	BENEFICIARY
a.	12/01/2025	Wire Transfer	USFI 3	\$2,500	Shell Company 5

U.S. Fraud Victim 4

44. Fraud Victim 4 (FV-4), located in Saint George, Utah, was a victim of the scheme described above. FV-4 reported to the FBI that in or around September 2025, FV-4 received a phone call from someone posing as a representative from the JP Morgan Chase fraud department. The unknown caller posing as a bank representative told FV-4 that a credit card account was opened in FV-4's name and was used to purchase firearms on WEBSITE 1. The caller told FV-4 that FV-4 needed to report this incident to the FBI and purported to transfer the call to the FBI. The second caller posing as a law enforcement officer with the FBI told FV-4 that FV-4's name was associated with a large money laundering investigation. FV-4 was asked by the unknown caller to send photos of FV-4 for verification, was asked to maintain daily contact, and was asked to make a recorded statement. Approximately a week later, FV-4 was told by an unknown caller posing as law enforcement that FV-4 would be detained if "bail money" was not sent.

45. FV-4 was fraudulently induced by the coconspirators to send the following amounts from FV-4's USFI to two accounts held at different financial institutions located in Hong Kong. Each of these wire transfers was to a different bank held in the name of different account holders, the details of which and the account numbers were provided by an unknown caller posing as law enforcement.

	DATE	TYPE	FACILITY	AMOUNT	BENEFICIARY
a.	9/17/2025	Wire Transfer	USFI 4	\$10,000	Shelly Company 7
b.	11/06/2025	Wire Transfer	USFI 4	\$28,000	Shell Company 8

U.S. Fraud Victim 5

46. Fraud Victim 5 (FV-5), located in Orlando, Florida, was a victim of the scheme described above. FV-5 reported to the FBI that on or around January 2026, FV-5 received a phone call from someone posing as a representative from the JP Morgan Chase fraud department. The unknown caller posing as a bank representative, told FV-5 that a credit card account was opened in FV-5’s name and was used to purchase firearms on WEBSITE 1. The caller told FV-5 that FV-5 needed to report this incident to the NYPD and purported to transfer to the call to the NYPD. The second caller posing as a law enforcement officer with the FBI asked FV-5 for their identifying information and told them their name was associated with a large money laundering and human trafficking investigation. FV-5 was told by the unknown caller that FV-5 would be transferred to someone who would be conducting a “trace review”.

47. FV-5 was fraudulently induced by the coconspirators to send the following amount from FV-5’s USFI to an account at a financial institution; the account number was provided by an unknown caller posing as someone affiliated with the NYPD:

	DATE	TYPE	FACILITY	AMOUNT	BENEFICIARY
a.	02/02/2026	Wire Transfer	USFI 5	\$58,379.20	Shell Company 6

E. TARGET PROPERTY Involvement in Cryptocurrency Money Laundering

48. In addition to the above reports, multiple victims reported transferring money to the coconspirators via cryptocurrency wallet transfers. A list follows:

Victim No.	Date of Transfer	Amount of Transfer	Wallet ID
FV-6	12/4/2025	\$23,000	Ending in ***pw7w5
FV-7	12/30/2025	\$150,000	Ending in ***975b9
FV-7	1/21/2026	\$235,000	Ending in ***87d01
FV-7	1/26/2026	\$20,000	Ending in ***87d01
FV-7	2/17/2026	\$150,000	Ending in ***87d01

U.S. Fraud Victim 6

49. Fraud Victim 6 (FV-6), located in Rockyhill, Connecticut was a victim of the scheme described above. FV-6 reported to the FBI that on or around December 4, 2025, FV-6 received a phone call from someone posing as a representative from a bank fraud department. The unknown caller posing as a bank representative, told FV-6 that a credit card account was opened in FV-6’s name and was used to purchase firearms on WEBSITE 1. The caller told FV-6 that FV-6 needed to report this incident to law enforcement and purported to transfer to the call to a law enforcement agency located overseas. The second caller posing as a law enforcement officer asked FV-6 for their identifying information and told them their name was associated with a large money laundering and human trafficking investigation. FV-6 was told by the unknown caller that FV-6 had a freeze order on their accounts and monies needed to be sent to a crypto platform to complete a “funds notarization process”.

50. FV-6 fraudulently induced by the coconspirators to send the above amounts from FV-6’s account at a U.S.-based cryptocurrency exchange, Coinbase.

U.S. Fraud Victim 7

51. Fraud Victim 7 (FV-7), located in Chicago, Illinois, was a victim of the scheme described above. FV-7 reported to the FBI that on or around March 12, 2026, FV-7 received a phone call from someone posing as a representative from the Wells Fargo fraud department. The unknown caller posing as a bank representative, told FV-7 that a credit card account was opened in FV-7's name and was used to purchase firearms on WEBSITE 1. The caller told FV-7 that FV-7 needed to report this incident to a law enforcement agency overseas and purported to transfer to the call to the law enforcement agency. The second caller posing as a law enforcement officer asked FV-7 for their identifying information and told them they were a suspect of an ongoing investigation and there was an "extradition order" to send FV-7 to Shanghai detention center for a sentence of up to two years. FV-7 told the unknown caller they did not want to go to China. The unknown caller sent FV-7 a "bail letter" and told them they needed to pay \$300,000 through cryptocurrency.

52. FV-7 fraudulently induced by the coconspirators to send the above amounts from FV-7's account at a U.S.-based cryptocurrency exchange, Coinbase.

53. Analysts from the USSS, who specialize in cryptocurrency tracing, reviewed the publicly-available blockchain regarding the transfers of these victim funds. The transactional patterns used to move the victims' proceeds revealed that many of the funds originating from the scam addresses engaged in "token-swapping." This process involves the transfer of one form of virtual currency token, in this case Bitcoin, for another, such as USDT. The swapping of virtual currency provides opportunities for money launderers to introduce additional complexities in obfuscation. Money launderers often swap coins or tokens for USDT because of its attractive features. USDT is desired because of its low transaction fees and stability compared to other more

volatile cryptocurrencies, as well as its demand in global markets making it easier to cash out once it reaches its destination point. Additionally, USDT is compatible on several different blockchains. CIF syndicates will use tokens that can be traded on multiple blockchains to help in concealing the origin of illicit funds and to add to the complexity, knowledge, and required steps needed for those who are tracing them. This money laundering technique is often referred to as “chain-hopping” and in this case’s instance occurred through “bridging”, the process of transferring assets between blockchain networks.

54. Both techniques of “chain-hopping” and “bridging”, also known as “token-swapping”, require an otherwise unnecessary and costly number of transactions. Criminals will deploy these techniques in the transfer of funds to layer ill-gotten funds, ultimately to conceal or disguise the nature, location, source, ownership, or control of those proceeds. The large number of rapid transfers, each occurring fees associated with the transactions, and with no apparent business purpose, of transactions throughout this case is a strong indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity (in this case, wire fraud).

55. Blockchain analysis showed that the controllers of the scam addresses utilized this technique of “bridging” on multiple occasions throughout the movement of the victims’ proceeds to include in the movement of proceeds derived from FV-6’s transactions on or about December 4, 2025, and FV-7’s transactions on or about December 30, 2025.

56. As shown in Figure 9 below, the controllers of the scam addresses utilized the bridging technique to swap FV-6’s originating Bitcoin transfer for USDT on the Tron network [REF: TXID: ending in ***57966]. Following the bridging, the controllers transferred FV-6’s proceeds to a wallet address ending in ***2Fq34 (scam address E2Fq34). Scam address E2Fq34

was blocklisted by Tether International S.A. de C.V. (d/b/a Tether Limited) at the request of law enforcement.



Figure 9 - Transactional pathway of Victim A.A. funds through bridges to blocklisted scam address E2Fq34.

57. A review of scam address E2Fq34 showed that it engaged in direct funds transfers between several high risk exchanges to include Xinbi Guarantee, a Chinese language telegram marketplace that was designated in or around March 2026 by the United Kingdom’s Foreign, Commonwealth and Development Office (FCDO), as an illicit marketplace responsible for crypto-enabled scam infrastructure scam services and pig-butchering fraud models [REF TXID: ending in ***e4dee9], and Hawang Guarantee, an associated entity of cryptocurrency exchange Huione Guarantee that in 2025 was declared by the U.S. Financial Crimes Enforcement Network (FinCen) as a primary money laundering concern for scam centers and crypto investment fraud [REF TXID: ending in ***756e2].

58. Blockchain analysis associated with FV-7’s transactions showed that the controllers of the scam addresses utilized “bridging” techniques before splitting the victim proceeds between multiple destinations. One of the destinations included a transfer to the cryptocurrency exchange Nested Exchange Limited (d/b/a Binance), 4606 Addax Tower Abu Dhabi, UAE, via the deposit address: ending in ***ZaN4iF [REF: ending in ***b6e52].

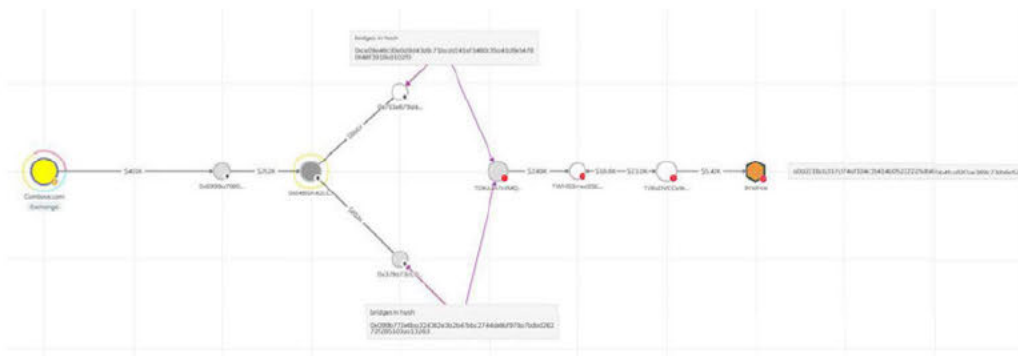


Figure 10 - Transaction Pathway of W.A. funds bridging to Binance deposit: wallet ending in *aN4iF.**

59. Business records of Binance revealed that the deposit address at Binance (Wallet ending in ***aN4iF) was associated with user ID #1195669929 under a Malaysian Passport (Fig. 11) to an individual with a Gmail email address.



Figure 11 - Passport Provided by Binance User ID#1195669929

60. A review of User ID #1195669929 account revealed that the Internet Protocol (IP) logins associated with the account's activity resolved back to Phnom Penh, Cambodia and was flagged by Binance for withdrawal attempts related to scams (Fig. 12).

2026-01-23 17:16:48	CAPITAL_WITHDRAW	CAPITAL	null	201.00000000
2026-03-04 14:29:10	CAPITAL_WITHDRAW	CAPITAL	null	501.00000000
2025-12-18 10:31:37	CAPITAL_WITHDRAW	CAPITAL	null	20.00000000
2025-12-18 10:48:42	CAPITAL_WITHDRAW	CAPITAL	ANTI_SCAM_CD_ACCOUNT_GENERIC_1H	100.00000000
2025-12-19 09:46:01	CAPITAL_WITHDRAW	CAPITAL	null	200.00000000
2025-12-19 09:15:29	CAPITAL_WITHDRAW	CAPITAL	null	300.00000000
2026-01-29 02:41:25	CAPITAL_WITHDRAW	CAPITAL	null	1,001.00000000
2026-01-29 02:48:47	CAPITAL_WITHDRAW	CAPITAL	null	951.00000000

Figure 12 - Binance Record Flagging #1195669929 Withdrawal Attempts

61. In conclusion, as shown above, **TARGET PROPERTY** was a Telegram channel used by scammers to entice workers to travel to Cambodia, after which they were held against their will and forced to scam U.S. victims through the use of U.S. wires, and further convince them to wire money from their financial institutions and transfer money through cryptocurrency wallets, which was then laundered. As such, the **TARGET PROPERTY** is a key node in soliciting actors to commit wire fraud against U.S. persons, through the use of U.S. wires (i.e., WhatsApp, Microsoft Teams, and multiple U.S. financial institutions). The **TARGET PROPERTY** is further property involved in a money laundering conspiracy, in which the funds that are procured through the wire fraud enabled by the **TARGET PROPERTY** are thereafter laundered through multiple cryptocurrency wallets, as stated. In other words, the **TARGET PROPERTY** was involved in and facilitated the transfer of funds from a place in the United States to a place outside the United States with the intent to promote a specified unlawful activity of wire fraud.

SEIZURE PROCEDURE

62. The top-level domain for **TARGET PROPERTY** is hosted by Telegram Messenger Inc. (“Telegram”), a company registered in the BVI with a legal address for correspondence usually listed as Conyers Trust Company (BVI) Limited, Commerce House, Wickhams Cay 1, P.O. Box 3140, Road Town, Tortola, VG1110, BVI.

63. Upon execution of the seizure warrant, the United States shall seek to directly serve Telegram with the warrant and seek enforcement of the seizure warrant as detailed in Attachment

A-1. Telegram would restrain and lock the **TARGET PROPERTY** pending transfer of all rights, title, and interest in the **TARGET PROPERTY** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET PROPERTY** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the Department of Justice.

64. In addition, upon seizure of **TARGET PROPERTY** by the FBI, Telegram will be directed to associate **TARGET PROPERTY** to a new authoritative name server(s) to be designated by a law enforcement agent. The government will display a notice on the website to which **TARGET PROPERTY** will resolve indicating that the site has been seized pursuant to a warrant issued by this Court.

**REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE
ELECTRONIC MEANS**

65. 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 Application for a Seizure Warrant. I submit that Assistant U.S. Attorney Karen Seifert, an attorney for the United States, can identify my voice and telephone number for the Court.

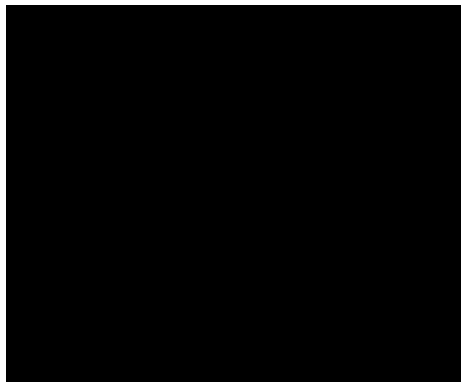
CONCLUSION

66. The **TARGET PROPERTY** was used to recruit trafficked workers, located outside the United States, to a compound facility in Cambodia, wherein the trafficked workers participated in a wire fraud conspiracy in which U.S. victims were instructed to send their U.S.-based funds to actors outside the United States, via the use of U.S. wire facilities, in violation of 18 U.S.C. §§ 1343, 1349. The **TARGET PROPERTY** was involved in a conspiracy to commit international promotional money laundering, 18 U.S.C. § 1956(a)(1)(B)(i), (h) specifically the

laundering of cryptocurrency funds, and can be seized and forfeited pursuant to 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1).

67. Based on the foregoing, I submit that the **TARGET PROPERTY** is subject to seizure and forfeiture, pursuant to the above referenced statutes, and I request that the Court issue the proposed seizure warrant.

68. Because the warrant will be served on the company that controls the **TARGET PROPERTY**, and the company at a time convenient to them will transfer control of the **TARGET PROPERTY** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time of day or night.



Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on April 22, 2026.

HONORABLE MATTHEW J. SHARBAUGH
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF COLUMBIA