

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff

-v-

26-CV-164

FOUR CASHIERS CHECKS SEIZED BY THE
DEPARTMENT OF HOMELAND
SECURITY TOTALING \$339,319.80 FROM
THE FOLLOWING ACCOUNTS:

ALL FUNDS ON DEPOSIT OR
TRANSFERRED
TO OR THROUGH CATHAY BANK
ACCOUNT NO. 88080145, HELD IN THE
NAME OF FAST YZ WHOLESALE, INC.,
AND ALL PROCEEDS TRACEABLE
THERETO;

ALL FUNDS ON DEPOSIT OR
TRANSFERRED TO OR THROUGH J.P.
MORGAN CHASE BANK
ACCOUNT NO. 686125298, HELD IN THE
NAME OF JSH WHOLESALE, INC., AND
ALL PROCEEDS TRACEABLE THERETO;

ALL FUNDS ON DEPOSIT OR
TRANSFERRED TO OR THROUGH PNC
BANK ACCOUNT NO. 8141732041, HELD IN
THE NAME OF WXIN WONDERFUL
TRADE, INC., AND
ALL PROCEEDS TRACEABLE THERETO; and

ALL FUNDS ON DEPOSIT OR
TRANSFERRED TO OR THROUGH
CITIBANK ACCOUNT NO.
6882396680, HELD IN THE NAME OF S2
EXPRESS, INC., AND ALL PROCEEDS
TRACEABLE THERETO.

Defendants *in Rem*.

VERIFIED COMPLAINT FOR FORFEITURE

The United States of America, by its attorneys, Michael DiGiacomo, United States Attorney for the Western District of New York, and Melanie J. Bailey, Assistant United States Attorney, of counsel, for its verified complaint herein alleges as follows:

1. This is an action *in rem* for the forfeiture of: forfeiture of Four Cashiers Checks (collectively hereafter “DEFENDANT PROPERTIES”) derived from the following four financial accounts (collectively hereafter, “Subject Accounts”):

- a. all funds on deposit or transferred to or through Cathay Bank Account No. 88080145, held in the name of Fast YZ Wholesale, Inc., and all proceeds traceable thereto (hereinafter, “SUBJECT ACCOUNT-1”), Cashier’s Check in the amount of \$98,227.29;
- b. all funds on deposit or transferred to or through J.P. Morgan Chase Bank Account No. 686125298, held in the name of JSH Wholesale, Inc., and all proceeds traceable thereto (hereinafter, “SUBJECT ACCOUNT-2”), Cashier’s Check in the amount of \$126,065.00;
- c. all funds on deposit or transferred to or through PNC Bank Account No. 8141732041, held in the name of WXIN Wonderful Trade, Inc., and all proceeds traceable thereto (hereinafter, “SUBJECT ACCOUNT-3”), Cashier’s Check in the amount of \$39,284.48; and
- d. all funds on deposit or transferred to or through Citibank Account No. 6882396680, held in the name of S2 Express Inc., and all proceeds traceable thereto (hereinafter, “SUBJECT ACCOUNT-4”), Cashier’s Check in the amount of \$75,743.03.

2. The DEFENDANT PROPERTIES are subject to forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and (C) as any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting “specified unlawful activity” (as defined in Section 1956(c)(7) of this title and hereinafter referred to as “SUA”), to include violations of Title 18, United States Code, Section 1343 (wire fraud) and

any property involved in a money laundering offense under Title 18, United States Code, Section 1957.

3. The jurisdiction of this Court is invoked pursuant to Title 28, United States Code, Sections 1345, 1355, and 1395. Venue is properly premised in the Western District of New York pursuant to Title 28, United States Code, Section 1395.

FACTS

Pig Butchering Investment Schemes

4. “Pig Butchering” is a term for an investment scam where fraudsters contact people, called “pigs”, on social media and build trust by engaging in long-term communication, establishing the idea of a fabricated friendship or romantic partnership. At some point, the fraudsters propose that the victim invest in cryptocurrency, stock, or precious metals on a fake investment platform the fraudsters control and operate.

5. In many cases, the fraudsters encourage the victims to invest increasing amount of money by sending their funds via wire transfer to financial accounts controlled by the fraudsters. Once the victims have sent the fraudsters a significant sum of money, the fraudsters disappear with the funds they stole from their victims which is, the “butchering” phase of the scheme.

6. The victims eventually attempt to withdraw their investments but are prevented from doing so. The victims are typically told that they first need to pay income taxes, additional processing fees, international transaction costs, or other miscellaneous fees before they can withdraw from their account. The scheme comes to an end when the fraudster stops communications and shuts down the fake cryptocurrency exchange or the victims give up

after realizing they have been scammed. This can be months into the scam where the victims have already given large sums of money to the fraudsters ranging from thousands to millions of dollars.

THE INVESTIGATION

7. Since 2021, HSI, along with other federal agencies, have been investigating a “Pig Butchering” scheme involving victims, who reside in the Western District of New York and elsewhere in the United States. Some of these victims are senior citizens who have been scammed of thousands of dollars by fraudsters utilizing overseas call centers, including some of the victims in this case.

8. During this investigation, evidence revealed a bank account primarily used in the Pig Butchering scheme. The account was opened at TD Bank in November 2024, in the name of Fast YZ Wholesale, Inc. Fast YZ Wholesale, Inc. was registered as a business in New Jersey less than a month before the TD Bank Account was opened. While the TD Bank Account was opened in New Jersey, the account was opened using both a New Jersey address and a Queens, New York address. (hereafter, the “Fraudulent Account”). Yuzhen Hu was the sole signatory listed on that account.

9. A review of bank records by law enforcement determined that during the period between November 21, 2024 and December 5, 2024, the Fraudulent Account received over seventeen wire transfers from at least sixteen individuals throughout the United States. During this two-week period, the wires collectively totaled approximately \$827,000. Moreover, the whole-dollar wires received into this account were made by various individuals across the country in large rapid transactions, which are common factors found in Pig Butchering fraud schemes.

10. On or about January 15, 2025, less than three months after the account was opened, The Fraudulent Account at TD Bank was closed. At the time the account was closed, TD Bank issued a bank check for the balance in the account in the amount of \$659,116, that was subsequently deposited into SUBJECT ACCOUNT-1. As set forth in further detail below, SUBJECT ACCOUNT-1 is held in the name of the same entity as the now closed Fraudulent Account, Fast YZ Wholesale, Inc., with the same signatory as the Fraudulent Account.

11. DHS has learned that the signatory of the account, Yuzhen Hu, is a female born in 1958, first entered the United States in 2014, sought asylum which was denied, and has since left the United States.

Victim-1 (H.F.)

12. In February 2025, law enforcement agents contacted an individual, who at that time was residing in Brooklyn, New York and who now resides in the Western District of New York. This individual was identified as a victim of this scheme. During the interview, Victim-1, a thirty-three-year-old male, stated to law enforcement that he was originally contacted through Facebook by someone he believed to be “Megumi”, a Japanese female who eventually befriended him. She introduced him to internet applications such as “Remitly” and “XmShoken” to use for what he believed was making investments in gold.

13. Victim-1 indicated he made two wire transfers totaling approximately \$66,000 to this gold investment platform, including sending a \$20,000 wire to the now closed Fraudulent Account on November 26, 2024.

14. Victim-1 further indicated that “Megumi” provided him with timing signals on when he should buy and sell gold on the platform. Victim-1 indicated that he eventually

tried to withdraw some of his funds, but received a message from the platform indicating that he needed to pay taxes in the amount of \$28,000 in order to access the balance of his account. Victim-1 indicated that he was no longer able to log into “Remitly” or “XmShoken.” Victim-1 further indicated that he lost all ability to communicate or contact “Megumi”.

Victim-2 (R.P.)

15. Victim-2 is an elderly male resident of Oro Valley, Arizona. Victim-2 was interviewed by law enforcement regarding a wire transfer he made to the now closed Fraudulent Account. Victim-2 indicated that he was originally sent a text message by someone claiming that she had erroneously sent a text message to a wrong number. Victim-2 continued to have a friendly conversation over text messaging with a woman named “Evelyn” who indicated, among other things, that she was divorced with a child.

16. Within a week of chatting, “Evelyn” asked Victim-2 if he knew anything about cryptocurrency investing and asked him if he wanted to make some money. She claimed she had an uncle with an investment firm who could assist. During the interview with law enforcement, Victim-2 indicated that, on “Evelyn’s” recommendation, he initially deposited \$10,000 into a cryptocurrency trading platform called “Onchain.” Subsequently, on or about November 27, 2024, Victim-2 was encouraged to and did wire transfer approximately \$300,000 to the now closed Fraudulent Account. When “Evelyn” told Victim-2 that she would not be getting any more trading signals from her uncle, Victim-2 tried to withdraw his investment but was told that he needed to pay a withdrawal fee of almost \$400,000. Victim-2 refused to pay this fee and was unable to receive any of the money he had deposited. Victim-2 also was unable to log into his “Onchain” account and was unable to communicate with “Evelyn”. At this point, Victim-2 realized he had been a victim of

financial fraud.

Victim-3 (G.P.)

17. Victim-3 is an elderly male resident of Lakewood, Colorado. Victim-3 was interviewed by law enforcement regarding a wire transfer he made to the now closed Fraudulent Account. Victim-3 indicated that in September 2024 he was contacted by a person via WhatsApp who chatted with him about investing in a cryptocurrency investment platform called "TDAA" for which Victim-3 had seen an internet advertisement.

18. Based on his communications with this person, Victim-3 subsequently wire transferred \$260,000 to this trading platform which he believed was being deposited into an account with this trading platform. At least one of these wire transfers was made on November 21, 2024, in the amount of \$99,951 to the now closed Fraudulent Account. When Victim-3 attempted to withdraw funds from his cryptocurrency account, he was messaged that he needed to pay a commission fee of hundreds of thousands of dollars before any funds would be transferred. Victim-3 advised that this trading platform website soon disappeared at which point he no longer was able to interact with his account. Victim-3 realized that he had been a victim of financial fraud.

Victim-4 (J.S.)

19. Victim-4 is an elderly male resident of Cape Coral, Florida. Victim-4 was interviewed by law enforcement regarding a wire transfer he made to the now closed Fraudulent Account. Victim-4 indicated that in July 2024 he was contacted by someone on WhatsApp who advised they could help him invest in stocks and cryptocurrency using software powered by artificial intelligence. Victim-4 said the investment platform used by this person was operated by "Trade Station Security Inc."

20. Based on his communications with this person, Victim-4 subsequently wire-transferred approximately \$19,000 to this trading platform which he believed was being deposited into his Trade Station Security account. At least one of these wire transfers was made on November 25, 2024, in the amount of \$10,000 to the now closed Fraudulent Account. When Victim-4 attempted to withdraw funds from his cryptocurrency account, he was messaged that he needed to pay taxes on his earnings before any funds would be transferred to his bank account. Victim-4 said the trading platform website soon disappeared and he no longer had the ability to interact with his account. Victim-4 realized that he had been a victim of financial fraud.

Victim-5 (T.N.)

21. Victim-5 is an elderly male resident of Buchanan Dam, Texas. Victim-5 was interviewed by law enforcement regarding a wire transfer he made to the now closed Fraudulent Account. Victim-5 indicated that in August 2024 he befriended what he believed to be an Asian female through the Tik-Tok application. Victim-5 continued to communicate with this person via Telegram at which point she convinced him to begin investing in a cryptocurrency investment platform called "IBKR International Brokers."

22. Based on his communications with this person, Victim-5 subsequently wire-transferred approximately \$50,000 to this trading platform which he believed was being deposited into his IBKR account. At least one of these wire transfers was made on November 22, 2024, in the amount of \$20,325 to the now closed Fraudulent Account. When Victim-5 attempted to withdraw funds from his cryptocurrency account, he received a message advising that he needed to pay additional fees on his account before he could receive his money. Victim-5 said this cryptocurrency investment trading platform soon disappeared and

he was no longer able to interact with his account. Victim-5 realized that he had been a victim of financial fraud.

Victim-6 (S.P.)

23. Victim-6 is a female resident of Fairview, Texas. Victim-6 was interviewed by law enforcement regarding a wire transfer she made to the now closed Fraudulent Account. Victim-6 indicated that in August 2024 she befriended an individual she met on the internet dating platform "Bumble." Victim-6 continued to communicate with this person at which point this individual convinced her to begin investing in a cryptocurrency investment platform called "BITONFIN."

24. Based on her communications with this person, Victim-6 subsequently wire-transferred approximately \$56,000 to this trading platform which she believed was being deposited into her BITONFIN account. At least one of these wire transfers was made on November 25, 2024, in the amount of \$20,000 to the now closed Fraudulent Account. Victim-6 said this cryptocurrency investment trading platform soon disappeared and she was no longer able to interact with her account. Victim-6 realized she had been a victim of financial fraud.

Victim-7 (M.G.)

25. Victim-7 is a male resident of Independence, Missouri. Victim-7 was interviewed by law enforcement regarding a wire transfer he made to the now closed Fraudulent Account. Victim-7 indicated that in Fall of 2024 he befriended an Asian female he met on the internet who convinced him to begin investing in a cryptocurrency investment platform. Victim-7 said he no longer recalls the name of this bogus platform.

26. Based on his communications with this person, Victim-7 subsequently wire-

transferred approximately \$20,000 to this trading platform which he believed was being deposited into his cryptocurrency investment account. At least one of these wire transfers was made on November 27, 2024, in the amount of \$18,000 to the now closed Fraudulent Account. Victim-7 said the operators of this cryptocurrency investment platform demanded he pay taxes to them when he wanted to withdraw some of the money from his account to repair his townhouse. Victim-7 said he became suspicious at this point and that the cryptocurrency investment trading platform soon disappeared. Victim-7 said he was no longer able to interact with his account and that he realized he had been a victim of financial fraud.

Victim-8 (R.E.)

27. Victim-8 is an elderly male resident of Bradenton, Florida. Victim-8 was interviewed by law enforcement regarding a wire transfer he made to the now closed Fraudulent Account. Victim-8 indicated that in September 2024 he found an advertisement on the internet involving cryptocurrency investment. Victim-8 advised he interacted with the advertisement and was subsequently contacted by someone on WhatsApp to discuss the investment opportunity further. Victim-8 said he eventually started sending money to a company called Investco and that he acquired access to the internet platform.

28. Based on his communications with this person, Victim-8 subsequently wire-transferred approximately \$210,000 to this trading platform which he believed was being deposited into his Investco account. At least one of these wire transfers was made on November 22, 2024, in the amount of \$40,000 to the now closed Fraudulent Account. Victim-8 said this cryptocurrency investment trading platform soon disappeared and he was no longer able to interact with his account. Victim-8 realized he had been a victim of financial fraud.

THE SUBJECT ACCOUNTS

Subject Account 1

29. SUBJECT ACCOUNT-1 consists of all funds on deposit at Cathay Bank account number 88080145, held in the name of Fast YZ Wholesale, Inc. Cathay Bank maintains branches in the Eastern District of New York and elsewhere in the United States.

30. Similar to the now closed Fraudulent Account, SUBJECT ACCOUNT-1 was opened on or about November 8, 2024. While SUBJECT ACCOUNT-1 was opened in New Jersey, in the name of a New Jersey entity, both a New Jersey and a Queens, New York address were provided to Cathay Bank when the SUBJECT ACCOUNT-1 was opened. Yuzhen Hu was the sold signatory for SUBJECT ACCOUNT-1.

31. The holder and signatory of SUBJECT ACCOUNT-1 is identical to the holder and signatory on the now closed Fraudulent Account at TD Bank.

Subject Account 2

32. SUBJECT ACCOUNT-2 consists of all funds on deposit at JP Morgan Chase Bank account number 686125298, held in the name of JSH Wholesale, Inc. JP Morgan Chase maintains branches in the Western District of New York and throughout the United States.

33. SUBJECT ACCOUNT-2 was opened in December 2024 at a Queens, New York branch of JP Morgan Chase, in the name of a New Jersey entity. The sole signatory on SUBJECT ACCOUNT-2 is Shushua Jiang.

Subject Account 3

34. SUBJECT ACCOUNT-3 consists of all funds on deposit at PNC Bank account number 8141732041, held in the name of Wxin Wonderful Trade, Inc. PNC Bank maintains branches in the Eastern District of New York and throughout the United States.

35. SUBJECT ACCOUNT-3 was opened at or around the same time as the now closed Fraudulent Account, and SUBJECT ACCOUNT-2 in the name of a New Jersey entity. The sole signatory on SUBJECT ACCOUNT-3 is Xin Weng.

Subject Account 4

36. SUBJECT ACCOUNT-4 consists of all funds on deposit at Citibank, NA bank account number 6882396680, held in the name of S2 Express Inc. Citibank maintains branches in the Western District of New York and elsewhere throughout the United States.

37. SUBJECT ACCOUNT-4 was opened in October 2024 at a Queens, New York branch of Citibank, NA. The sole signatory on SUBJECT ACCOUNT-4 is HaoWu using a Queens, New York address.

TRACING OF VICTIM FUNDS TO THE SUBJECT ACCOUNTS

38. On or about January 15, 2025, over \$659,116 in fraud proceeds originally from U.S. fraud victims, including but not limited to Victims-1, 2, and 3, were transferred from the now closed Fraudulent Account to SUBJECT ACCOUNT-1.

39. On or about January 27, 2025, approximately \$150,000 was wire transferred or caused to be wire transferred from SUBJECT ACCOUNT-1 to SUBJECT ACCOUNT-2, and this constitutes a violation of Title 18, United States Code, Section 1957.

40. On or about January 27, 2025, an additional approximate \$148,000 was wire transferred or caused to be wire transferred from SUBJECT ACCOUNT-1 to SUBJECT ACCOUNT-3, and this constitutes a violation of Title 18, United States Code, Section 1957.

41. On or about February 10, 2025, approximately \$100,000 was wire transferred or caused to be wire transferred from SUBJECT ACCOUNT-1 to SUBJECT ACCOUNT-4, and this constitutes a violation of Title 18, United States Code, Section 1957.

42. HSI has been notified by the respective financial institutions that each of the SUBJECT ACCOUNTS contains less than the funds originally transferred from the now closed Fraudulent Account and, in turn, from SUBJECT ACCOUNT-1.

SEIZURE OF THE SUBJECT ACCOUNTS

43. On June 6, 2025, seizure warrants for the SUBJECT ACCOUNTS were issued by the Honorable James R. Cho, United States Magistrate Judge in the Eastern District of New York.

44. Upon service of the seizure warrants on the respective financial institutions, all funds in each account were converted to a cashiers check and sent to the Department of Homeland Security to initiate administrative forfeiture proceedings against the DEFENDANT PROPERTIES.

CONCLUSION AND REQUESTS FOR RELIEF

45. The government submits that the DEFENDANT PROPERTIES are subject to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(C) In addition, the DEFENDANT PROPERTIES constitute proceeds or were derived from proceeds traceable to SUA, namely wire fraud in violation of Title 18, United States Code, Section 1343 (wire fraud) and Title 18, United States Code, Section 1957 (money laundering). The DEFENDANT PROPERTIES derived from the SUBJECT ACCOUNTS are therefore subject to forfeiture to the United States pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 981(a)(1)(C).

WHEREFORE, the United States of America respectfully requests that:

- (1) A Notice of Complaint for Forfeiture against the DEFENDANT PROPERTIES be issued;
- (2) Notice of this action be given to all persons known or thought to have an interest in or right against the DEFENDANT PROPERTIES;
- (3) A judgment be entered declaring the DEFENDANT PROPERTIES condemned and forfeited to the United States of America for disposition in accordance with the law;
- (4) The costs of this suit be paid to and recovered by the United States of America; and
- (5) The Court grant such other and further relief as deemed just and proper.

DATED: January 28, 2026 at Buffalo, New York

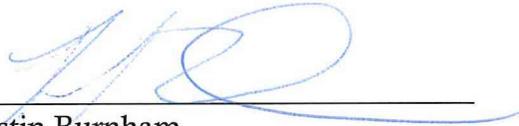
MICHAEL DIGIACOMO
United States Attorney
Western District of New York


By: _____
MELANIE J. BAILEY
Assistant U.S. Attorney
United States Attorney's Office
Western District of New York
138 Delaware Avenue
Buffalo, New York 14201
(716) 843-5863
melanie.bailey@usdoj.gov

STATE OF NEW YORK)
COUNTY OF ERIE) ss.:
CITY OF BUFFALO)

Justin Burnham, being duly sworn, deposes and says:

I am a Special Agent of Homeland Security Investigations, Department of Homeland Security, in the Western District of New York. I am also assigned to the Department of Homeland Security's files on the investigation of the DEFENDANT PROPERTIES referenced in the above complaint. The matters alleged in the Verified Complaint for Forfeiture and the attached Exhibit are true to the best of my knowledge and belief, and were obtained during the course of the investigation of the DEFENDANT PROPERTIES from the official files of the Department of Homeland Security, Homeland Security Investigations, and provided to the officials of the United States Department of Justice, United States Attorney's Office.



Justin Burnham
Special Agent
Homeland Security Investigations

Sworn to before me this 28th day of
January, 2026.



Notary Public
GABRIELA KICK
Notary Public, State of New York
Qualified in Niagara County
My Commission Expires: 09/04/2026