

MELISSA HOLYOAK, United States Attorney (#9832)
CARL D. LESUEUR, Assistant United States Attorney (#16087)
BRENT L. ANDRUS, Assistant United States Attorney (NY #5143474)
Attorneys for the United States of America
Office of the United States Attorney
111 South Main Street, Suite 1800
Salt Lake City, Utah 84111-2176
Telephone: (801) 524-5682
Email: brent.andrus@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

UNITED STATES OF AMERICA,

Plaintiff,

vs.

SHIKUN TAN,

Defendant.

FELONY CRIMINAL COMPLAINT

Case No. 2:26mj11-DAO

Judge Daphne A. Oberg

Before the Honorable Dustin B. Pead, United States Magistrate Judge for the District of Utah, appeared the undersigned, who on oath deposes and says:

COUNT I
18 U.S.C. § 1349
(Conspiracy to Commit Wire Fraud)

1. From at least February 2025 to the present, defendant, SHIKUN TAN, and others knowingly and willfully conspired and agreed with each other to commit wire fraud in violation of 18 U.S.C. § 1343, all in violation of 18 U.S.C. § 1349. TAN and his co-conspirators created and coordinated the use of fake online personas, used those

fake online personas to engage in online communication with unwitting victims, lured the victims to fraudulent investment websites, all in order to trick the victims into believing the fraudsters offered lucrative investment opportunities. After gaining the victims' trust, the fraudsters then directed the victims to send their own personal funds to bank accounts controlled by TAN and his co-conspirators.

2. TAN is a Chinese national living in the United States with no legal status. The undersigned believes he is an active threat to flee the country.

This complaint is made on the basis of an investigation consisting of, in part, the following:

Bank of America account 6567: destination for victim funds

3. Bank of America account 5010-3162-6567 (**BoA 6567**) is a business account under the name Horizon Builders LLC. SHIKUN TAN the only known signer on the account. The account was opened on November 20, 2025. Since opening, there have been twenty-nine (29) wire transfers into the account totaling approximately \$1,600,000. These incoming wires include funds from seven (7) different online fraud victims:

Date	From	Address	From	Wire Transfer Amount to xx6567
12/23/2025	Carl Belnap	American Fork, UT	Victim #1	\$25,000
12/23/2025	Michael Herrick	Waterville, NY	Victim #4	\$25,000
12/23/2025	Kevin T. Koltvedt	Albany, OR	Victim #7	\$20,000
12/30/2025	Robert Balliger	Cortez CO	Victim #2	\$129,771
12/31/2025	Vijay Shah	Paramus NJ	Victim #6	\$150,000
12/31/2025	Mark S Lair	Clinton IA	Victim #5	\$33,000

1/2/2026	Earl C Dean	South Park PA	Victim #3	\$16,000
Total				\$398,771

4. The account was frozen after the above wire for \$20,000 was sent to BoA 6567 on December 23, 2025 from Victim #7's Red Canoe Credit Union (RCCU). RCCU notified Bank of America that the wire transfer was sent in furtherance of suspected fraud and asked for a recall. Bank of America was unable to return the funds to Victim #7 because TAN would not authorize it.

FBI Undercover Call with SHIKUN TAN

5. On January 7, 2026, an FBI Undercover Employee (UCE) called the signer for BoA 6567, SHIKUN TAN, at phone number (303) 847-5803. TAN told the UCE he could not speak English and requested a Mandarin translator. After finding a translator, the UCE called (303) 847-5803 but no one answered. The UCE then called (725) 285-9890 and TAN answered. TAN confirmed he was the owner of BoA 6567. He said Horizon Builders LLC was a construction company that provided lumber and construction products, as well as labor, for construction projects in the Las Vegas, Nevada area.

6. The UCE asked TAN specifically about the \$129,770.96 Victim #2 wired to BoA 6567 on December 30, 2025. TAN said the money was used for a construction project in the Las Vegas, Nevada area.

7. The UCE asked TAN specifically about the \$16,000 Victim #3 wired to BoA 6567 on January 2, 2026. TAN said the money was used for a construction project in the Las Vegas, Nevada area.

8. The UCE asked TAN specifically about the \$25,000 Victim #1 wired to BoA 6567 on December 30, 2025. TAN said the money was used for a construction project in the Las Vegas, Nevada area.

9. TAN told the UCE he was willing to meet the UCE at a Bank of America branch in the Las Vegas, Nevada area in order to recover funds from BoA 6567.

Fraud Victims

Victim #1

10. Victim #1 resides in American Fork, Utah and fell victim to an investment scam. In February or March of 2025, Victim #1 found a company online called Horizon. Horizon held itself out as an online crypto investment company. Victim #1 communicated with individuals purporting to be Horizon customer service representatives online and they helped him download an investment application for Horizon to his phone.

11. Horizon customer service personnel told Victim #1 if he wanted to invest in Horizon, they would provide him with bank account to wire money to. Victim #1 started small by investing about \$5,000. Horizon customer service personnel provided bank accounts for Victim #1 to wire money to. They provided different accounts each time

they asked Victim #1 to send money. When Victim #1 sent wire transfers to different accounts, his Horizon online app would show the money was deposited and that it generated large profits.

12. Victim #1 estimates that between February and December 2025, he wired a total of around \$400,000 to different bank account when directed by Horizon customer service personnel. Victim #1's Horizon account showed he had a balance of \$2,900,000.

13. Victim #1 provided bank receipts showing he sent the following wire transfers in support of the fraud:

Date	Amount	To	Address	Bank	Account
7/3/2025	\$5,000	My Toys LLC	Santa Clara, CA	Bank of America	**6510
7/15/2025	\$40,000	BMO Trade	Denver, CO	Choice Financial Group	**9483
7/25/2025	\$6,000	WHDC Supply Inc.	Little Neck, NY	Bank of America	**4439
8/12/2025	\$25,000	Starlight Vogue Inc.	Aurora, CO	Wells Fargo	**4637
8/20/2025	\$24,000	Mengqi Farms Intl Inc.	Rowland Heights, CA	Citi Bank	**0765
10/10/2025	\$32,350	Stormtime Investment Limited	Lusaka, Zambia	First National Bank Zambia LTD	**7442
11/5/2025	\$50,000	Goroda hardware LTD	Nairobi, Kenya	Equity Bank	**4195

11/19/2025	\$50,000	Wrenchworks Build LLC	Baltimore, MD	Truist Bank	**0883
11/25/2025	\$90,000	Fordstamp Inc.	Hicksville, NY	Bank of America	**9593
12/11/2025	\$117,000	Skylines Decorate Inc.	El Monte, CA	Bank of America	**7931
12/23/2025	\$25,000	Horizon Builders LLC	Las Vegas, NV	Bank of America	**6567
TOTAL	\$464,350				

14. Victim #1 tried to withdrawal money from his Horizon account, but Horizon customer service personnel told him he had to pay \$117,000 in taxes and fees before he could withdrawal any money.

15. Victim #1 said the \$25,000 he wired **BoA 6567** on December 23, 2025, was supposed to be used to pay taxes and fees so he could withdrawal money from the Horizon account.

16. Horizon customer service personnel told Victim #1 if anyone asked why he was wiring money to **BoA 6567** he should tell them it was for a construction project.

17. Victim #1 lost approximately \$464,350 to the scam.

Victim #2

18. Victim #2, age 60 resides in Cortez, Colorado and fell victim to an investment scam. In June 2025, a person claiming to be Emily Lee called Victim #2 and said she accidentally called a wrong number. Victim #2 and Lee started talking and developed an online relationship. Lee told Victim #2 she had an Aunt who could help

him invest in online gold trading. Lee helped Victim #2 download an application to his phone to do online gold trading.

19. On June 15, 2025, Lee helped Victim #2 create a Crypto.com account. She directed Victim #2 to purchase \$100,000 worth of cryptocurrency using his Crypto.com account and then transfer the money to another account. Victim #2's online gold trading platform purported to show the money was deposited to his gold trading account. Lee's aunt told Victim #2 when to trade money for gold using the online platform and the platform showed Victim #2 was making large profits every time he traded.

20. In July 2025, Lee directed Victim #2 to wire another \$400,000 to another account. After sending the \$400,000 to the account, Victim #2's online trading account showed the money was deposited. To determine if the online trading account was legitimate, Victim #2 asked to withdrawal \$35,000. The \$35,000 was transferred to Victim #2's Zions Bank account. Feeling confident it was not fraud, Victim #2 continued to send money wherever Lee told him to.

21. On December 20, 2025, Victim #2 wired \$129,770.96 to **BoA 6567** at Lee's direction. Lee told Victim #2 that Horizon Builders LLC was a conduit used by his online trading platform to collect money to trade in gold. Victim #2's online account showed the deposit and as of January 6, 2029 a balance of \$1,379,065.

22. Victim #2 lost approximately \$600,000 to the scam

Victim #3

23. Victim #3 resides in South Park, Pennsylvania and fell victim to an investment scam. In November 2025, Victim #3 met a person calling herself Nora Mueller on Facebook. Mueller told Victim #3 she had a friend named Adam Jenkins who could help him invest in cryptocurrency. At Jenkins' direction, Victim #3 downloaded an online application called EQUATORVIT-MAX.com.

24. During the week of December 21, 2025, Victim #3 wired \$25,000 from his BNC Bank account to Coinbase at Cross River Bank. Jenkins and Mueller told Victim #3 that the \$25,000 was converted to Ether (ETH, a digital currency of the Ethereum blockchain) and the ETH was deposited to Victim #3's EQUATORVIT-MAX.com account. Victim #3 looked online at his EQUATORVIT-MAX.com account and it appeared to show that the \$25,000 was deposited. Jenkins and Mueller told Victim #3 when to make trades using his EQUATORVIT-MAX.com account and the platform showed large profits.

25. On January 2, 2026, Jenkins directed Victim #3 to wire \$16,000 to **BoA 6567**, an account titled Horizon Builders LLC. After Victim #3 wired the money to **BoA 6567** his EQUATORVIT-MAX.com showed the money was deposited. On January 6, 2026, Victim #3's EQUATORVIT-MAX.com account showed a balance of \$99,601.82.

26. In fact, the \$16,000 Victim #3 wired to **BoA 6567** was never deposited to the EQUATORVIT-MAX.com account. Bank of America froze **BoA 6567** with Victim

#6's funds still in the account after Bank of America received a complaint from another victim about fraud involving the account.

27. Victim #3 lost approximately \$42,000 to the scam.

Victim #4

28. Victim #4 age 70, resides in Waterville, New York and fell victim to an investment scam. In September 2025, Victim #4 met a person calling herself Salina Yilmaz on an online dating site. Victim #4 and Yilmaz started an online romance. Yilmaz told Victim #4 her aunt was an investment expert who could help him invest in cryptocurrency and gold. Yilmaz helped Victim #4 set up an account on a trading platform called TRUST WALLET. Yilmaz helped Victim #4 communicate with TRUST WALLET customer service personnel, and they told Victim #4 where to send money.

29. On October 14, 2025, Victim #4 wired \$1,010 from his Key Bank account to Coinbase at Cross River Bank account **9723. Victim #4's TRUST WALLET account showed the deposit and then Yilmaz told Victim #4 when to trade the money for gold using the TRUST WALLET application. The TRUST Wallet application showed large profits from the gold trades. Victim #4 asked to withdraw \$500 to prove the TRUST WALLET application was legitimate, and \$500 was wired to Victim #4's account.

30. Yilmaz and TRUST WALLET customer service personnel asked Victim #4 to wire payments to bank accounts in Vietnam, but Key Bank refused and notified Victim #4 it was fraud. After failing to send money to foreign accounts, Yilmaz and TRUST

WALLET personnel directed Victim #4 to send future payments to bank accounts in the United States.

31. On October 11, 2025, Victim #4 wired \$4,210 to the same Cross River Bank account at Yilmaz and TRUST WALLET's direction. Victim #4's TRUST WALLET account showed the deposit.

32. On December 23, 2025, Victim #4 wired \$70,000 to the **BoA 6567** at Yilmaz and TRUST WALLET's direction.

33. Victim #4 lost \$155,420 to the scam.

Victim #5

34. Victim #5 resides in Clinton, Iowa and fell victim to an investment fraud. Victim #5 was approached via WhatsApp by unknown individuals who convinced him to invest in cryptocurrency.

35. The scammers directed Victim #5 to wire \$33,000 to **BoA 6567** on December 31, 2025 in furtherance of the scam. Victim #5 was told he had to send \$33,000 to Horizon Builders LLC in order to pay taxes necessary to recover money he previously invested in the cryptocurrency scam.

Victim #6

36. Victim #6 resides in Paramus, New Jersey and fell victim to an investment fraud. Victim #6 was introduced to an online investment company called exameleonfinance.com (EXAM). Victim #6 communicated via text with customer service personnel who claimed to work for EXAM. These personnel told Victim #6 they

were building a new cryptocurrency that would be going public soon. They told Victim #6 that if he invested \$2,000,000 in EXAM he would make \$20,000,000. The EXAM customer service personnel told Victim #6 where and when to send money.

37. On July 17, 2025, Victim #6 initiated a crypto wallet transfer withdrawal, totaling \$2,970.17, at the direction of EXAM personnel.

38. On September 18, 2025, Victim #6 opened an account at Capital One Bank. Between September 18, 2025 and December 1, 2025, Victim #6 moved \$3,055,500 from his JP Morgan Chase (JPMC) account to his Capital One Bank account. Victim #6 used the money to make \$2,761,461.55 worth of payments to the eight different accounts at six different financial institutions at the direction of EXAM personnel.

39. Victim #6 made all these payments at the direction of EXAM personnel in order to gain access to the promised \$20,000,000.

40. On December 31, 2025, Victim #6 wired \$150,000 to **BoA 6567** titled Horizon Builders, LLC because he was directed to by EXAM personnel. The EXAM personnel told Victim #6 this was the final payment he had to make before they would finally release the \$20,000,000.

41. Victim #6 estimated he lost approximately \$3,000,000 to the scam.

Victim #7

42. Victim #7 resides in Albany, Oregon and fell victim to an investment fraud. In October 2025, Victim #7 met a person calling herself Rachel Soto through

Facebook's dating site. Soto and Victim #7 communicated using WhatsApp. Soto and Victim #7 started an online romance.

43. Soto told Victim #7 she made money by investing in cryptocurrency. She invited Victim #7 to invest using an online platform at fidelityera@eras.com. At Soto's direction, Victim #7 created a username and password so he could invest using his account at fidelityera@eras.com.

44. In my training and experience it is common for scammers to create fraudulent trading platforms that resemble legitimate and well know trading platforms like Fidelity (<https://www.fidelity.com>).

45. In November 2025, Victim #7 was directed to wire \$1,000 to a bank account at Soto's direction. After he wired \$1,000, the balance on his fidelityera@eras.com account reflected the deposit.

46. In November 2025, Victim #7 was asked to purchase \$1,000 worth of cryptocurrency using a Coinbase account Soto helped him establish. After making the purchase Coinbase closed Victim #7's account for fraud.

47. On December 23, 2025, Soto directed Victim #7 to wire \$20,000 to **BoA 6567** (under Horizon Builders, LLC). When Victim #7 went to Red Canoe Credit Union (RCCU) to send the \$20,000 wire to **BoA 6567**, RCCU employees warned Victim #7 it was fraud. Victim #7 ignored their warnings and sent the wire. Victim #7 did not know that RCCU reported the fraud to Bank of America and asked for a wire recall.

48. On January 6, 2026, Victim #7's fidelityera@eras.com documented a balance of \$37,000 even though the \$20,000 was frozen in **BoA 6567**.

Misrepresentations by SHIKUN TAN in furtherance of the
wire fraud conspiracy

49. Each of the seven (7) victims who sent money to SHIKUN TAN's Bank of America account (**BoA 6567**) thought they were sending money to an online investment opportunity involving gold, cryptocurrency, or something similar. None believed they were investing in real estate or construction projects in the Las Vegas area. TAN told the FBI UCE that incoming wires into the BoA 6567 account, including specific victim wires described above, were payments for construction projects.

50. When speaking with the FBI UCE (posing as a representative of Bank of America), TAN claimed that he did not speak English. He claimed to have an English-speaking partner who supposedly talks to all clients. TAN claimed that the incoming wires from victims were from clients for construction projects. But none of the victims lived near Las Vegas or had construction projects there.

51. Two victims recounted that they were told by perpetrators of the scheme to tell the same fictitious story that TAN told regarding the purpose of the proceeds (for construction funds) to anyone asking questions about the purpose of the funds.

52. When asked if he had a warehouse in Nevada where he stored construction equipment and the supplies, TAN claimed that all his construction supplies were stored in Nevada. In reality, Horizon Builders LLC is not a licensed business in Nevada and the

address listed for Horizon Builders LLC is single family home located on a 8,276 square foot lot.

53. Victim #7's financial institution, Red Canoe Credit Union (RCCU), notified Bank of America that the wire transfer sent to TAN's 6567 account was in furtherance of suspected fraud. RCCU asked for a recall of the funds. TAN did not authorize the return. As a result, the funds were not returned. TAN's BoA 6567 account continued to receive additional victim funds after RCCU's fraud return request resulted in the freezing of TAN's account.

54. TAN's conversation with the FBI UCE wherein he claimed the victim funds were for construction projects also occurred after TAN's account was frozen following the fraud return request regarding Victim #7's wire.

Based on the foregoing information, your affiant respectfully requests that a warrant of arrest be issued for SHIKUN TAN for violations of 18 U.S.C. § 1349.

s/ Bret Curtis
Affiant,
Special Agent BRET CURTIS

SUBSCRIBED AND SWORN to before me this 9th day of January, 2026.

Daphne A. Oberg
Daphne A. Oberg
United States Magistrate Judge

APPROVED:

MELISSA HOLYOAK
United States Attorney

s/ Brent Andrus

BRENT L. ANDRUS
Assistant United States Attorney