2021R00234/JHS

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Edward S. Kiel
	:	
v.	:	Mag. No. 22-15279
	:	
KENNY OSAS OKUONGHAE	:	**CRIMINAL COMPLAINT**

I, Andrew Hodge, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Andrew Hodge 10/7/22

Andrew Hodge, Special Agent
Federal Bureau of Investigation

Special Agent Hodge attested to this Affidavit by telephone pursuant to F.R.C.P. 4.1(B)(2)(A) on this 7th day of October, 2022.

Edward S. Kiel (Signed) 10/7/22

Hon. Edward S. Kiel
United States Magistrate Judge

ATTACHMENT A
(Money Laundering Conspiracy)

From in or around 2019 through the present, in the District of New Jersey and elsewhere, the defendant

KENNY OSAS OKUONGHAE

did knowingly, combine, conspire, confederate, and agree with others to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved proceeds of specified unlawful activity, that is, wire fraud, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(l)(B)(i), all in violation of Title 18, United States Code, Section 1956(h).

ATTACHMENT B

I, Andrew Hodge, am a Special Agent of the Federal Bureau of Investigation. The information contained in the complaint is based upon my personal knowledge, as well as information obtained from other sources, including: (a) statements made or reported by various witnesses with knowledge of the relevant facts; (b) my review of publicly available information; and (c) my review of evidence, including complaints, business records, bank records, and other documents and records. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where the contents of documents and the actions and statements of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background:

1. During the time period relevant to this criminal complaint:
    a. Kenny Osas Okuonghae was a resident of New Jersey.
    b. Okuonghae maintained several different bank accounts in his own name and in the name of "Kenny Global Enterprises LLC" that he used to launder money obtained through various Internet-enabled fraud schemes.
    c. Law enforcement has identified at least 14 bank accounts at nine different banks that Okuonghae controlled, including accounts at Banks-1 through -7.
    d. A "romance scam," generally speaking, was a type of fraudulent scheme whereby perpetrators pretended to be individuals looking for a romantic partner on an online dating website. Commonly, these types of fraud schemes are perpetrated by individuals who actually reside overseas but who pretend to live in the United States. Once a victim expresses interest in the false persona who is purporting to be romantically interested in the victim, the perpetrator pretends to have a series of unfortunate events occur, usually while he or she is supposedly traveling outside the United States for work and asks the victim to send money on the purported romantic partner's behalf. The victim, believing that he or she is in a romantic relationship with the false persona, sends money for the benefit of whom they believe is the person they met on the online dating website, but who is actually one or more overseas perpetrators.
    e. "Pig Butchering" is a term derived from the Chinese word "Shāzhūpán," and referred to an Internet scheme that is believed

to have originated in China. The scheme involves a romance scam victim developing what the victim perceives to be a romantic relationship online with the perpetrator. The perpetrator emotionally "fattens" the victim up before enticing the victim to invest in a fake cryptocurrency scheme and then, metaphorically, "slaughters" the victim by taking the victim's real money that he or she placed in the fake cryptocurrency investment scheme.

f. Trade-based money laundering is a common form of money laundering whereby the perpetrators attempt to conceal the illegal nature of crime proceeds by using trade transactions to make the crime proceeds appear legitimate. The sale and shipment of used cars and car parts is a common form of trade-based money laundering.

Okuonghae's Money Laundering Scheme

2. As set forth below, there is probable cause to believe that Okuonghae is laundering the proceeds of Internet-enabled fraud, including pig butchering, rental scams, and romance scams, all through bank accounts he controls.

3. While the investigation remains ongoing, law enforcement estimates that Okuonghae has received at least approximately $2.5 million in fraudulent proceeds from approximately 2019 to the present.

Pig Butchering Scam: Alphacoin

Victim-1:

4. Victim-1, a resident of Ohio, was a victim of a pig butchering scam involving a purported cryptocurrency investment platform called "Alphacoin."

5. Victim-1 met someone purporting to be a woman named "Aggie Gonzales" on an online professional social media website. Through the course of their online relationship, "Aggie Gonzales" asked Victim-1 to help her purchase medical equipment, with the intention that "Aggie Gonzales" would repay Victim-1. Victim-1 sent money for the benefit and at the direction of "Aggie Gonzales." After Victim-1 sent money, "Aggie Gonzales" claimed that she was injured in Canada and needed Victim-1 to send her additional money to cover hospital bills.

6. In furtherance of the scheme, the perpetrators sent Victim-1 various financial documents to attempt to establish the legitimacy of the fraudulent narratives. The perpetrators also developed and relayed elaborate emotional stories designed to guilt Victim-1 into sending more money on "Aggie Gonzales'" behalf. Victim-1 also received communications from other purported individuals associated with "Aggie Gonzales." For example, an individual purporting to be "Dr. Ben Levy," a doctor in Brazil, sent Victim-1 a photograph of a woman in a hospital bed and stated the following:

> Aggie's situation is getting serious, I was informed by one of the nurses assigned to her that she noticed she was stooling blood, though she's been given medications to stop it, this is to say that her inner bleeding is getting worse and right now blood has flown down to her digestive organs and that is not a good sign at all. I plead with you on behalf of her to please save this woman's life. I understand that you may be doing the best you can but you need to know that time is not on her side.

7. "Aggie Gonzales" told Victim-1 that she would repay Victim-1 hundreds of thousands of dollars for the sale of medical equipment, but that Victim-1's bank would not accept the money. Instead, "Aggie Gonzales" told Victim-1 that she would repay Victim-1's money by placing money on Victim-1's behalf into cryptocurrency investments through a platform called "Alphacoin Lab." In or around September 2021, Victim-1 received a notification that an account had been set up on Victim-1's behalf with Alphacoin Lab.

8. Alphacoin Lab maintained several different websites purporting to reflect that Alphacoin was a legitimate cryptocurrency investment platform. One of the websites promised a "120% per annum (10% per month)" return on investments and stated further:

> We enable users to enter the crypto market with zero learning curve required, and we help construct diversified portfolios with the aim to maximize returns while maintaining your preferred risk profile. AlphaCoin offers state-of-the-art trading technology and online electronic brokerage services to active individual and co-operate traders worldwide. The company's innovative trading and analysis platform provides one-click access to all major exchanges and market centers, while its expansive product offering enables clients to design, test, optimize, monitor and automate their own custom equities, options and futures trading strategies. AlphaCoin's fully customizable market monitoring, charting and analysis tools help clients to identify and act instantly on trading opportunities.

9. Purported representatives of Alphacoin Lab contacted Victim-1 via email and WhatsApp. Victim-1 was told that Victim-1 would receive the money that was deposited into Victim-1's Alphacoin Lab account after Victim-1 paid taxes and fees on the funds. After communicating with several purported representatives of the company, a woman named "Olivia Silvester" began contacting Victim-1 via email to handle wire transfers that Victim-1 was told were required to be sent to pay taxes and fees on Victim-1's account.

10. As a part of the scheme, Victim-1 was told that Victim-1 would have to send wire transfers to cover various fees and taxes to a bank account in the name of Kenny Global Enterprise LLC, Okuonghae's entity. Victim-1 was told that Kenny Global Enterprise LLC was a subsidiary of Alphacoin Lab.

Victim-1 was also told further that Victim-1 could invest further funds in cryptocurrency by sending funds to Kenny Global Enterprises' bank account.

11. In or around November 2021, a representative from Alphacoin sent an email to Victim-1 containing bank account information for Victim-1 to deposit money into, purportedly to resolve an issue related to Victim-1 wanting to withdraw money from his account. The bank account listed was in the name of Kenny Global Enterprises LLC at Bank-1.

12. In or around April 2022, Victim-1 mailed a $29,000 certified check made payable to "Kenny Okuonghae" to an address in Edison, New Jersey.

13. As a part of the scheme, Victim-1 was also instructed to wire money to Okuonghae's Kenny Global Enterprise account at Bank-2.

14. A representative from Bank-2 reached out to Okuonghae about Victim-1's wire transfers to Okuonghae's Kenny Global Enterprises, LLC business bank account. In or around January 2022, Okuonghae called Bank-2 and provided them with information that was different than what Victim-1 told the bank. Okuonghae did not mention cryptocurrency investment as a reason for having received the funds. Okuonghae falsely told the bank representative that his business bank account was an operating account for his car parts business. Okuonghae also falsely told the bank that Victim-1's wire transfers were to purchase car engines and car parts, and Okuonghae claimed that he had known Victim-1 for five years and had purchased car parts for Victim-1 in the past.

Online Rental Property Scam

Victim-2:

15. In or around January 2022, Victim-2 searched online to find a rental home. Victim-2 found a home located in Washington state that was listed on a popular rental property website. Victim-2 submitted an online rental agreement containing her personal information.

16. On or about January 9, 2022, Victim-2 received an email from someone purporting to be "Matthew J. Penny." "Matthew J. Penny" told Victim-2 that Victim-2 could lease the rental property, but that Victim-2 needed to wire money to an account to secure the rental. Victim-2 was advised further that Victim-2 would not be able to view the home until the current tenant moved out approximately one month later.

17. On or about January 11, 2022, Victim-2 wired approximately $4,100.00 to Okuonghae's Kenny Global Enterprises bank account at Bank-2. Approximately two days later, Victim-2 was notified by Victim-2's bank that Victim-2 may have been the victim of a fraud scheme. Victim-2 then drove to the address of the home listed on the rental agreement and knocked on the door to ask the current tenant if they were vacating the home in a month. The tenant of the home told Victim-2 that she was not moving, that Victim-2 was

the victim of a scam, and that other people had come to the home with similar inquiries.

Romance Scams

Victim-3:

18. Victim-3, a resident of Washington, was a victim of a romance scam who, as part of the scam, was directed to send money to Okuonghae's Kenny Global Enterprises, LLC account at Bank-3.

19. In or around the middle of 2019, Victim-3 met an individual purporting to be named "Perry Colman" on an online dating website. "Perry Colman" told Victim-3 that he was from Manchester, England, and always wore sunglasses when they video chatted. Victim-3 and "Perry Colman" discussed plans to purchase a house together and get married.

20. Eventually, "Perry Colman" asked Victim-3 to send him money to help with his business in China and Istanbul, and even convinced Victim-3 to quit Victim-3's job. "Perry Colman" told Victim-3 that he had been injured to a degree that required hospitalization. Victim-3 received a call from a woman claiming to be "Perry Colman's" neurosurgeon, who requested that Vicitm-3 send approximately $8,000 to cover the costs of "Perry Colman's" hospitalization and care.

21. A review of records obtained for one of "Perry Colman's" email accounts reflects a message directing money to be sent to Okuonghae's Kenny Global Enterprises Bank-3 account and other bank accounts controlled by other individuals.

22. In or around October 2019, Victim-3 wired approximately $15,000 to Okuonghae's Bank-3 account in the name of Kenny Global Enterprises LLC. The wire noted that it was for a "personal loan."

Victim-4:

23. Victim-4, a resident of California, was the victim of a romance scam who, as part of the scam, was directed to send money to Okuonghae's account at Bank-4 in the name of Kenny Global Enterprises LLC.

24. Victim-4 told law enforcement that Victim-4 met a man who went by the name "Adelbert Gunther" on an online dating website in or around August 2020 and regularly communicated with him. "Adelbert Gunther" directed Victim-4 to wire money to Okuonghae's Bank-4 account in the name of Kenny Global Enterprises LLC.

25. Records from Victim-4's bank account reflect that in or around August 2020, Victim-4 transferred approximately $15,000 to Okuonghae's Bank-4 account in the name of Kenny Global Enterprises.

26. On or about September 16, 2020, an email account believed to be used by Okuonghae, sent an email with the subject "FINAL WORK." I know

from my training and experience that the term "WORK" is often used among criminals as a term to describe information or documents related to a particular fraud scheme. Attached to the "WORK" email were several different invoices for purported trucks/trucking parts. One of the invoices for a Mack Tractor, which would not be shipped but instead would be "pick[ed]up," was addressed to Victim-4 (who resides in California) and was dated September 1, 2020, in the total approximate amount of $15,000.

27. I know from my training and experience that money launderers commonly create and exchange false invoices to conceal the illegally derived nature of the funds they are laundering and to create fake "proof" that they believed the illegally derived money being sent to their accounts was for a legitimate business. Here, the invoice purportedly prepared for Victim-4 is dated *after* the date of the Victim-4's wire transfer to Okuonghae's account, suggesting strongly that the invoice is fake.

Victim-5:

28. Victim-5, a resident of Ohio, was a victim of a romance scam who was directed to send cashier's checks payable to Okuonghae.

29. In or around June 2022, a representative from Victim-5's bank became suspicious of large cashier's checks being procured by Victim-5's accounts. Victim-5 told bank representatives that Victim-5 had met a woman on an online dating website named "Jodie DeSidero." "Jodie DeSidero" told Victim-5 that she was a former army general who used to be deployed in Syria, where she had over a million dollars in Syrian bank accounts. "Jodie DeSidero" promised Victim-5 that if Victim-5 helped her get her money out of Syria, she would give Victim-5 a million dollars. After forming an emotional bond with "Jodie DeSidero," Victim-5 agreed to purchase cashier checks and make them all made payable to "Kenny Okuonghae." Victim-5, at "Jodie DeSidero's" instruction, mailed the cashier's checks to an address in New Jersey.

30. Records from Victim-5's bank reflect that Victim-5 obtained cashier's checks made payable to "Kenny Okuonghae," including the following on or about the following dates:

a. June 13, 2022, in the approximate amount of $15,000;

b. June 17, 2022, in the approximate amount of $37,800;

c. June 22, 2022, in the approximate amount of $44,540; and

d. June 24, 2022, in the approximate amount of $28,600.

Victim 6:

31. Victim-6 was a resident of Connecticut and a victim of a romance scam who was directed to send cashier's checks made payable to Okuonghae.

32. Victim-6 informed Victim-6's bank that Victim-6 had been communicating with an individual named "Jodi DeSiderio," whom he met through an online dating site. "Jodi DeSiderio" told Victim-6 that she was a high-ranking military official in Syria who needed Victim-6's financial assistance to obtain a package that was caught in customs.

33. In or around July 2022, Victim-6 obtained two cashier's checks made payable to "Kenny Okuonghae," one in the approximate amount of $14,995 and the other in the approximate amount of $39,890.

34. Both cashier's checks obtained by Victim-6 were deposited into bank accounts controlled by Okuonghae, one at a branch in Edison, New Jersey and the other at a branch in Staten Island, New York.