IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. 284.99904 ETH CRYPTO CURRENCY, Defendant *in Rem*.	)	CIVIL ACTION NO.: 3:23-cv-00446-MGL

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 284.99904 Ethereum Crypto Currency ("ETH") ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consist of 284.99904 ETH valued at approximately $467,400 in United States Currency, obtained by agents with the United States Secret Service ("USSS"). The funds were seized from cryptocurrency custodial wallet: 0xb99ee5802cb9aab6aedba043fabfca8fd9b0117a under the control of Binance Holdings Limited and under the name Ji Dong.

4. The USSS seized the 284.99904 ETH, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $467,400 in United States Currency.

KNOWN POTENTIAL CLAIMANTS

6. The known individual whose interests may be affected by this litigation are:

(a) Ji Dong who may have an interest in the Defendant Funds because he was the named account holder of the account seized by USSS during this investigation.

(b) Victim 1 identified as V.P may have an interest in the Defendant Funds because he filed a report with the City of Sumter Police Department, reporting that he was scammed out of funds through several cryptocurrency transactions.

(c) Victim 2 identified as C.H. may have an interest in the Defendant Funds because he filed a report with the FBI's Internet Crime Complaint Center, reporting that he was scammed out of funds through several cryptocurrency transactions.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. The Defendant Funds consist of $467,400 seized by USSS on July 6, 2022, pursuant to a seizure warrant issued by a United States Magistrate Judge. The Defendant Funds were located in cryptocurrency custodial wallet: 0xb99ee5802cb9aab6aedba043fabfca8fd9b0117a under the control of Binance Holdings Limited and under the name Ji Dong.

b. Digital currency (also known as virtual currency or cryptocurrency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a physical

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with fiat or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network, often referred to as the blockchain or public ledger. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership, or control of illegally obtained proceeds. Bitcoin ("BTC") is one of the most commonly used and well-known digital currencies. Ethereum ("ETH") is another popular and commonly used digital currency.

c. A stablecoin is a digital currency whose market value is attached to or "pegged" to another stable asset. Differing from normal digital currencies, the value of stablecoins are pegged to assets such as fiat currencies like the United States Dollar ("USD") or the Euro, or other types of assets like precious metals or other digital currencies. Stablecoins are thus used to mitigate the volatility in the price of digital currency by mimicking the value of a fiat currency, without converting digital currency into fiat. While there are various legitimate uses for stablecoins, they are popular with cyber-criminals who seek to hold digital currency

proceeds of crime at a stable or near-fixed value without moving those funds into the legitimate financial system into a fiat currency such as USD. Some examples of stablecoins include:

a. Tether (USDT) was developed by Tether Limited Inc. and is designed to maintain its value at $1.00 USD. USDT can utilize the existing ETH blockchain or the newer TRON ("TRX") blockchain.

b. Binance USD (BUSD), which was developed by Binance Holdings Limited and Paxos Trust Company, LLC, is designed to maintain its value at $1.00 USD. BUSD utilizes the existing ETH blockchain.

d. A digital currency exchange (an "exchange") is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Most exchanges are located outside the boundaries of the United States in order to avoid regulation and legal requirements, but some popular exchanges operate inside the jurisdiction of the United States. Binance is an example of a popular online exchange that is located outside of the United States but cooperates with and accepts legal process from American law enforcement agencies.

e. A wallet is a means of storing digital currency identified by unique electronic addresses that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be

analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchanger to make a transaction between digital currency and fiat, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

f. Although cryptocurrencies such as Bitcoin, Ethereum and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

Use of Target Cryptocurrency Wallet to Defraud Victim 1

g. On May 23, 2022, Victim 1 identified as V.P filed a report with the City of Sumter Police Department, reporting that he was scammed out of $372,439 through several

cryptocurrency transactions. V.P stated the unknown actors developed a connection with him through the social media and communication applications Twitter and WhatsApp. WhatsApp is an end-to-end encrypted chat. Targets commonly prefer end-to-end encrypted communications to facilitate criminal activity, including cryptocurrency fraud schemes, because such platforms provide real or perceived protections against detection and recovery of the content of communications. WhatsApp is commonly used to communicate with subjects overseas.

h. On February 16, 2022, V.P. received a message on Twitter from an unknown individual who identified themself as "OuYangBingBing." The conversation began by sharing cooking recipes and turned quickly into financial talk about cryptocurrency and investing. The two continued to communicate and "OuYangBingBing" befriended the victim and offered to become his financial coach. "OuYangBingBing" eventually convinced V.P. to download Nexo.io and create an account for trading. Nexo.io is an online cryptocurrency exchange that allows users to purchase and exchange different types of cryptocurrencies and fiat currency. Nexo.io is based out of Zug, Switzerland. The communication continued, but "OuYangBingBing" requested they change platforms of communication to WhatsApp messenger. Upon switching to WhatsApp, the same identifier was used as "OuYangBingBing" with phone number 202-247-8921. As a result of his communications with the target on WhatsApp, V.P. was induced to transfer money

to accounts as directed by "OuYangBingBing" under the premise that V.P. was investing in legitimate cryptocurrency investment vehicles.

i. Specifically, between February 16, 2022 and March 7, 2022, V.P. completed several wire transfers and subsequently several digital currency transfers from V.P. fiat into digital currency accounts at the direction of "OuYangBingBing." Victim 1 transferred $375,000.00, from his Wells Fargo bank account into an account that V.P. created Nexo.io, the Switzerland based digital currency exchanger. Once the funds were active in Victim 1's Nexo.io cryptocurrency account, the value in US dollars deposited was converted to USDT (Tether) cryptocurrency at the direction of "OuYangBingBing" and "Nami Morikawa" through WhatsApp messaging. Nami Morikawawas was introduced to V.P. as a "customer support representative" to assist in the investment process and provide technical support. Once the funds were successfully converted to USDT, V.P. was duped into navigating to a website that is likely controlled by "OuYangBingBing," "Nami Morikawa," or their affiliates.

j. There is evidence that the website was designed to closely resemble a legitimate digital currency platform, BitPay, leading V.P. to believe the website was affiliated with BitPay. The link V.P. was induced to navigate to was http://www.bitpaypro.xyz rather than the legitimate URL, http://www.bitpay.com. This link provided was made to imitate the legitimate BitPay URL, but the addition of "Pro" and ".xyz" indicate it instead was a faked and spoofed website

made to appear as the legitimate website. In fact, V.P. was specifically directed by the target(s) to not go to the traditional BitPay mobile application, but instead to go to the URL provided. All of this provides evidence that the website provided to V.P. is associated with a fraud scheme.

k. In February 2022-March 2022, V.P. engaged in a series of transfers to accounts as directed by the target: to the following wallets: (Transfer A) In USDT to wallet 0x0b78177f4f016902565fb0a9454a1319ada4f733 given by bitpaypro.xyz, (Transfer B) In USDT and USDC to wallet 0xa5326eb40ca60a3e9f8a33076a007e9a2a358f7b given by direct message through WhatsApp from "OuYangBingBing", and (Transfer C) In ETH to wallet 0x517070883d4184f62ad635467d0d1cb3629b63eb through m.funcube.org at the direction of "OuYangBingBing" via WhatsApp messaging. The transfers totaled $372, 439.00 in United States Dollars.

l. V.P. began to believe he was part of a fraudulent scheme. On or after March 17, 2022, V.P. requested "OuYangBingBing" to return all of the funds he had transferred to bitpaypro.xyz and m.funcube.org accounts back to him, and "OuYangBingBing" refused to do so unless V.P. paid an additional $60,000.00 U.S. dollars in 'taxes' to release the money. The target(s) ceased communicating at all with V.P.

m. On June 6, 2022, SA Hannon sent the above three wallet addresses to a USSS Investigative Analyst who performs cryptocurrency tracing for USSS. The analyst

located wallets and determined they were maintained by the cryptocurrency exchange Binance Holdings Limited. The analyst traced the transactions of funds associated with the transfers across the blockchain and determined that Victim 1's funds associated with those transfers were sent to the following USDT addresses:

a. 0xaca4fd92172de9c88e29d32713fa4d81a0dc7dee;
b. 0x239a5c2e92a1ae5ff9221fd23a45e6004636c0b7;
c. 0x0f60439bb2a1a05b604a512f1a96c79a7ddce369; and
d. 0x515a5d995ffeb43f114e00743a340f0da2db18e8

The funds were then comingled and distributed to other wallets as funds commonly are in the blockchain and money laundering schemes before being deposited as here.

n. Based on SA Hannon's training and experience, the scheme described above is a common scheme used to defraud victims into sending money to an account of the choosing of the bad actor and there is probable cause to believe the target(s) defrauded V.P. out of $372,439.00 by leading him to believe he was investing the funds in a legitimate cryptocurrency vehicle when in truth and in fact it was a false, fraudulent, and spoofed investment vehicle designed to defraud V.P. of his funds.

o. This investigation has produced evidence that another victim has been defrauded of $125,000.00 in nearly identical circumstances also through the spoofed bitpaypro.xyz website, providing evidence that the fraud is broader than what is described with respect to V.P.

Bitpaypro.xyz Scheme Used to Defraud Victim 2

p. On March 31, 2022, Victim 2 identified as C.H. filed a report with the FBI's Internet Crime Complaint Center (IC3) Report # 12203311103383171, through which C.H. detailed how he was scammed out of $125,000.00 through several cryptocurrency transactions. C.H. stated that unknown actors developed a connection with him through the online communication applications Facebook Messenger and WhatsApp.

q. On or about September 15, 2021, C.H. received a Facebook message from a user with the profile name "Lin" who appeared to be a female of Asian descent and was "very attractive" according to C.H. The conversations continued for a few weeks ranging in topics from casual lifestyle to investment strategy. Once the investment conversations began, "Lin" requested the conversation change applications to WhatsApp, just as what occurred with the first victim, V.P. The conversation began on WhatsApp following "Lin's" suggestion with a contact number 202-247-8921, the same phone number used to communicate with Victim 1 for the same investment scheme. "Lin" then aggressively purported that she would coach and mentor C.H. on how to make money through investing because her aunt allegedly worked for MCB Fortis, a legitimate bank located in New York City that serves as the corresponding bank for cryptocurrency exchangers such as Crypto.com. Crypto.com is an online cryptocurrency exchange that allows users to purchase

and exchange different types of cryptocurrencies and fiat currency. "Lin" alleged her aunt worked on the cryptocurrency trading floor and would provide the best possible information for C.H. to succeed.

r. Between November 10, 2021 and February 23, 2022, C.H. completed at least ten separate wire transfers from his personal account to MCB Fortis, totaling $95,300.00 as directed by "Lin" through WhatsApp. C.H. sent the money from his personal account which he owns and operates, to a Crypto.com account which he created and operated in order to invest in cryptocurrency as directed by "Lin." C.H. deposited each wire transfer into his Crypto.com account and immediately converted the USD to digital coin, Tether (USDT), under the direction of "Lin." Upon successfully converting USD to USDT, C.H. was then instructed – just like Victim 1 –to navigate to bitpaypro.xyz, the same website used by Victim 1 to deposit his USDT to "Lin." As described in the Victim 1 section above, this URL appeared to be designed to imitate the legitimate URL of BitPay but in truth and in fact was a spoofed website that sent the visitor to a location that was not the legitimate BitPay platform.

s. Beginning on November 10, 2021 and continuing through February 23, 2022, C.H. purchased and sent in USDT to wallet bitpaypro.xyz provided by "Lin" in conjunction with bitpaypro.xyz in an amount that totaled $95,300.00. Beginning January 4, 2022, "Lin" began demanding C.H. pay "taxes" if he wanted to have access to the money he invested, just as the target(s) did with the

first victim. C.H. complied with requests from "Lin," and over the final three (3) transactions, C.H. sent additional money for "taxes" in an effort to access his money. In response to the additional payments, "Lin" then demanded C.H. fill out a form captioned "Internal Revenue Office" from Hong Kong that would have required C.H. to disclose additional personal data. After C.H. ultimately declined to fill out and submit that form, communications from the target(s) stopped immediately, and C.H. was unable to retrieve any of his funds.

t. There is probable cause to believe that the fraud perpetuated against Victim 1 and Victim 2 were conducted by the same target(s) given the nearly identical method and means, victim, and transfers, and the use of the same phone number on WhatsApp and the same spoofed bitpaypro.xyz URL to defraud both victims.

u. On June 15, 2022, USSS Investigative Analyst and SA Hannon continued to research investigative leads regarding bitpaypro.xyz. The investigation produced evidence that the targets(s) associated with that website appear to have registered numerous websites through NameCheap.com located in Iceland that are designed to appear as if they are legitimate cryptocurrency investment vehicles, when in truth and in fact they are not.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957

CONCLUSION

9. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

Adair F. Boroughs
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

February 1, 2023