

IN THE CIRCUIT COURT OF THE EIGHTEENTH JUDICIAL CIRCUIT  
IN AND FOR BREVARD COUNTY, FLORIDA

CASE NO: 05-2022-CA- XXX-XX  
CIVIL FORFEITURE

IN RE: FORFEITURE OF:

CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE  
WALLET(S) NUMBER UID 153035005 REGISTERED TO “YICAI LUO” TO WIT:

USDT	TetherUS	238830.7437
CAKE	PancakeSwap	14771.75682
ETH	Ethereum	27.73634179
BNB	BNB	89.69501919
SFP	SafePal	60060.07842
BTC	Bitcoin	1.0000034
UNI	Uniswap	2749.764169
ADA	Cardano	38740.48277
DOGE	Dogecoin	140031.784
DOT	Polkadot	960.8127723
ETHW	Ethereum PoW	27.73634179
AAVE	Aave	2.184973
LUNC	Terra Classic	0.00079

CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE  
WALLET(S) NUMBER UID 198318266 REGISTERED TO “LUA HENG MUN” TO  
WIT:

USDT	TetherUS	2000.2
USDT	TetherUS	295.5257

Defendant Property.

\_\_\_\_\_ /

**VERIFIED COMPLAINT/PETITION FOR JUDGMENT OF FORFEITURE**

The Petitioner, THE BREVARD COUNTY SHERIFF’S OFFICE, by and through the undersigned counsel, pursuant to the Florida Contraband Forfeiture Act sections 932.701–7062, Florida Statutes, and files this Verified Complaint/Petition for Judgment of Forfeiture and alleges:

**SUBJECT MATTER**

1. This is a civil action for forfeiture *in rem* of:

a. CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE WALLET(S) NUMBER UID 153035005 REGISTERED TO “YICAI LUO” TO WIT:

i. USDT	TetherUS	238830.7437
ii. CAKE	PancakeSwap	14771.75682
iii. ETH	Ethereum	27.73634179
iv. BNB	BNB	89.69501919
v. SFP	SafePal	60060.07842
vi. BTC	Bitcoin	1.0000034
vii. UNI	Uniswap	2749.764169
viii. ADA	Cardano	38740.48277
ix. DOGE	Dogecoin	140031.784
x. DOT	Polkadot	960.8127723
xi. ETHW	Ethereum PoW	27.73634179
xii. AAVE	Aave	2.184973
xiii. LUNC	Terra Classic	0.00079

b. CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE WALLET(S) NUMBER UID 198318266 REGISTERED TO “LUA HENG MUN” TO WIT:

i. USDT	TetherUS	2000.2
ii. USDT	TetherUS	295.5257

(hereinafter referred to as THE CONTRABAND PROPERTY), brought pursuant to The Florida Contraband Forfeiture Act, section 932.701 et. seq., Florida Statutes, arising from violations of sections 812.014, 817.034, 896.101, and 895.03, Florida Statutes.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to section 932.704(2), Florida Statutes.
3. This Court also has *in rem* jurisdiction over THE CONTRABAND PROPERTY and venue lies in Brevard County pursuant to section 47.011, Florida Statutes, in that THE CONTRABAND PROPERTY was seized by law enforcement officers on or about October 21, 2022, pursuant to a criminal investigation, particularly described hereinafter, occurring regarding Binance Holding Ltd. d/b/a Binance wallet/accounts numbered [REDACTED] registered to “YICAI LUO” and 198318266 registered to “LUA HENG MUN,” under Agency Case Number(s) 2022-270411, and THE CONTRABAND PROPERTY will

remain within Brevard County during the pendency of this civil forfeiture action in the custody/control of The Brevard County Sheriff's Office, 700 S. Park Avenue, Titusville, FL 32780, under Agency Case Number(s) 2022-270411.

THE PARTIES AND POTENTIAL CLAIMANT(S)

4. The Petitioner and the seizing law enforcement agency, as set forth in section 932.703, Florida Statutes, is the BREVARD COUNTY SHERIFF'S OFFICE (hereinafter referred to as "BCSO").
5. Information in the possession of the Petitioner indicates that as to Binance wallet/account number [REDACTED], YICAI LUO may claim an interest and as to Binance wallet/account number [REDACTED] LUA HENG MUN may claim an interest in THE CONTRABAND PROPERTY by virtue of possession, ownership registration law, or other claim of ownership, or by virtue of a lien purportedly perfected in the manner prescribed by law. However, at this time, no person has established standing to contest the forfeiture in the instant matter.

THE INVESTIGATION

6. The criminal investigation resulting in the seizure of THE CONTRABAND PROPERTY uncovered the following:
  - a. On August 1st, 2022, Tony Lawter of 4509 Ponds Drive, Cocoa, Brevard County, Florida reported to the Brevard County Sheriff's Office Economic Crimes Unit that he fell victim to a cryptocurrency romantic investment scam which resulted in the loss of approximately \$177,502.29.
  - b. Tony Lawter met an individual known to him as "Bunny" through social media (Facebook) and started a romantic relationship with her. During the relationship,

Bunny offered Mr. Lawter a way to make money through cryptocurrency so they could afford to buy a farm and live together one day.

- c. Known as “Pig butchering” schemes, these scams originated in Southeast Asia and are predominately executed by a ring of cryptocurrency scammers. The scam incorporates a romance scam, building a long-term communication relationship with the victim, typically using social media or dating applications. Once the trust of the victim is gained, the suspect(s) propose an investment opportunity using cryptocurrency and fraudulent or fake cryptocurrency investment platforms.
- d. During the relationship, Bunny convinced Tony Lawter to invest in cryptocurrency through “Pearcoin,” a fake cryptocurrency trading application, unknown to Tony Lawter at the time.
- e. Ultimately, Lawter attempted to withdrawal his funds from Pearcoin and was told he must pay the taxes up front or he would risk a 3% deduction each day he did not pay. At this point, Lawter realized he was involved in a scam and subsequently contacted the Brevard County Sheriff’s Office to report the incident. Lawter was unable to transfer, withdrawal, or access any of his funds through the investment platform.
- f. Agent Justin Wood completed a tracing analysis of Tony Lawter’s outgoing transactions and discovered that in two (2) of the transactions Tony Lawter completed, the final destination was a wallet address associated with an account at Binance Holding Ltd. d/b/a Binance (hereinafter “Binance”). A third transaction Tony Lawter completed was analyzed and determined to have been received by a wallet address associated with a second account at Binance.

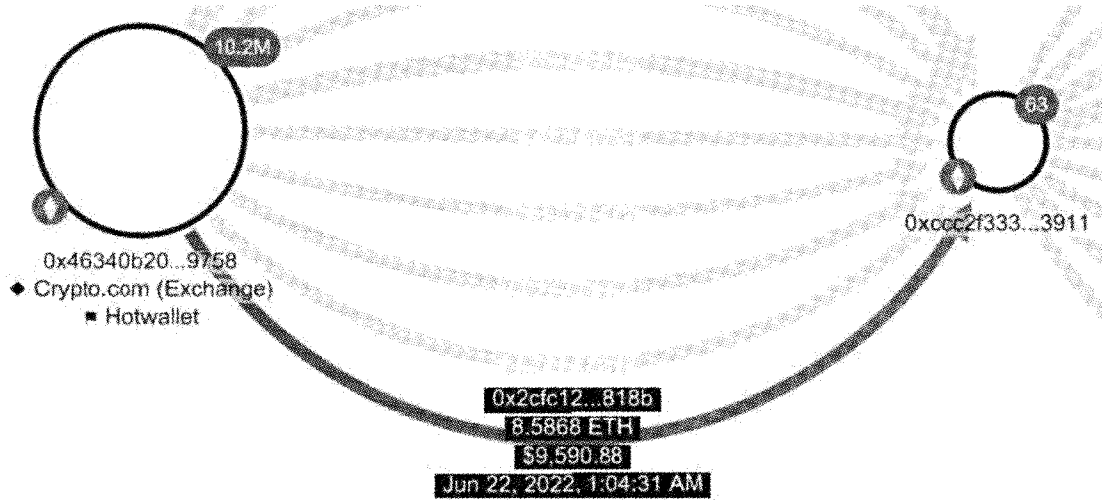
- g. Agent Justin Wood discovered the first Binance account (Account # [REDACTED]) was owned by Yicai Luo, a male from China and the second Binance account (Account # [REDACTED]) was owned by Lua Heng Mun, a male from Malaysia. Tony Lawter believed he was investing in his romantic relationship and did not indicate he was ever conducting business with any persons from China or Malaysia.
- h. Prior to tracing the final comingled funds in Luo's and Mun's Binance account, Agent Wood received the following information: On August 23<sup>rd</sup>, 2022, Crypto.com responded to a subpoena request and supplied account information for Lawter's Crypto.com account. Through the information provided by Crypto.com, Agent Justin Wood located thirteen (13) withdrawal transaction from Lawter's account. The thirteen (13) withdrawals totaled over 132 Ethereum (valued at \$177,502.39 at the time of the subpoena response). Of the thirteen (13) withdrawal transactions, Agent Justin Wood observed that twelve (12) of the transactions went to a single Ethereum wallet address, 0xccc2f333e57cb739a3a62ed1e7a76ce17d3c3911. Of the twelve (12) transactions, nine (9) withdrawal transactions were greater than four (4) Ethereum. Agent Justin Wood focused on the nine (9) transactions which contained a greater amount and accounted for almost all of Lawter's funds.
- i. Agent Justin Wood utilized the Ethereum blockchain to trace the Ethereum that Lawter had sent to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ce17d3c3911, in which he believed he was investing in cryptocurrency. Agent Justin Wood determined that once Lawter sent

Ethereum to 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911, that wallet address utilized an Ethereum smart contract to convert the received Ethereum into Tether (USDT), which is a stable coin pegged to the United States Dollar (USD).

- j. One transaction in particular occurred on June 22<sup>nd</sup>, 2022 at 12:59 PM. The transaction included Lawter’s Crypto.com account which sent approximately 8.590725 Ethereum (ETH) to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. (See Step # 1 below)

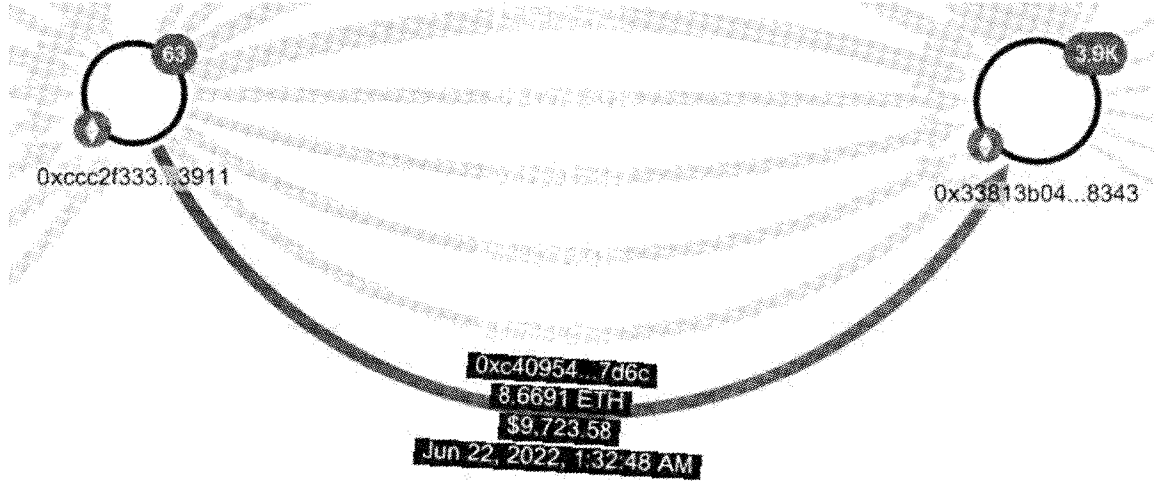
**TRANSACTION # 1**

**STEP #1**



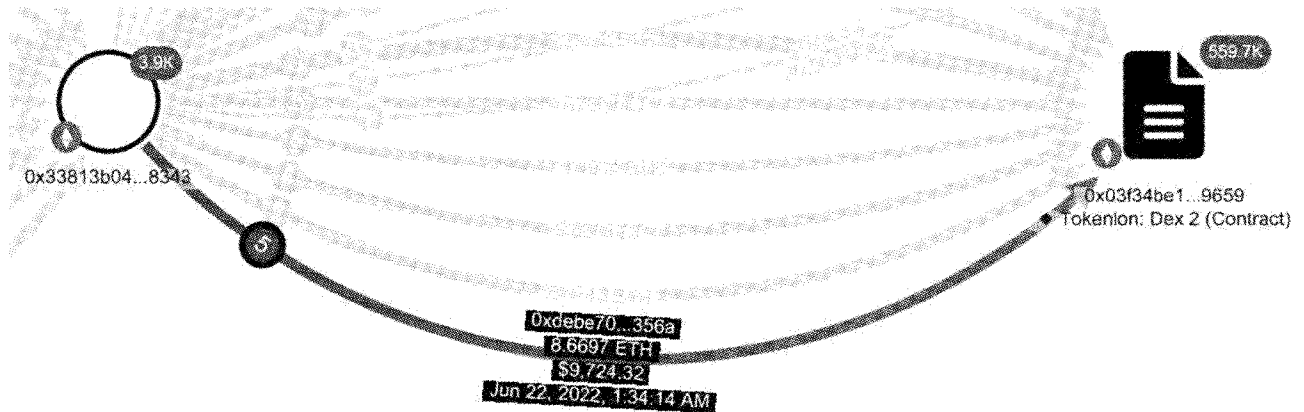
- k. After wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911 received the funds, ~8.5868 ETH, the funds were then sent to wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. This transaction occurred on June 22<sup>nd</sup>, 2022 at 1:32 AM. (See Step # 2 below)

**STEP # 2**



- I. After wallet address `0x33813b04ca9dab0a2f41ae2c1a617d946e708343` received the funds, ~8.6691 ETH, the wallet address then used a smart contract to convert the ETH to USDT. This transaction occurred on June 22nd, 2022 at 1:34 AM. (See Step # 3 below)

**STEP # 3**

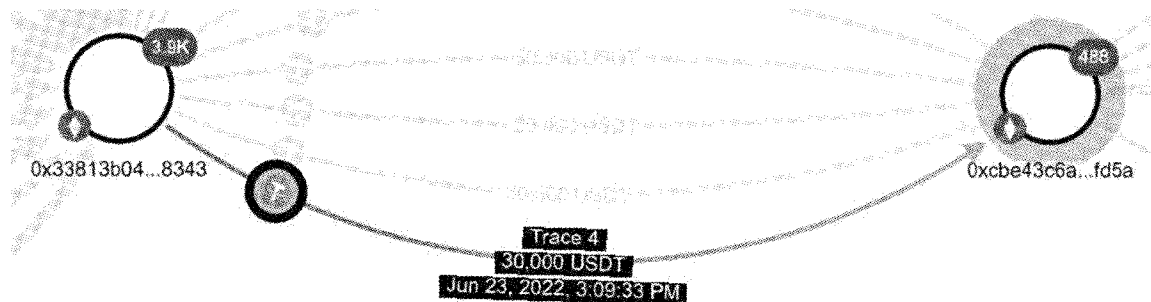


- m. As a result of the ETH to USDT conversion, wallet address `0x33813b04ca9dab0a2f41ae2c1a617d946e708343` received approximately 9,728.28 USDT. The transaction HASH, or HASH ID, for the conversion was `0xc40954ded5f9ccca4d3984454fa6a98af593d92436190d6951412737d361356a`.

A HASH ID is a unique string of letters and numbers assigned to each transaction which is posted to the Ethereum blockchain.

- n. After the funds, 9,728.28 USDT, were received by wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343, the funds were then sent to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a. This transaction occurred on July 23rd, 2022 at 3:09 PM. It should be noted Lawter's funds, 9,728.28 USDT, were co-mingled with additional funds from unknown sources. Wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 sent Lawter's funds, and co-mingled funds, to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a, which totaled 30,000 USDT. (See Step # 4 below)

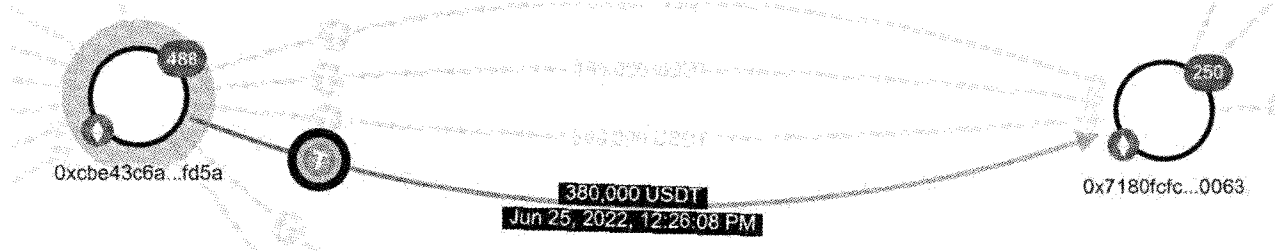
**STEP # 4**



- o. After wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 30,000 USDT, the funds were then transferred. On June 25th, 2022 at 12:26 PM wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a sent 380,000 USDT to wallet address 0x7180fcfc7b7913948920b84387579daf97530063. The transfer included co-mingled funds from wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. (See Step # 5 below)



### STEP # 5



- p. After wallet address 0x7180fcfc7b7913948920b84387579daf97530063 received the funds, 380,000 USDT, the funds were then transferred. On July 13th, 2022 at 6:55 AM wallet address 0x7180fcfc7b7913948920b84387579daf97530063 sent 615,686 USDT to wallet address 0x8459dd488c507b20331e0f6ac481f75ee9f4ae97. The transfer included commingled funds from wallet address 0x7180fcfc7b7913948920b84387579daf97530063. (See Step # 6 below)

### STEP # 6

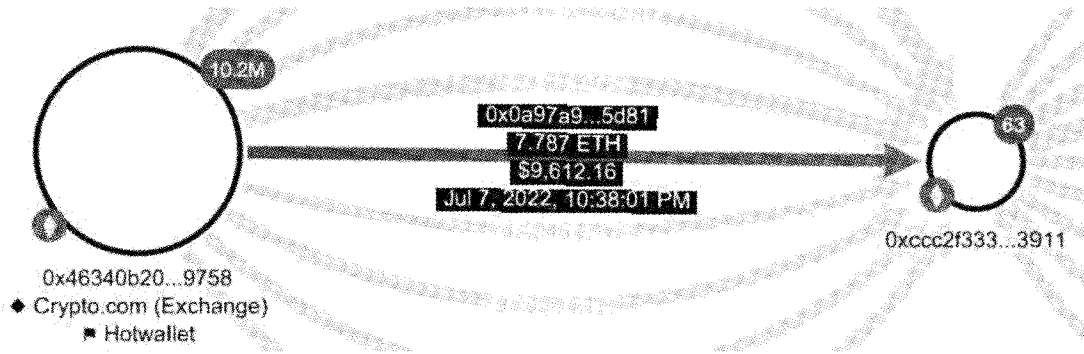


- q. Through cryptocurrency tracing tools, Agent Wood identified wallet address 0x8459dd488c507b20331e0f6ac481f75ee9f4ae97 as being associated with the wallet address is 153035005 which is registered to Yicai Luo.

**TRANSACTION # 2**

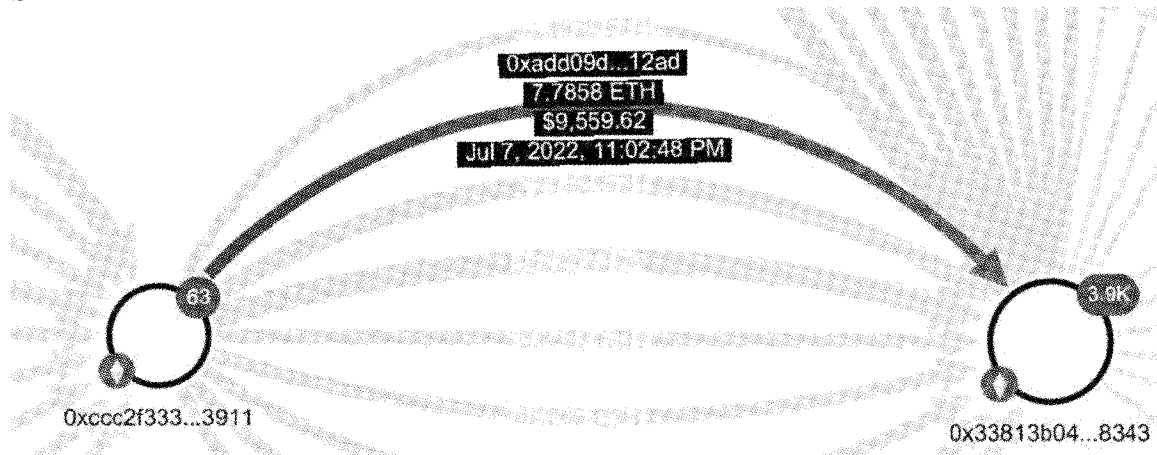
- r. The second transaction in question occurred on July 7th, 2022 at 10:37 PM. The transaction included Lawter’s Crypto.com account which sent approximately 7.790992027 Ethereum (ETH) to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. (See Step # 1 below)

**STEP # 1**



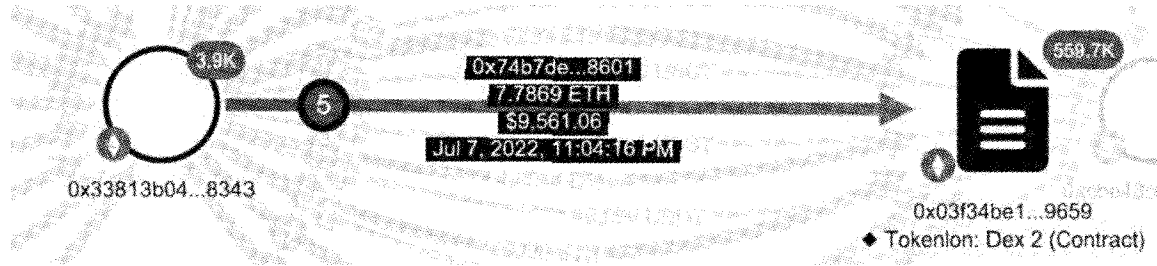
- s. After wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911 received the funds, ~7.787 ETH, the funds were then sent to wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. This transaction occurred on July 7th, 2022 at 11:02 PM. (See Step # 2 below)

**STEP # 2**



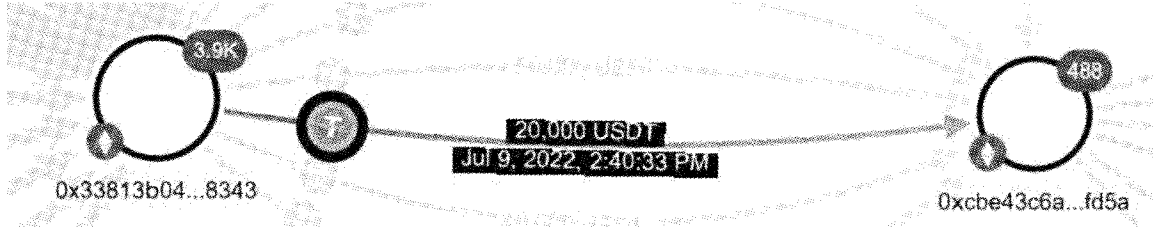
- t. After wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received the funds, ~7.7858 ETH, the wallet address then used a smart contract to convert the ETH to USDT. This transaction occurred on July 7th, 2022 at approximately 11:04 PM. (See Step # 3 below)

**STEP # 3**



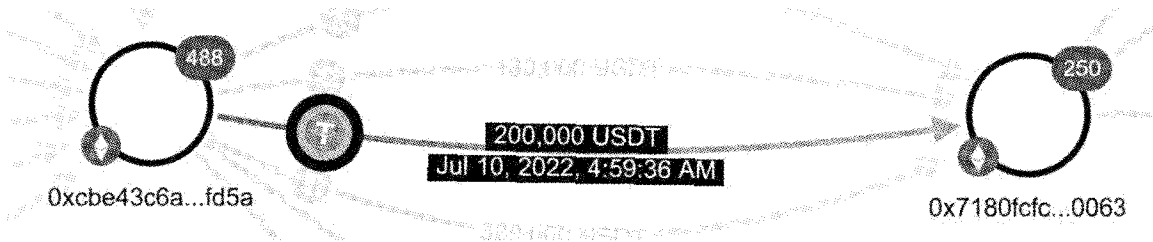
- u. As a result of the ETH to USDT conversion, wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received approximately 9,575.95 USDT. The transaction HASH, or HASH ID, for the conversion was 0x74b7ded0efe4e9cf569febca9bc91cd683f35a695b81f5c11058b24f4f498601.
- v. After the funds, 9,575.95 USDT, were received by wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343, the funds were then sent to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a. This transaction occurred on July 9th, 2022 at 2:40 PM. Wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 sent Lawter's funds, and co-mingled funds, to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a, which totaled 20,000 USDT. (See Step # 4 below)

#### STEP # 4



w. After wallet address `0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a` received the 20,000 USDT, the funds were then transferred. On July 10th, 2022 at 4:59 AM wallet address `0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a` sent 200,000 USDT to wallet address `0x7180fcfc7b7913948920b84387579daf97530063`. The transfer included co-mingled funds from wallet address `0x33813b04ca9dab0a2f41ae2c1a617d946e708343`. (See Step # 5 below)

#### STEP # 5



x. After wallet address `0x7180fcfc7b7913948920b84387579daf97530063` received the funds, 200,000 USDT, the funds were then transferred. On July 13th, 2022 at 6:55 AM wallet address `0x7180fcfc7b7913948920b84387579daf97530063` sent 615,686 USDT to wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97`. The transfer included co-mingled funds from wallet address `0x7180fcfc7b7913948920b84387579daf97530063`. (See Step # 6 below)

## STEP # 6



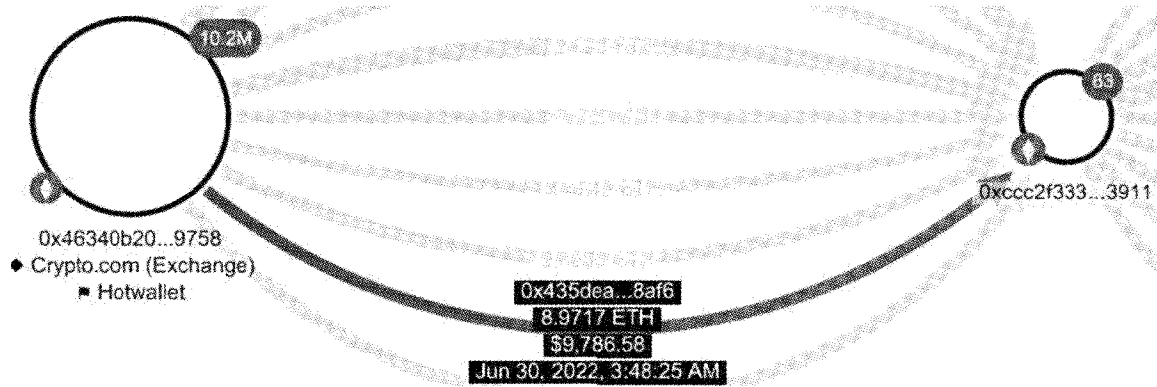
- y. Through cryptocurrency tracing tools, Agent Wood identified wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97` as being associated with Yicai Luo's account at Binance. Wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97` was the same wallet address that received funds from "TRANSACTION #1" described above.
- z. Agent Wood located the above pictured transactions (TRANSACTION #1: STEP # 6 and TRANSACTION # 2: STEP # 6), and observed the funds, 615,686 USDT enter Luo's Binance account on July 13th, 2022 at 6:56 AM. Approximately twenty-four (24) minutes after the funds entered Luo's account, Luo completed a withdrawal transaction. The transaction was on July 13th, 2022 at 7:20 AM, and consisted of 1,399,996 USDT being sent to wallet address `0x5453fd1ef17c8c4F2042b07416573c3eCa19D247`.
- aa. Agent Wood used open source Ethereum blockchain to continue to trace the funds. Once wallet address `0x5453fd1ef17c8c4F2042b07416573c3eCa19D247` received the funds on July 13th, 2022 at 7:21 AM, the funds were immediately transferred to wallet address `0x3d1d8a1d418220fd53c18744d44c182c46f47468`. This outgoing transaction, for 1,399,996 USDT, occurred on July 13th, 2022 at 7:27 AM

- bb. Using open sources, Agent Wood determined that wallet address 0x3d1d8a1d418220fd53c18744d44c182c46f47468 was a Bitkub hot wallet. Bitkub is a cryptocurrency exchange based out of Thailand.
- cc. Based on Agent Wood's training and experience, he concluded that the actions Luo's account completed were indicative of an account involved in fraud schemes and money laundering. Luo's account, and the transactions prior, were attempts to disguise the original source of funds, which was acquired through false pretenses. Luo's account had a consistent pattern of the above described movement of funds which is common among fraud suspects. Luo's account, once it received USDT had completed one hundred and sixteen (116) transactions, totaling approximately 54,387,177 USDT, between January 14th, 2022, and August 29th, 2022. The quick and rapid movement of fraudulently obtained funds to an exchange based outside of the United States, in an effort to avoid account seizure is common practice of those involved in the money laundering of cryptocurrency assets.
- dd. Luo's account also had another consistent pattern used to launder money. The technique known as "chain hopping" and has been identified as one of the fastest-growing money laundering typologies. This layering technique consists of converting one form of cryptocurrency to another and moving the funds from one blockchain to another. In this case, Luo's account had a pattern of receiving USDT and transferring the funds to a TRON wallet address hosted on the TRON blockchain. This technique is common in schemes to defraud and money laundering and its purpose is to disguise the source of funds and make tracing the stolen funds more difficult for law enforcement. Luo's account completed ninety-

- nine (99) withdrawal transaction to various TRON wallet addresses which were hosted on the TRON blockchain between June 20th, 2021, and August 29th, 2022. These ninety-nine (99) transactions totaled approximately 19,116,832.80 USDT.
- ce. On October 25th, 2022, Binance alerted Agent Justin Wood that the REACT Task Force, based out of California, had been working an investigation and had interest in Yicai Luo's Binance account. Agent Justin Wood contacted Sergeant Brad Smith of the Milpitas Police Department and Task Force Officer of the REACT Task Force to deconflict.
- ff. Sgt. Smith provided information on an individual in Los Angeles, California who had fallen victim to a "pig butchering" scheme. Sgt. Smith, provided Agent Justin Wood with a Los Angeles Police Department Investigative Report filed on August 23rd, 2022.
- gg. The victim, Tai Feng Tang, reported she had been romantically involved with an individual through social media. During the relationship, she was convinced to invest in cryptocurrency. Ms. Tang reported a loss of approximately \$300,000.00. Sgt. Smith provided his trace analysis which showed Ms. Tang had completed four (4) USDT (Tether) transactions to what she believed was an investment platform. One of the transactions Sgt. Smith provided showed part of Tang's funds (approximately 81,696 USDT) were traced and ultimately transferred to Yicai Luo's Binance account.
- hh. Next, Agent Justin Wood conducted a trace analysis on a third transaction Tony Lawter completed on June 30th, 2022 at 0348 hours. The transaction included

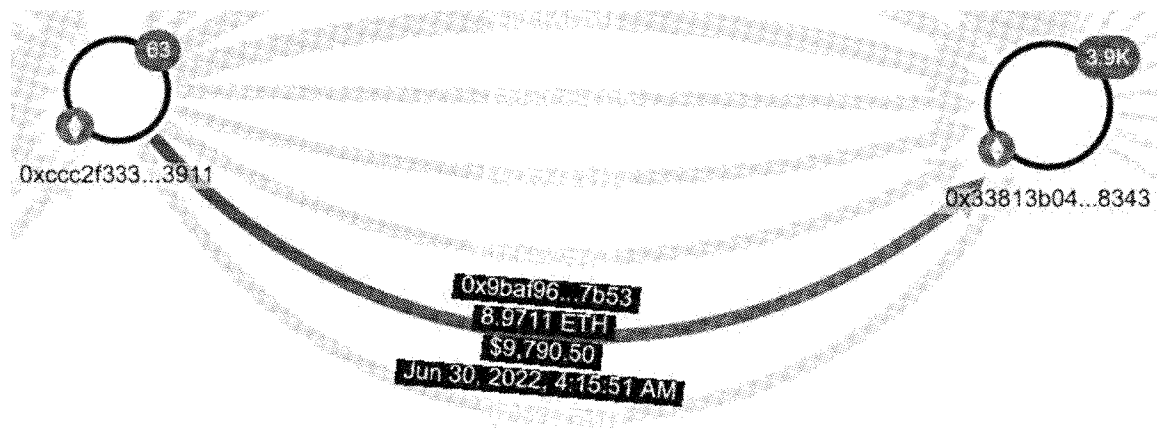
Lawter's Crypto.com account, which sent 8.975636 Ethereum (ETH) to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. (See Step # 1 below)

**STEP #1**



- ii. After wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911 received the funds, ~8.97 ETH, the funds were then sent to wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. This transaction occurred on June 30th, 2022 at 0415 hours. (See Step # 2 below)

**STEP # 2**

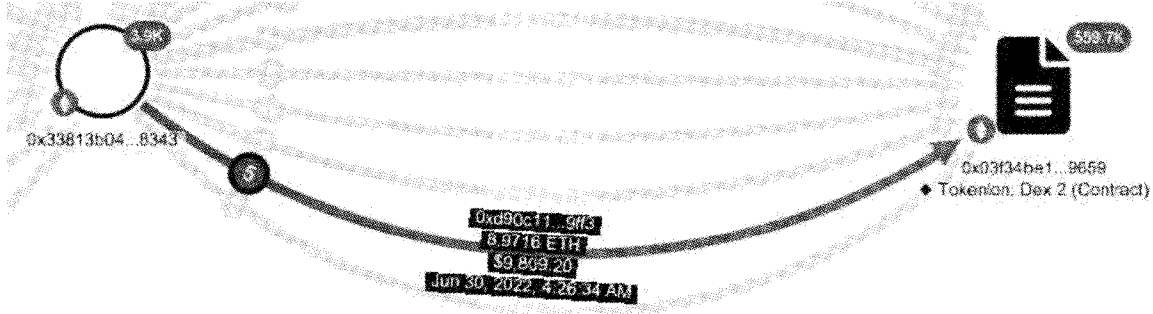


- jj. After wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received the funds, ~8.97 ETH, the wallet address then used a smart contract to convert the



ETH to USDT. This transaction occurred on June 30th, 2022 at 0426 hours. (See Step # 3 below)

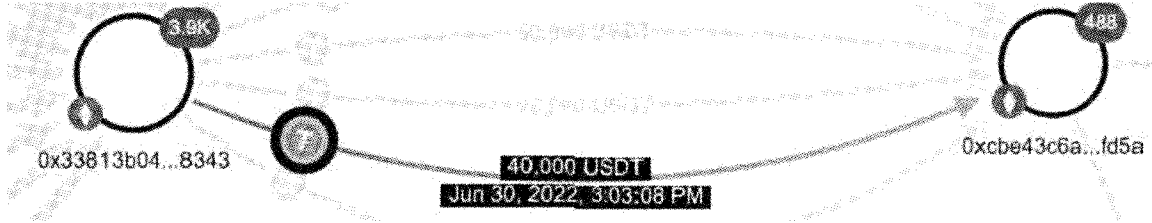
**STEP # 3**



kk. As a result of the ETH to USDT conversion, wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received 9,796.84 USDT. The transaction HASH, or HASH ID, for the conversion was 0xd90c1137c4d0f2163f3c859ad6977d7b205713c4bbc6f2907c1e92b636929ff3.

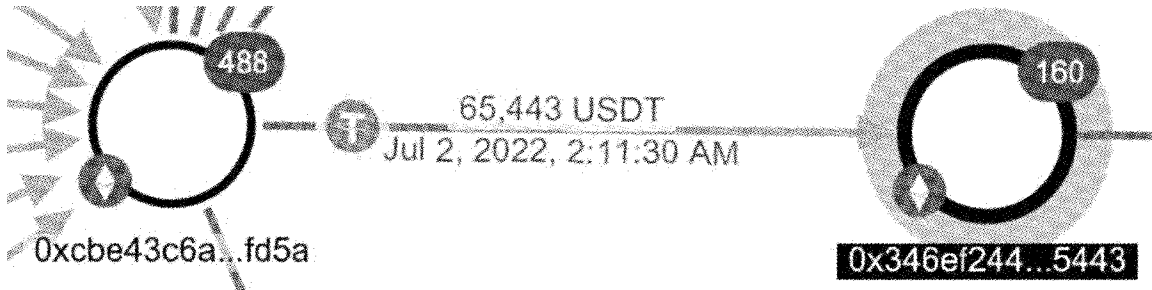
ll. After the funds, ~9,796.84 USDT, were received by wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343, the funds were then sent to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a. This transaction occurred on June 30th, 2022 at 1503 hours. Lawter's funds, ~9,796.84 USDT, were co-mingled with additional funds from unknown sources. Wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 sent Lawter's funds, and co-mingled funds, to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a, which totaled 40,000 USDT. (See Step # 4 below)

**STEP # 4**



mm. After wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 40,000 USDT, the funds were then transferred. On July 2nd, 2022 at 0211 hours wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a sent 65,443 USDT to wallet address 0x346ef244464679b031750f70d750b3fa65165443. The outgoing transfer was the next transaction posted after wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 40,000 USDT. (See Step # 5 below)

**STEP # 5**



nn. After wallet address 0x346ef244464679b031750f70d750b3fa65165443 received the funds, 65,443 USDT of the funds were then transferred to wallet address 0x1970118296c32923c1039a775ac6fb90dfec2419. The transaction occurred on July 11th, 2022 at 0951 hours. (See Step # 6 below)

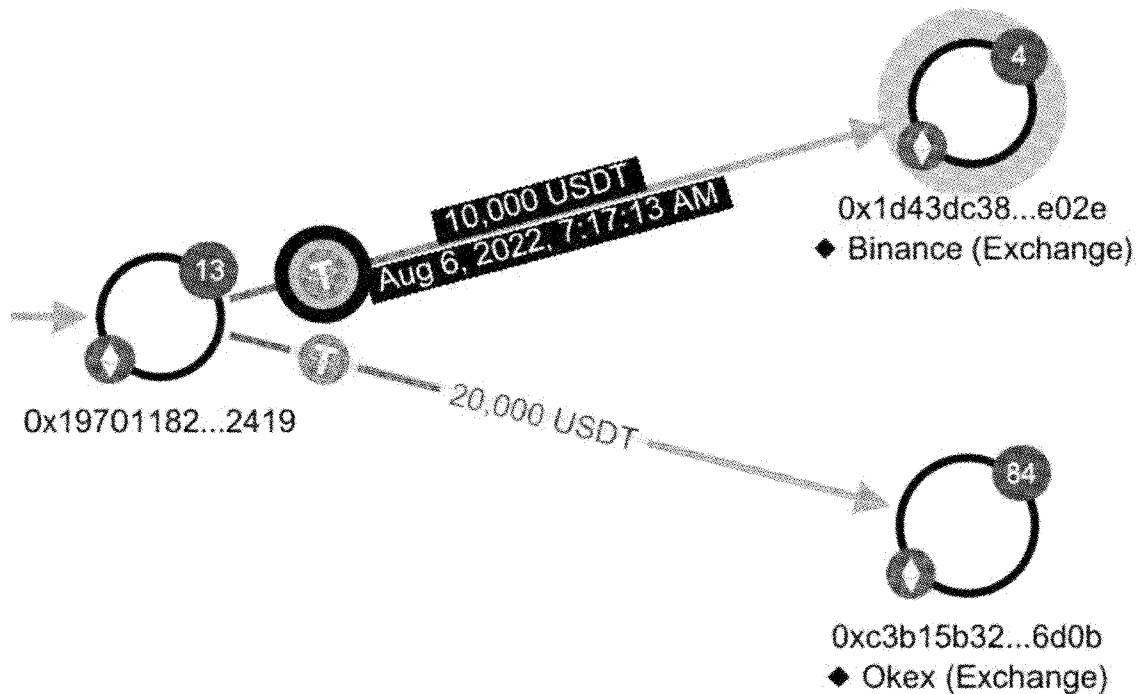
**STEP # 6**



oo. After wallet address 0x1970118296c32923c1039a775ac6fb90dfec2419 received the funds, 30,000 USDT of the funds were then sent to two (2) different wallet addresses via two (2) separate transactions. The transactions were as follows:

- i. August 2nd, 2022 at 0442 hours for 20,000 USDT to wallet address 0xc3b15b326c0ed1576f918a3b36c9de789f936d0b.
- ii. August 6th, 2022 at 0717 hours for 10,000 USDT to wallet address 0x1d43dc389993cb3818724e0d06746bbaa6a9e02e. (See Step # 7 below)

**STEP # 7**



- pp. Through cryptocurrency tracing tools, Agent Wood identified wallet address 0xc3b15b326c0ed1576f918a3b36c9de789f936d0b as being associated with an account at Okex, a cryptocurrency exchange. Based on prior investigations, Agent Wood was aware the Okex exchange does not cooperate with United States based law enforcement.
- qq. Through cryptocurrency tracing tools and Binance confirmation, Agent Wood identified wallet address 0x1d43dc389993cb3818724e0d06746bbaa6a9e02e as being associated with account number [REDACTED] at Binance, which is an account owned by Lua Heng Mun.
- rr. Agent Wood located the above pictured transaction (STEP # 7), and observed the funds, 10,000 USDT enter Mun's Binance account on August 6th, 2022 at 0718 hours. Approximately five (5) hours after the funds entered Mun's account, Mun completed a withdrawal transaction. The transaction occurred on August 6th, 2022 at 1204 hours, and consisted of 23,999.20 USDT being sent to wallet address TWLy3aGGkRck2uoZenQQPVi7AapyTVNebC. This amount, 23,999.20, included Lawter's stolen funds, approximately 10,000 USDT and was the first outgoing transfer once the initial 10,000 USDT was received.
- ss. Based on Agent Wood's training and experience, he concluded that the actions Mun's account completed were indicative of an account involved in fraud schemes and money laundering. Mun's account, and the transactions prior, made attempts to disguise the original source of funds, which was acquired through false pretenses. Mun's account had a consistent pattern of the above described

movement of funds which is common among fraud suspects. Mun's account used a money laundering technique known as "chain hopping."

- tt. In this case, Mun's account received the already swapped USDT (from Ethereum) which had also been co-mingled, as described above. The initial fraud proceeds were transacted on the Ethereum blockchain. Mun's account then transferred to the USDT to a TRON wallet address hosted on the TRON blockchain.
- uu. Of the thirteen (13) transactions that Tony Lawter completed, two (2) transactions were traced and found to have ultimately been co-mingled and sent to Yicai Luo's Binance account. A 3<sup>rd</sup> transaction Toney Lawter completed was traced and found to have been ultimately sent to Lua Heng Mun's Binance account.

**GROUNDS FOR FORFEITURE**

**COUNT ONE**  
**ILLEGAL FELONY INSTRUMENTALITY**

- 7. The Petitioner adopts and re-alleges paragraphs 1 through 6 and further alleges:
- 8. THE CONTRABAND PROPERTY is money, securities, negotiable instrument, or currency, which was used or was attempted to be used as an instrumentality in the commission of, or in aiding or abetting in the commission of one or more of the following illegal felonies:
  - a. Knowingly obtaining or using, or endeavoring to obtain or to use, the property of another with intent to, either temporarily or permanently deprive the other person of a right to the property or a benefit from the property; or appropriating property to his or her own use or to the use of any person not entitled to the use of the property – said property having a value of \$750.00 or more in violation of section 812.014, Fla. Stat.;
  - b. Engaging in a scheme to defraud through a systematic, ongoing course of conduct with the intent to defraud one or more person, or with intent to obtain property from one or more persons by false or fraudulent pretenses, representation, or promises or willful misrepresentation of a future act in violation of section 817.034, Fla. Stat.;

c. Receiving any proceeds derived, directly or indirectly from a pattern of racketeering activity or acquiring or maintaining, directly or indirectly any interest in or control of any enterprise; or being employed by or associated with, any enterprise to conduct or participate directly or indirectly, in such enterprise through a pattern of racketeering activity; or conspiring or endeavoring to violate any of the above in violation of section 895.03, Fla. Stat.;

d. Knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, to conduct or to attempt to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity with the intent to promote the carrying on of the specified unlawful activity; or knowing that the transaction or transportation is designed in whole or in part to conceal or disguise the nature, location, source, ownership or control of the proceeds of specified unlawful activity in violation of section 896.101, Fla. Stat.; and/or

e. Agreeing, conspiring, combining, or confederating to commit any of the above felonies in violation of section 777.04(3), Fla. Stat.

COUNT TWO  
PROCEEDS OBTAINED AS A RESULT OF A VIOLATION OF  
THE FLORIDA CONTRABAND FORFEITURE ACT

9. The Petitioner adopts and re-alleges paragraphs 1 through 6 and further alleges:

10. THE CONTRABAND PROPERTY is personal property acquired by proceeds obtained as a result of a violation of The Florida Contraband Forfeiture Act.

11. It is a violation of Fla. Stat. § 895.03 to receive any proceeds directly or indirectly, from a pattern of racketeering activity, with criminal intent. A pattern of racketeering activity means engaging in at least two incidents of racketeering conduct that have the same or similar intents, results, accomplices, victims, or methods of commission or that otherwise are interrelated by distinguishing characteristics and are not isolated incidents. Racketeering activity means to commit, to attempt to commit, to conspire to commit, or to solicit, coerce, or intimidate another person to commit any crime chargeable under Chapter 812 relating to theft and related crimes; Chapter 817 relating to fraudulent

practices, false pretenses, fraud generally; or Chapter 896 relating to offenses related to financial transactions.

12. Furthermore, the Defendant Property represents the proceeds of Grand Theft in violation of Fla. Stat. § 812.014; Scheme to Defraud in violation of Fla. Stat. § 817.034; and Money Laundering in violation of Fla. Stat. § 896.101. As such, the Defendant Property is forfeitable pursuant to The Florida Contraband Forfeiture Act.

BASIS FOR FORFEITURE AS TO ALL COUNTS

13. The Petitioner adopts and re-alleges paragraphs 1 through 12 and further alleges:

14. THE CONTRABAND PROPERTY is a contraband article as defined in section 932.701(2)(a), Florida Statutes and subject to forfeiture pursuant to The Florida Contraband Forfeiture Act because under section 932.702, it is unlawful:

- a) To transport, carry, or convey any contraband article in, upon, or by means of any vessel, motor vehicle, or aircraft;
- b) To conceal or possess any contraband article;
- c) To use any vessel, motor vehicle, aircraft, other personal property, or real property to facilitate the transportation, carriage, conveyance, concealment, receipt, possession, purchase, sale, barter, exchange, or giving away of any contraband article;
- d) To conceal, or possess, or use any contraband article as an instrumentality in the commission of or in aiding or abetting in the commission of any felony or violation of the Florida Contraband Forfeiture Act; or
- e) To acquire personal property by the use of proceeds obtained in violation of the Florida Contraband Forfeiture Act.

15. Thus, THE CONTRABAND PROPERTY is forfeitable to the Brevard County Sheriff's Office in that, any contraband article, vessel, motor vehicle, aircraft, other personal property, or real property used in violation of any provision of the Florida Contraband Forfeiture Act, or in, upon, or by means of which any violation of the Florida Contraband Forfeiture Act has

taken or is taking place, may be seized and shall be forfeited subject to the provisions of the Florida Contraband Forfeiture Act pursuant to section 932.703(1)(a), Florida Statutes.

16. To the extent the Defendant Property includes funds that did not originate as proceeds from the illegal activities discussed herein, those funds were comingled with and used to conceal and disguise the nature, location, source, ownership or control of the criminal proceeds, or were involved in a conspiracy to launder such proceeds and are therefore subject to forfeiture under the Florida Contraband Forfeiture Act.

#### SUBSTITUTED ASSETS

17. Further, Petitioner requests that pursuant to Section 932.703(6), Fla. Stat., this Court order the forfeiture of any other property of any claimant, up to the value of any property subject to forfeiture if any of the contraband property described in this Petition, or otherwise shown to exist during the course of this action:

- (a) Cannot be located;
- (b) Has been transferred to, sold to, or deposited with, a third party;
- (c) Has been placed beyond the jurisdiction of the court;
- (d) Has been substantially diminished in value by any act or omission of the person in possession of the property; or
- (e) Has been comingled with any property which cannot be divided without difficulty.

#### **PETITIONER'S COMPLIANCE WITH FLORIDA STATUTES SECTIONS 932.701, 932.703, AND 932.704**

18. A Verified Affidavit in Support of this Forfeiture Action signed by Agent Justin Wood is attached and incorporated as Petitioner's **Exhibit "A"**.
19. The Petitioner has complied with section 932.703(3)(a), Florida Statutes by mailing to all persons entitled to notice within five working (5) days after the seizure, notice of the seizure and notice of the right to an adversarial preliminary hearing and notice that said person(s) may request an adversarial preliminary hearing within fifteen (15) days after receiving such



notice. Notice(s) of Seizure for Forfeiture are attached and incorporated as Petitioner's Composite **Exhibit "B."**

20. The Petitioner has complied with section 932.703(2)(a), Florida Statutes, by applying for and obtaining the attached Ex-Parte Order Finding Probable Cause for Seizure. The Order Finding Probable Cause is attached hereto as Petitioner's Composite **Exhibit "C."**

21. The Petitioner has promptly proceeded against THE CONTRABAND PROPERTY by filing the initial Verified Complaint/Petition for Judgment of Forfeiture within forty-five (45) days of the seizure as mandated by section 932.704(4), Florida Statutes.

WHEREFORE, Petitioner requests this Court, pursuant to The Florida Contraband Forfeiture Act, issue a judgment of forfeiture and order THE CONTRABAND PROPERTY forfeited to the Brevard County Sheriff's Office subject to the provisions of The Florida Contraband Forfeiture Act, for its use or disposal according to law, and all right, title, and interest in THE CONTRABAND PROPERTY, relating back to the date of seizure, be perfected in the Brevard County Sheriff's Office.

Dated: December 2, 2022.

**BREVARD COUNTY SHERIFF'S OFFICE**  
340 Gus Hipp Blvd.  
Rockledge, FL 32955

***/s/ Laura Moody*** \_\_\_\_\_

Laura Moody, Esq.  
Chief Legal Counsel  
Florida Bar No. 0041676  
Telephone (321) 633-8499  
Facsimile (321) 633-8415  
Laura.moody@bcsso.us  
*Attorney for Petitioner*

**IN THE CIRCUIT COURT OF THE EIGHTEENTH JUDICIAL CIRCUIT  
IN AND FOR BREVARD COUNTY, FLORIDA**

**IN RE—FORFEITURE OF:**

**CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE WALLET(S)  
NUMBER UID 153035005 TO WIT:**

<b>USDT</b>	<b>TetherUS</b>	<b>238830.7437</b>
<b>CAKE</b>	<b>PancakeSwap</b>	<b>14771.75682</b>
<b>ETH</b>	<b>Ethereum</b>	<b>27.73634179</b>
<b>BNB</b>	<b>BNB</b>	<b>89.69501919</b>
<b>SFP</b>	<b>SafePal</b>	<b>60060.07842</b>
<b>BTC</b>	<b>Bitcoin</b>	<b>1.0000034</b>
<b>UNI</b>	<b>Uniswap</b>	<b>2749.764169</b>
<b>ADA</b>	<b>Cardano</b>	<b>38740.48277</b>
<b>DOGE</b>	<b>Dogecoin</b>	<b>140031.784</b>
<b>DOT</b>	<b>Polkadot</b>	<b>960.8127723</b>
<b>ETHW</b>	<b>Ethereum PoW</b>	<b>27.73634179</b>
<b>AAVE</b>	<b>Aave</b>	<b>2.184973</b>
<b>LUNC</b>	<b>Terra Classic</b>	<b>0.00079</b>

**CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE WALLET(S)  
NUMBER UID 198318266 TO WIT:**

<b>USDT</b>	<b>TetherUS</b>	<b>2000.2</b>
<b>USDT</b>	<b>TetherUS</b>	<b>295.5257</b>

**AFFIDAVIT**

**STATE OF FLORIDA  
COUNTY OF BREVARD**

BEFORE ME personally appeared **Agent Justin Wood** of the Brevard County Sheriff’s Office (“BCSO”), who first being duly sworn, deposes and says: The facts tending to establish the grounds for this application and the probable cause of Affiant believing that such facts exist are as follows:

On August 1st, 2022, **Tony Lawter** (Victim) of 4509 Ponds Drive, Cocoa, Brevard County, Florida reported that he fell victim to an investment scam involving cryptocurrency.

**Tony Lawter** met an individual through social media (Facebook) and started a romantic relationship. During the relationship, the individual convinced **Tony Lawter** to invest in cryptocurrency through “Pearcoin”, a fake cryptocurrency trading application, unknown to **Tony Lawter** at the time. **Agent Justin Wood** completed a tracing analysis of **Tony Lawter’s** outgoing transactions and discovered that in two (2) of the transactions **Tony Lawter** completed, the final destination was a wallet address associated with an account at Binance. A third (3<sup>rd</sup>) transaction **Tony Lawter** completed was analyzed and determined to have been received by a wallet address associated with a second account at Binance. The other transactions **Tony Lawter** completed were traced to exchanges outside of the United States and have consistently not complied with United States based law enforcement.

**Agent Justin Wood** contacted Binance and requested account information for the wallet addresses associated with the suspect Binance accounts. **Agent Justin Wood** discovered the first (1st) Binance account was owned by **Yicai Luo**, a male from China and the second (2<sup>nd</sup>) Binance account was owned by **Lua Heng Mun**, a male from Malaysia. Tony Lawter believed he was investing in his romantic relationship and did not indicate he was ever conducting business with any persons from China or Malaysia.

On October 21<sup>st</sup>, 2022, **Agent Justin Wood** obtained a Search and Seizure Warrant for **Yicai Luo's** Binance account (Account # [REDACTED]) and a Search and Seizure Warrant for **Lua Heng Mun's** Binance account (Account # [REDACTED]), which was served to Binance on the same day.

**THE FACTS** which established the grounds for the application and the probable cause of **Agent Justin Wood's** search warrant and overall investigation and seizure for forfeiture are as follows:

On August 1<sup>st</sup>, 2022, Toney Lawter (Victim) of 4509 Ponds Drive, Cocoa, Brevard County, Florida reported that he fell victim to an investment scam involving cryptocurrency.

Lawter reported the following, in summary: In April of 2022, Lawter received a Facebook message from a female named "Bunny". The conversation turned romantic and the two (2) established an online relationship. During the relationship, Bunny offered Mr. Lawter a way to make money through cryptocurrency so they can afford to buy a farm and live together one day.

The fraud scheme Tony Lawter fell victim to has recently been identified as a "pig butchering" scheme. This type of fraud typically starts on social media or an online dating platform. After the suspect's trust has been gained by the victim, a romantic relationship is developed. During the relationship, the victim is convinced to invest in cryptocurrency. The investment opportunity commonly promises unrealistic gains. The victim is provided credentials to log in to the "investment platform" and see the exponential growth in their account. The investment platform commonly consists of a fake website or application. Once the victim attempts to withdrawal funds from the investment account they are required to pay fees and taxes before their funds are released. Pig butchering scams have been identified as originating from Southeast Asia and predominately executed by a ring of cryptocurrency scammers.

Lawter was instructed to download Crypto.com, a cryptocurrency exchange platform, on his cell phone and establish an account. Lawter wired funds from his bank to his Crypto.com account and purchased Ethereum. After the Ethereum was purchased he was instructed to transfer the funds to a wallet address associated with an "investment platform". From June 15<sup>th</sup>, 2022 to July 27<sup>th</sup>, 2022, Lawter completed thirteen (13) withdrawal transactions from his Crypto.com account. Lawter believed he was investing through "Pearcoin," and had downloaded the application through the Google Play Store. He was provided log in credentials and was able to see his account balance and profits. Lawter watched his investments grow rapidly through Pearcoin. When Lawter went to withdrawal his funds, he was told he must pay the taxes up front or he would risk a 3% deduction each day he didn't pay. At this point, Lawter realized he was involved in a scam and subsequently contacted the Brevard County Sheriff's Office to report the incident. Lawter was unable to transfer, withdrawal, or access any of his funds through the investment platform.

On August 8<sup>th</sup>, 2022, Agent Justin Wood completed and sent a subpoena to Crypto.com to the State Attorney's Office for review. The purpose of the subpoena was to obtain information on Lawter's Crypto.com account and identify every withdrawal transaction he completed that was linked to the

investment scam.

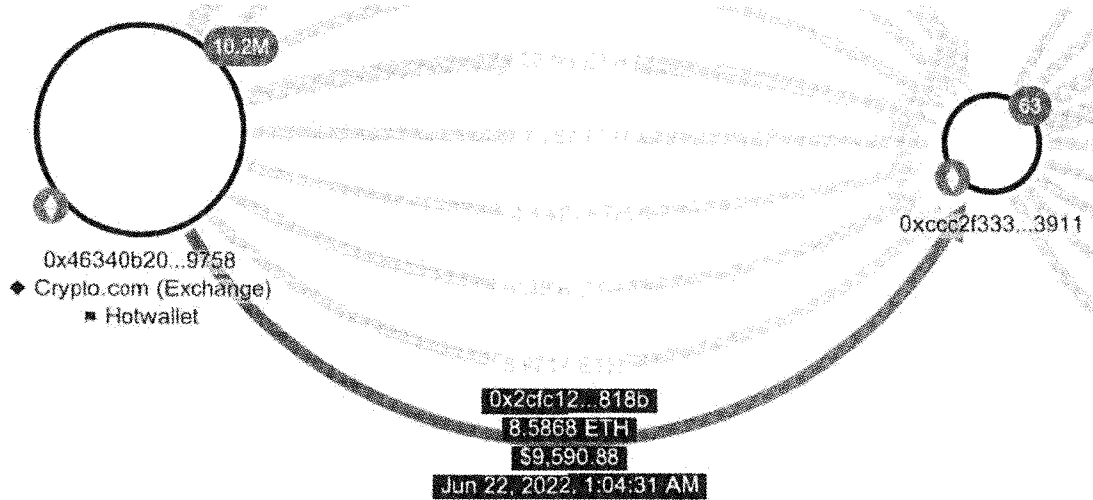
On August 23<sup>rd</sup>, 2022, Crypto.com responded to the subpoena request and supplied account information for Lawter’s Crypto.com account. Through the information provided by Crypto.com, Agent Justin Wood located thirteen (13) withdrawal transaction from Lawter’s account. The thirteen (13) withdrawals totaled over 132 Ethereum (valued at \$177,502.39 at the time of the subpoena response). Of the thirteen (13) withdrawal transactions, Agent Justin Wood identified observed twelve (12) of the transactions went to a single Ethereum wallet address, 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. Of the twelve (12) transactions, nine (9) withdrawal transactions were greater than four (4) Ethereum. Agent Justin Wood focused on the nine (9) transactions which contained a greater amount and accounted for almost all of Lawter’s funds.

Agent Justin Wood began to utilize the Ethereum blockchain to trace the Ethereum that Lawter had sent to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911, in which he believed he was investing in cryptocurrency. Agent Justin Wood determined that once Lawter sent Ethereum to 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911, that wallet address utilized an Ethereum smart contract to convert the received Ethereum into Tether (USDT), which is a stable coin pegged to the United States Dollar (USD).

One transaction in particular was initiated on June 22<sup>nd</sup>, 2022 at 12:59 AM UTC. The transaction included Lawter’s Crypto.com account which sent approximately 8.590725 Ethereum (ETH) to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. (See Step # 1 below)

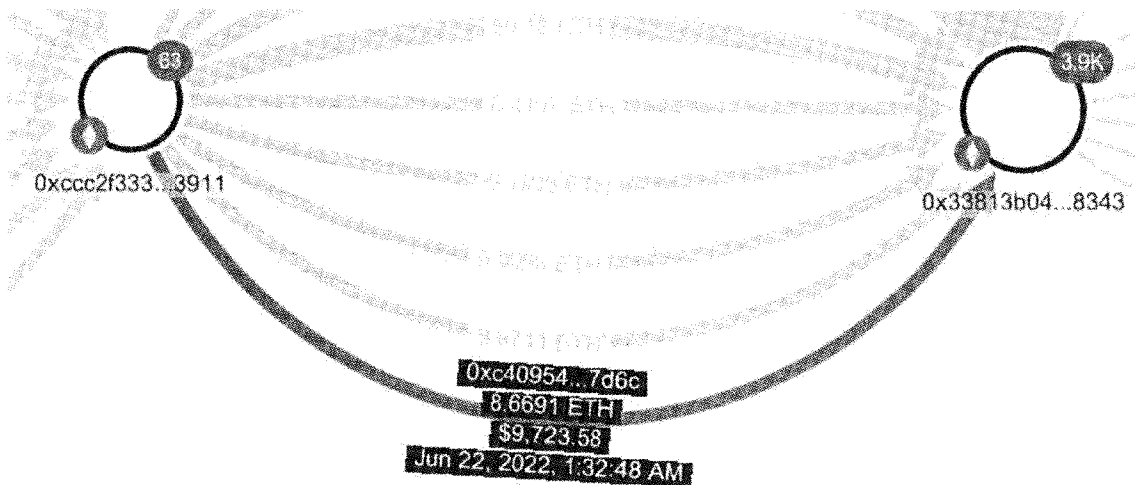
**TRANSACTION # 1**

**STEP #1**



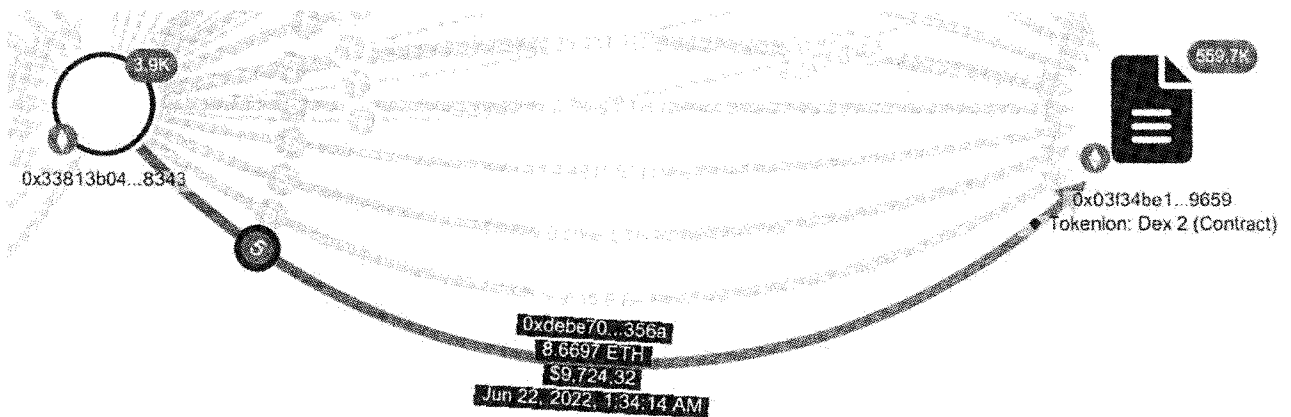
After wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911 received the funds, ~8.5868 ETH, the funds were then sent to wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. This transaction occurred on June 22<sup>nd</sup>, 2022 at 1:32 AM. (See Step # 2 below)

**STEP # 2**



After wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received the funds, ~8.6691 ETH, the wallet address then used a smart contract to convert the ETH to USDT. This transaction occurred on June 22<sup>nd</sup>, 2022 at 1:34 AM. (See Step # 3 below)

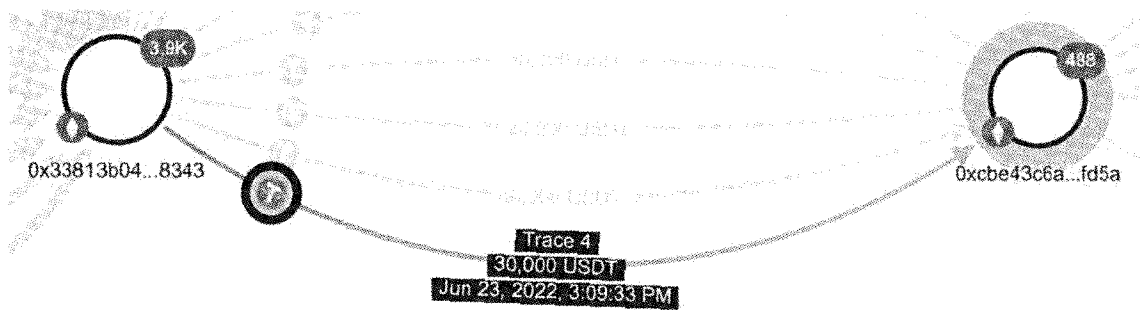
**STEP # 3**



As a result of the ETH to USDT conversion, wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received approximately 9,728.28 USDT. The transaction HASH, or HASH ID, for the conversion was 0xdebe70ded5f9ccca4d3984454fa6a98af593d92436190d6951412737d361356a. A HASH ID is a unique string of letters and numbers assigned to each transaction which is posted to the Ethereum blockchain.

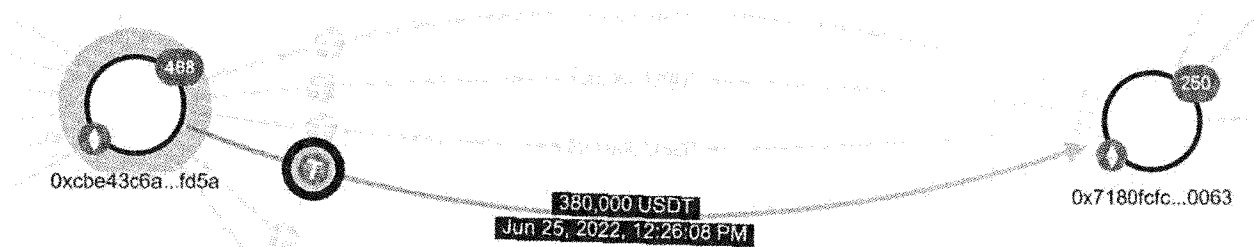
After the funds, 9,728.28 USDT, were received by wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343, the funds were then sent to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a. This transaction occurred on July 23<sup>rd</sup>, 2022 at 3:09 PM. It should be noted Lawter's funds, 9,728.28 USDT, were co-mingled with additional funds from unknown sources. Wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 sent Lawter's funds, and co-mingled funds, to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a, which totaled 30,000 USDT. (See Step # 4 below)

**STEP # 4**



After wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 30,000 USD, the funds were then transferred. On June 25<sup>th</sup>, 2022 at 12:26 PM wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a sent 380,000 USD to wallet address 0x7180fcfc7b7913948920b84387579daf97530063. The transfer included co-mingled funds from wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. (See Step # 5 below)

**STEP # 5**



After wallet address 0x7180fcfc7b7913948920b84387579daf97530063 received the funds, 380,000 USD, the funds were then transferred. On July 13<sup>th</sup>, 2022 at 6:55 AM wallet address 0x7180fcfc7b7913948920b84387579daf97530063 sent 615,686 USD to wallet address 0x8459dd488c507b20331e0f6ac481f75ee9f4ae97. The transfer included co-mingled funds from wallet address 0x7180fcfc7b7913948920b84387579daf97530063. (See Step # 6 below)

**STEP # 6**



Through cryptocurrency tracing tools, your Affiant identified wallet address 0x8459dd488c507b20331e0f6ac481f75ee9f4ae97 as being associated with an account at Binance, a cryptocurrency exchange. The account number associated with the wallet address is 153035005

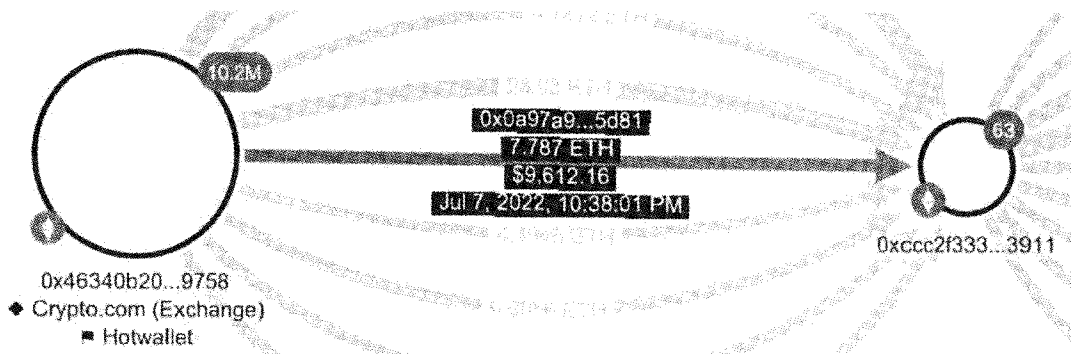
2022-270411

which is registered to Yicai Luo.

**TRANSACTION # 2**

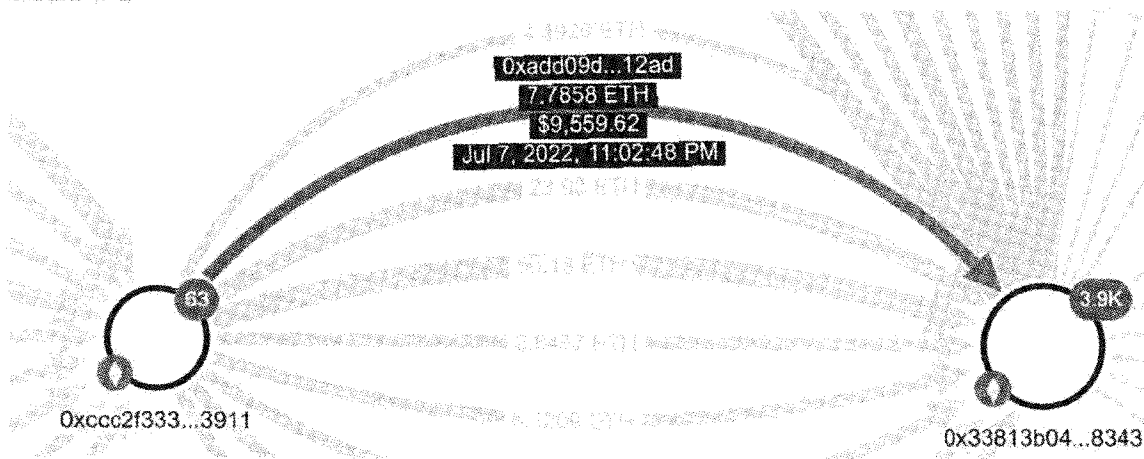
The second transaction in question occurred on July 7<sup>th</sup>, 2022 at 10:37 PM. The transaction included Lawter's Crypto.com account which sent approximately 7.790992027 Ethereum (ETH) to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. (See Step # 1 below)

**STEP # 1**



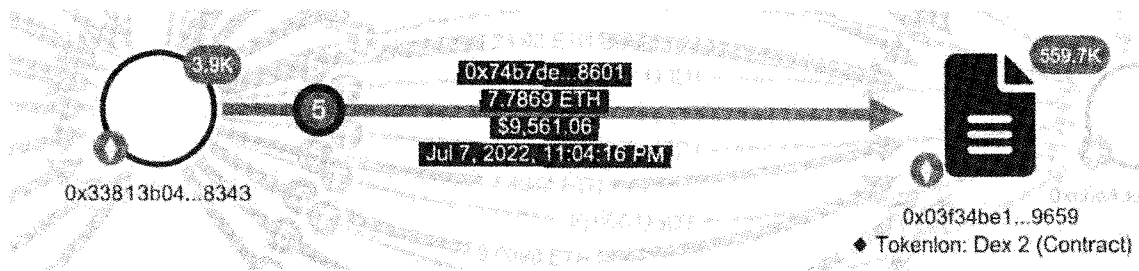
After wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911 received the funds, ~7.787 ETH, the funds were then sent to wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. This transaction occurred on July 7<sup>th</sup>, 2022 at 11:02 PM. (See Step # 2 below)

**STEP # 2**



After wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received the funds, ~7.7858 ETH, the wallet address then used a smart contract to convert the ETH to USDT. This transaction occurred on July 7<sup>th</sup>, 2022 at approximately 11:04 PM. (See Step # 3 below)

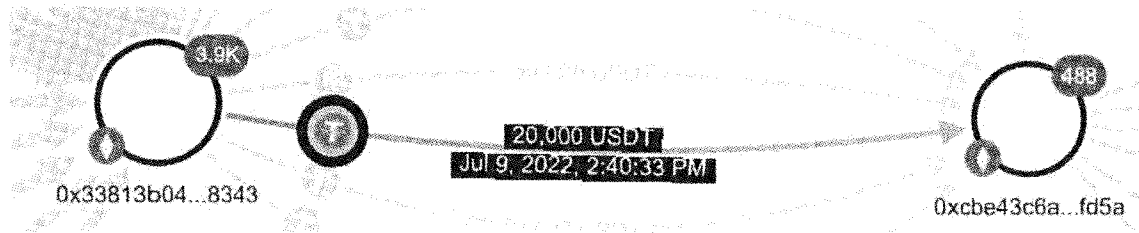
**STEP # 3**



As a result of the ETH to USDT conversion, wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received approximately 9,575.95 USDT. The transaction HASH, or HASH ID, for the conversion was 0x74b7ded0efe4e9cf569febca9bc91cd683f35a695b81f5c11058b24f4f98601. A HASH ID is a unique string of letters and numbers assigned to each transaction which is posted to the Ethereum blockchain.

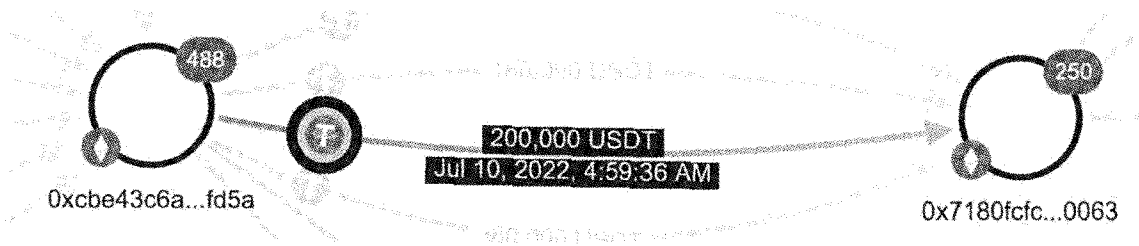
After the funds, 9,575.95 USDT, were received by wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343, the funds were then sent to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a. This transaction occurred on July 9<sup>th</sup>, 2022 at 2:40 PM. It should be noted Lawter’s funds, 9,575.95 USDT, were co-mingled with additional funds from unknown sources. Wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 sent Lawter’s funds, and co-mingled funds, to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a, which totaled 20,000 USDT. (See Step # 4 below)

**STEP # 4**



After wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 20,000 USDT, the funds were then transferred. On July 10<sup>th</sup>, 2022 at 4:59 AM wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a sent 200,000 USDT to wallet address 0x7180fcfc7b7913948920b84387579daf97530063. The transfer included co-mingled funds from wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. (See Step # 5 below)



**STEP # 5**

After wallet address `0x7180fcfc7b7913948920b84387579daf97530063` received the funds, 200,000 USDT, the funds were then transferred. On July 13<sup>th</sup>, 2022 at 6:55 AM wallet address `0x7180fcfc7b7913948920b84387579daf97530063` sent 615,686 USDT to wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97`. The transfer included co-mingled funds from wallet address `0x7180fcfc7b7913948920b84387579daf97530063`. (See Step # 6 below)

**STEP # 6**

Through cryptocurrency tracing tools, your Affiant identified wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97` as being associated with an account at Binance, a cryptocurrency exchange. Wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97` was the same wallet address that received funds from “**TRANSACTION #1**” described above.

On October 18<sup>th</sup>, 2022, your Affiant contacted Binance and requested account information for the Binance account associated with wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97`.

On October 19<sup>th</sup>, 2022, your Affiant received a response from Binance, who provided account information for the account number [REDACTED] associated with wallet address `0x8459dd488c507b20331e0f6ac481f75ee9f4ae97`. The account owner was identified **Yicai Luo**, a male from the Republic of China.

Your Affiant located the above pictured transactions (**TRANSACTION #1: STEP # 6** and **TRANSACTION # 2: STEP # 6**), and observed the funds, 615,686 USDT enter Luo’s Binance account on July 13<sup>th</sup>, 2022 at 6:56 AM. Approximately twenty-four (24) minutes after the funds entered Luo’s account, Luo completed a withdrawal transaction. The transaction was on July 13<sup>th</sup>, 2022 at 7:20 AM, and consisted of 1,399,996 USDT being sent to wallet address `0x5453fd1ef17c8c4F2042b07416573c3eCa19D247`.

Your Affiant used open source Ethereum blockchain to continue to trace the funds. Once wallet address `0x5453fd1ef17c8c4F2042b07416573c3eCa19D247` received the funds on July 13<sup>th</sup>, 2022 at 7:21 AM, the funds were immediately transferred to wallet address

2022-270411

0x3d1d8a1d418220fd53c18744d44c182c46f47468. This outgoing transaction, for 1,399,996 USDT, occurred on July 13<sup>th</sup>, 2022 at 7:27 AM

Using open sources, your Affiant determined wallet address 0x3d1d8a1d418220fd53c18744d44c182c46f47468 was a Bitkub hot wallet. Bitkub is a cryptocurrency exchange based out of Thailand. In your Affiant's experience, cryptocurrency exchange companies based outside of the United States do not comply with United States based law enforcement and do not accept state issued subpoenas or search and seizure warrants.

Based on your Affiant's training and experience, your Affiant concluded that the actions Luo's account completed were indicative of an account involved in fraud schemes and money laundering. Luo's account, and the transactions prior, were attempts to disguise the original source of funds, which was acquired through false pretenses. Luo's account had a consistent pattern of the above described movement of funds which is common among fraud suspects. Luo's account, once it received USDT had completed one hundred and sixteen (116) transaction, totaling approximately 54,387,177 USDT, between January 14<sup>th</sup>, 2022 and August 29<sup>th</sup>, 2022. The quick and rapid movement of fraudulently obtained funds to an exchange based outside of the United States, in an effort to avoid account seizure is common practice of those involved in the money laundering of cryptocurrency assets.

Luo's account also had another consistent pattern used to launder money. The technique known as "chain hopping" and has been identified as one of the fastest-growing money laundering typologies. This layering technique consist of converting one form of cryptocurrency to another and moving the funds from one blockchain to another. In this case, Luo's account had a pattern of receiving USDT and transferring the funds to a TRON, another type of cryptocurrency, wallet address hosted on the TRON blockchain. The technique is common among fraudsters and its purpose served to disguise source of funds and make tracing the stolen funds more difficult for law enforcement. Luo's account completed ninety-nine (99) withdrawal transaction to various TRON wallet addresses which were hosted on the TRON blockchain between June 20<sup>th</sup>, 2021 and 29<sup>th</sup>, 2022. These ninety-nine (99) transactions totaled approximately 19,116,832.80 USDT.

On October 21<sup>st</sup>, 2022, Agent Justin Wood Search and Seizure Warrant for Yicai Luo's Binance account. The warrant and application were reviewed and approved by the Honorable Judge Aaron Peacock of the Eighteenth Judicial Circuit of Brevard County, Florida. The warrant was served to Binance on the same day.

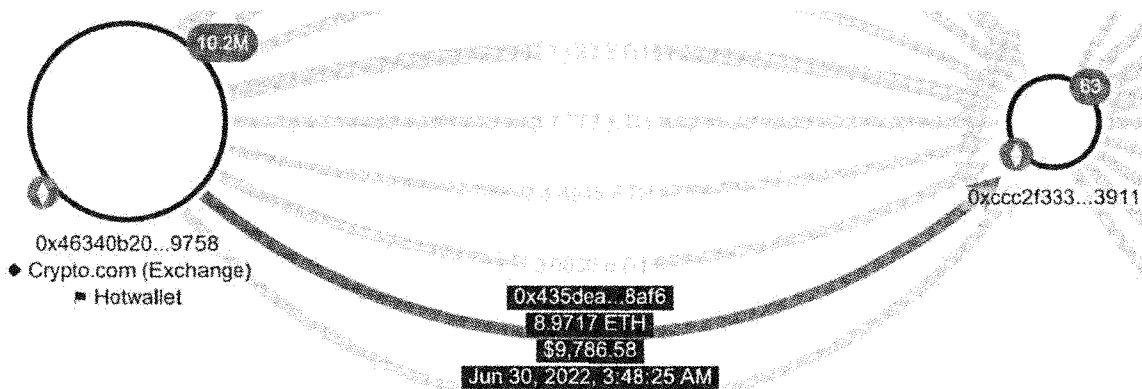
On October 25<sup>th</sup>, 2022, Binance alerted Agent Justin Wood that the REACT Task Force, based out of California, had been working an investigation and had interest in Yicai Luo's Binance account. Agent Justin Wood made contact with Sergeant Brad Smith of the Milpitas Police Department and Task Force Officer of the REACT Task Force to deconflict. While the investigation did not meet the jurisdictional limitations of the REACT Task Force, Sgt. Smith provided information on an individual in Los Angeles, California who had fallen victim to a "pig butchering" scheme. Sgt. Smith, provided Agent Justin Wood with a Los Angeles Police Department Investigative Report filed on August 23<sup>rd</sup>, 2022. The victim, Tai Feng Tang, reported she had been romantically involved with an individual through social media. During the relationship, she was convinced to invest in cryptocurrency. Ms. Tang reported a loss of approximately \$300,000.00. Sgt. Smith provided his trace analysis which showed Ms. Tang had completed four (4) USDT (Tether) transactions to what she believed was an investment platform. One of the transactions Sgt. Smith provided showed part of Tang's funds (approximately 81,696 USDT) were traced and ultimately transferred to Yicai Luo's Binance account. (See Attached **Exhibit A** for additional

2022-270411

case details.)

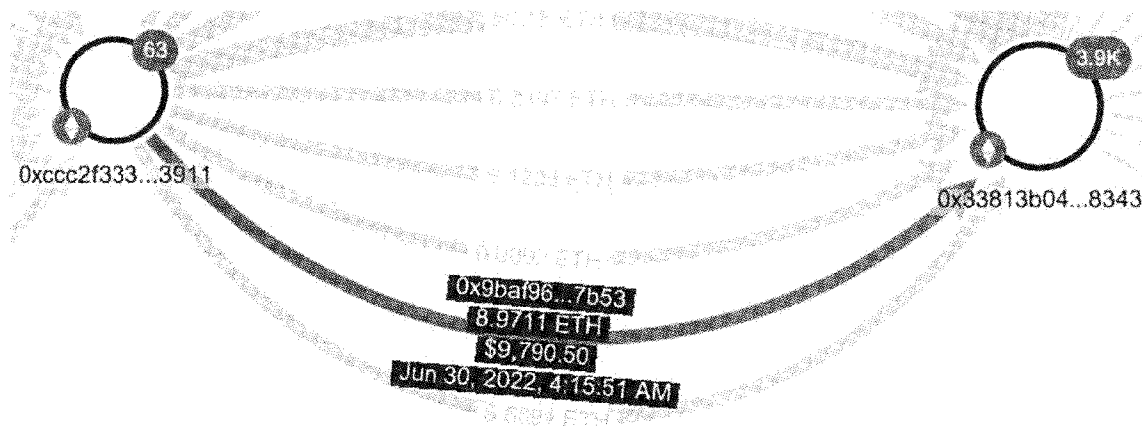
Agent Justin Wood conducted a trace analysis on a third (3<sup>rd</sup>) transaction Tony Lawter completed on June 30<sup>th</sup>, 2022 at 0348 hours. The transaction included Lawter's Crypto.com account, which sent 8.975636 Ethereum (ETH) to wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911. (See Step # 1 below)

### STEP #1



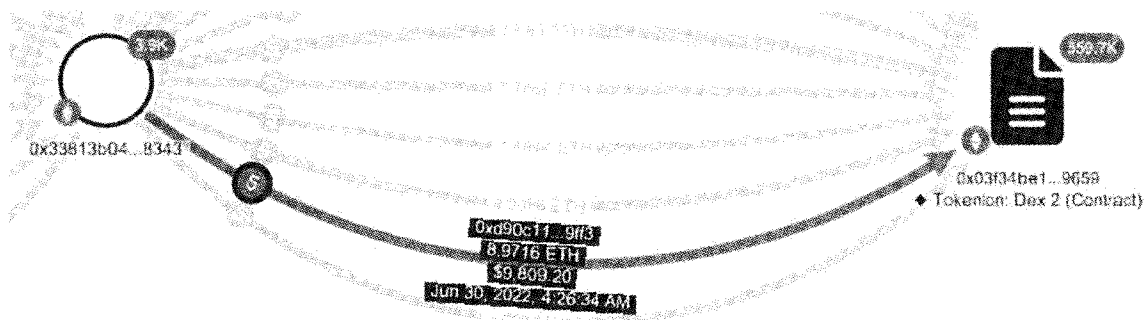
After wallet address 0xccc2f333e57cb739a3a62ed1e7a76ee17d3c3911 received the funds, ~8.97 ETH, the funds were then sent to wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343. This transaction occurred on June 30<sup>th</sup>, 2022 at 0415 hours. (See Step # 2 below)

### STEP # 2



After wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received the funds, ~8.97 ETH, the wallet address then used a smart contract to convert the ETH to USDT. This transaction occurred on June 30<sup>th</sup>, 2022 at 0426 hours. (See Step # 3 below)

**STEP # 3**

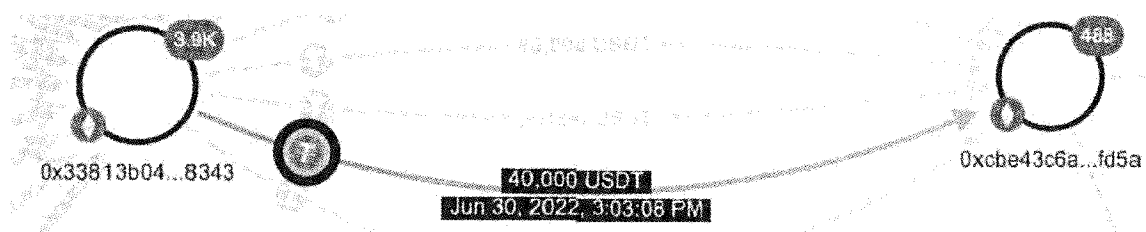


As a result of the ETH to USDT conversion, wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 received 9,796.84 USDT. The transaction HASH, or HASH ID, for the conversion was 0xd90c1137c4d0f2163f3c859ad6977d7b205713c4bbc6f2907c1e92b636929ff3. A HASH ID is a unique string of letters and numbers assigned to each transaction which is posted to the Ethereum blockchain.

After the funds, ~9,796.84 USDT, were received by wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343, the funds were then sent to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a. This transaction occurred on June 30<sup>th</sup>, 2022 at 1503 hours. It should be noted Lawter’s funds, ~9,796.84 USDT, were co-mingled with additional funds from unknown sources. Wallet address 0x33813b04ca9dab0a2f41ae2c1a617d946e708343 sent Lawter’s funds, and co-mingled funds, to wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a, which totaled 40,000 USDT.

(See Step # 4 below)

**STEP # 4**



After wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 40,000 USDT, the funds were then transferred. On July 2<sup>nd</sup>, 2022 at 0211 hours wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a sent 65,443 USDT to wallet address 0x346ef244464679b031750f70d750b3fa65165443. It should be noted the outgoing transfer was the next transaction posted after wallet address 0xcbe43c6ad3b4c1700dfd47904467158949b0fd5a received the 40,000 USDT. (See Step # 5 below)

2022-270411

**STEP # 5**



After wallet address 0x346ef244464679b031750f70d750b3fa65165443 received the funds, 65,443 USDT, part of the funds were then transferred to wallet address 0x1970118296c32923c1039a775ac6fb90dfec2419. The transaction occurred on July 11<sup>th</sup>, 2022 at 0951 hours. (See Step # 6 below)

**STEP # 6**

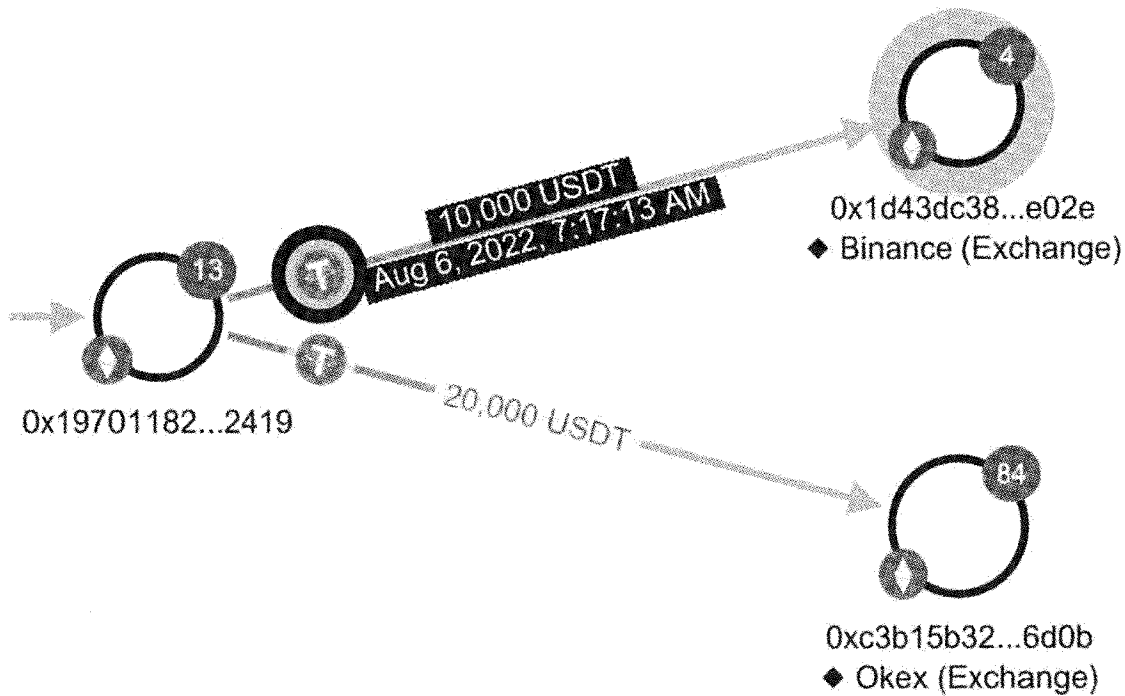


After wallet address 0x1970118296c32923c1039a775ac6fb90dfec2419 received the funds, 30,000 USDT, the funds were then sent to two (2) different wallet addresses via two (2) separate transactions. The transactions were as follows:

- 1) August 2<sup>nd</sup>, 2022 at 0442 hours for 20,000 USDT to wallet address 0xc3b15b326c0ed1576f918a3b36c9de789f936d0b
- 2) August 6<sup>th</sup>, 2022 at 0717 hours for 10,000 USDT to wallet address 0x1d43dc389993cb3818724e0d06746bbaa6a9e02e

(See Step # 7 below)

STEP # 7



Through cryptocurrency tracing tools, your Affiant identified wallet address `0xc3b15b326c0ed1576f918a3b36c9de789f936d0b` as being associated with an account at Okex, a cryptocurrency exchange. Based on prior investigations, your Affiant was aware the Okex exchange does not cooperate with United States based law enforcement.

Through cryptocurrency tracing tools, your Affiant identified wallet address `0x1d43dc389993cb3818724e0d06746bbaa6a9e02e` as being associated with an account at Binance, a cryptocurrency exchange.

On October 18<sup>th</sup>, 2022, your Affiant contacted Binance and requested account information for the Binance account associated with wallet address `0x1d43dc389993cb3818724e0d06746bbaa6a9e02e`.

On October 19<sup>th</sup>, 2022, your Affiant received a response from Binance, who provided account information for the account number [REDACTED] associated with wallet address `0x1d43dc389993cb3818724e0d06746bbaa6a9e02e`. The account owner was identified **Lua Heng Mun**, a male from Malaysia.

Your Affiant located the above pictured transaction (STEP # 7), and observed the funds, 10,000 USDT enter Mun’s Binance account on August 6<sup>th</sup>, 2022 at 0718 hours. Approximately five (5) hours after the funds entered Mun’s account, Mun completed a withdrawal transaction. The transaction was on August 6<sup>th</sup>, 2022 at 1204 hours, and consisted of 23,999.20 USDT being sent to wallet address `TWLy3aGGkRck2uoZenQQPVi7AapyTVNebC`. This amount, 23,999.20, included Lawter’s stolen funds, approximately 10,000 USDT and was the first outgoing transfer once the initial 10,000 USDT was received.

Based on your Affiant’s training and experience, your Affiant concluded that the actions Mun’s account completed were indicative of an account involved in fraud schemes and money laundering. Mun’s

account, and the transactions prior, made attempts to disguise the original source of funds, which was acquired through false pretenses. Mun's account had a consistent pattern of the above described movement of funds which is common among fraud suspects. Mun's account used a money laundering technique known as "chain hopping". Chain hopping has been identified as one of the fastest-growing money laundering typologies. This layering technique consist of converting one form of cryptocurrency to another and moving the funds from one blockchain to another. In this case, Mun's account received the already swapped USDT (from Ethereum) which had also been co-mingled, as described above. The initial fraud proceeds were transacted on the Ethereum blockchain. Mun's account then transferred to the USDT to a TRON, another type of cryptocurrency, wallet address hosted on the TRON blockchain. The technique is common among fraudsters and its purpose served to disguise source of funds and make tracing the stolen funds more difficult for law enforcement.

In summary, Tony Lawter, a Brevard County resident, filed a report with the Brevard County Sheriff's Office on August 1<sup>st</sup>, 2022. Lawter had reported that he fell victim to a romantic investment scam which resulted in the loss of approximately \$177,502.29. Lawter completed thirteen (13) cryptocurrency transactions on the Ethereum blockchain after being instructed to create a Crypto.com account. A majority of the funds were sent to Ethereum wallet address 0xcce2f333e57cb739a3a62ed1e7a76ee17d3c3911. Using open source tools, your Affiant traced Lawter's funds to several different wallet addresses which were utilized to facilitate the investment fraud. Agent Justin Wood identified two (2) separate wallet address associated with two (2) separate Binance accounts, which ultimately received part of Tony Lawter's fraudulently obtained funds. Agent Justin Wood contacted Binance and discovered one (1) account was owned by Yicai Luo, a male from the Republic of China and the second (2<sup>nd</sup>) account was owned by Lua Heng Mun, a male from Malaysia. Agent Justin Wood discovered that Luo's account quickly transferred Lawter's funds, which had been co-mingled during the process, to an exchange based outside of the United States. Agent Justin Wood discovered that Mun's account quickly transferred Lawter's funds to a TRON wallet address. Based on your Affiant's training and experience, both Binance accounts owned by Luo and Mun had patterns indicative of a scheme to defraud and money laundering, including an individual attempting to conceal or disguise the source of funds, and making additional efforts to avoid the funds from being linked or a beneficiary of known fraud.

**Your Affiant**, Agent Justin Wood (hereinafter referred to as Your Affiant) is a sworn Law Enforcement Officer employed by the Brevard County Sheriff's Office and has been employed as such since 2012. Your Affiant is currently a Law Enforcement Officer certified by the Florida Police Standards Board and has been a certified Law Enforcement Officer in the state of Florida since 2012. Your Affiant is currently assigned as an Agent with the Brevard County Sheriff's Office Criminal Investigative Division. Your Affiant has made well over 100 felony arrests. Your Affiant has attended Florida Department of Law Enforcement.

Your Affiant seized the said property based on the following facts:

- **Yicai Luo's** Binance account and **Lua Heng Mun's** Binance account received and currently contain co-mingled fraudulently obtained funds which derived from a "pig butchering" scheme.
- Pig butchering schemes originated in Southeast Asia and are predominately executed by a ring of cryptocurrency scammers. The scam incorporates a romance scam, building a long-term communication relationship with the victim, typically using social media or dating applications.

Once the trust of the victim is gained, the suspect(s) propose an investment opportunity using cryptocurrency and fraudulent or fake cryptocurrency investment platforms.

- Of the thirteen (13) transactions the victim, **Tony Lawter** completed, two (2) transactions were traced and found to have ultimately been co-mingled and sent to **Yicai Luo's** Binance account. A 3<sup>rd</sup> transaction Toney Lawter completed was traced and found to have been ultimately sent to **Lua Heng Mun's** Binance account.
- **Yicai Luo's** Binance account and **Lua Heng Mun's** Binance account had a pattern of receiving funds that had been fraudulently obtained and co-mingled. Each account made efforts to further disguise the source of funds.
- The pattern observed in **Yicai Luo's** account consisted of 116 transactions in which **Yicai Luo's** Binance account received USDT (approximately 54,387,117.99 USDT) between January 14<sup>th</sup>, 2022 and August 29<sup>th</sup>, 2022. The funds, once received were quickly transferred, and usually co-mingled, to other wallet addresses associated with international exchanges.
- **Yicai Luo's** account also completed ninety-nine (99) withdrawal transactions to various TRON wallet addresses from June 20<sup>th</sup>, 2021 to June 29<sup>th</sup>, 2022 totaling 19,116,832.80 USDT. This method of withdrawal is part of a money laundering technique called "chain hopping".
- **Lua Heng Mun's** Binance account had a pattern of receiving USDT from various TRON wallet addresses. Once received, **Lua Heng Mun's** account transferred the USDT to other various TRON wallet address, often shortly after receiving the funds.
- From October 11<sup>th</sup>, 2021 to October 17<sup>th</sup>, 2022, **Lua Heng Mun's** Binance account received fifty-eight (58) deposits totaling approximately 607,206.39 USDT. From within the same time frame, **Lua Heng Mun's** Binance account completed forty (40) withdrawal transactions totaling 356,206.91 USDT. **Lua Heng Mun's** Binance account showed a Binance Pay card made thirty-six (36) C2C (Customer to Customer) transactions totaling 238,031 USDT. The actions observed on **Lua Heng Mun's** account were indicative of an individual using various techniques to launder funds.
- Chain hopping has been identified as one of the fastest-growing money laundering typologies. This layering technique consist of converting one form of cryptocurrency to another and moving the funds from one blockchain to another. **Yicai Luo and Lua Heng Mun's** Binance accounts, on multiple occasions, received funds (USDT) that were once in the form of Ethereum, hosted on the Ethereum blockchain. Once received, **both Yucal Luo and Lua Heng Mun's** accounts had a pattern of transferring USDT to various TRON wallet addresses, hosted on the TRON network. This money laundering technique is commonly used by scammers to obfuscate fraudulently obtained funds and disguise the origin or source of funds.



2022-270411

Seized as evidence and confiscated under authority of the Florida Contraband forfeiture Act, 932.701-932.7062:

**CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE WALLET(S) NUMBER UID 153035005 REGISTERED TO "YICAI LUO" TO WIT:**

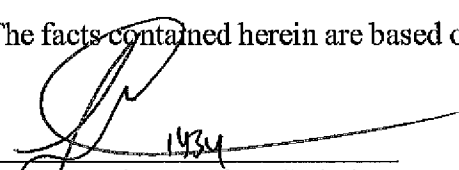
<b>USDT</b>	<b>TetherUS</b>	<b>238830.7437</b>
<b>CAKE</b>	<b>PancakeSwap</b>	<b>14771.75682</b>
<b>ETH</b>	<b>Ethereum</b>	<b>27.73634179</b>
<b>BNB</b>	<b>BNB</b>	<b>89.69501919</b>
<b>SFP</b>	<b>SafePal</b>	<b>60060.07842</b>
<b>BTC</b>	<b>Bitcoin</b>	<b>1.0000034</b>
<b>UNI</b>	<b>Uniswap</b>	<b>2749.764169</b>
<b>ADA</b>	<b>Cardano</b>	<b>38740.48277</b>
<b>DOGE</b>	<b>Dogecoin</b>	<b>140031.784</b>
<b>DOT</b>	<b>Polkadot</b>	<b>960.8127723</b>
<b>ETHW</b>	<b>Ethereum PoW</b>	<b>27.73634179</b>
<b>AAVE</b>	<b>Aave</b>	<b>2.184973</b>
<b>LUNC</b>	<b>Terra Classic</b>	<b>0.00079</b>

**CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE WALLET(S) NUMBER UID 198318266 REGISTERED TO "LUA HENG MUN" TO WIT:**

<b>USDT</b>	<b>TetherUS</b>	<b>2000.2</b>
<b>USDT</b>	<b>TetherUS</b>	<b>295.5257</b>

The above-described funds are believed to be proceeds of fraud, specifically identified as a pig butchering scheme with the involvement of money laundering.

The facts contained herein are based on personal knowledge of the investigation and are true and correct.

  
Agent Justin Wood ID #1434

Sworn to (or affirmed) and subscribed before me this 4<sup>th</sup> day of November, 2022, by Agent Justin Wood ID #1434, who is personally known to me.

  
Notary Signature

**BREVARD COUNTY SHERIFF'S OFFICE**



**NOTICE OF SEIZURE OF CRYPTOCURRENCY FOR FORFEITURE**

TO: YICAI LUO VIA th863982668\_mobileuser@binance.com

**YOU ARE HEREBY NOTIFIED, PURSUANT TO THE FLORIDA CONTRABAND FORFEITURE ACT, FLORIDA STATUTES § 932.701-932.7062, THAT THE BELOW DESCRIBED PROPERTY HAS BEEN SEIZED BY LAW ENFORCEMENT OFFICERS OF THE BREVARD COUNTY SHERIFF'S OFFICE AND IS BEING HELD IN A WALLET ESTABLISHED BY AND AT 700 SOUTH PARK AVENUE, TITUSVILLE, FL 32780 PENDING CIVIL FORFEITURE ACTION:**

**Cryptocurrency Binance Wallet Address containing the following balance and coinage on 10/27/2022:**

UID 153035005 Estimate Total Balance (BTC) 22.85586635 ≈ \$471522.00838085

Currency	Currency Code	Total Balance
USDT	TetherUS	238830.7437
CAKE	PancakeSwap	14771.75682
ETH	Ethereum	27.73634179
BNB	BNB	89.69501919
SFP	SafePal	60060.07842
BTC	Bitcoin	1.0000034
UNI	Uniswap	2749.764169
ADA	Cardano	38740.48277
DOGE	Dogecoin	140031.784
DOT	Polkadot	960.8127723
ETHW	Ethereum PoW	27.73634179
AAVE	Aave	2.184973
LUNC	Terra Classic	0.00079

ALL PERSONS WHO HAVE AN INTEREST IN THE SUBJECT PROPERTY MAY REQUEST AN ADVERSARIAL PRELIMINARY HEARING IN THE CIRCUIT COURT OF THE EIGHTEENTH CIRCUIT, BREVARD COUNTY, WITHIN FIFTEEN (15) DAYS OF RECEIPT OF THIS NOTICE TO DETERMINE WHETHER PROBABLE CAUSE EXISTS THAT THE PROPERTY HAS BEEN, IS BEING, OR IS INTENDED TO BE USED IN VIOLATION OF THE FLORIDA CONTRABAND FORFEITURE ACT. PURSUANT TO FLA. STAT. § 932.703(3)(a), THE REQUEST FOR AN ADVERSARIAL PRELIMINARY HEARING SHALL BE MADE IN WRITING BY CERTIFIED MAIL, RETURN RECEIPT REQUESTED, AND DIRECTED TO COUNSEL FOR THE BREVARD COUNTY SHERIFF'S OFFICE: **LAURA MOODY, ESQ. and GEORGE C. GASPARD, ESQ., 340 GUS HIPPI BLVD., ROCKLEDGE, FL 32955.** A COURT HEARING WILL BE SET WITHIN TEN (10) DAYS AFTER YOUR REQUEST IS RECEIVED OR AS SOON AS PRACTICABLE THEREAFTER. FAILURE TO REQUEST AN ADVERSARIAL PRELIMINARY HEARING WITHIN THE TIME CONTEMPLATED BY THIS NOTICE WILL RESULT IN THE WAIVER OF YOUR ENTITLEMENT TO AN ADVERSARIAL PRELIMINARY HEARING, HOWEVER YOU MAY STILL HAVE THE RIGHT TO CONTEST THE FORFEITURE ACTION AT A LATER DATE. IT IS ANTICIPATED THAT A COMPLAINT, PURSUANT TO FLA. STAT. § 932.701, ET. SEQ., WILL BE FILED IN THE CIRCUIT COURT OF THE EIGHTEENTH JUDICIAL CIRCUIT IN AND FOR BREVARD COUNTY, FLORIDA, WITHIN FORTY-FIVE (45) DAYS OF THE DATE OF SEIZURE.

Dated this 27<sup>th</sup> day of OCTOBER, 2022

\_\_\_\_\_  
(Asset Interest Claimant Signature)  
YICAI LUO

Th863982668\_mobileuser@binance.com

Agent J. Ward #1434 / ECU  
(Seizing Deputy Signature / ID# / Unit)  
Brevard County Sheriff's Office  
Attn: SIU Administrative Assistant  
340 Gus Hipp Boulevard  
Rockledge, Florida 32955



**NOTICE OF SEIZURE OF CRYPTOCURRENCY FOR FORFEITURE**

TO: LUA HENG MUN VIA mun163t@gmail.com

**YOU ARE HEREBY NOTIFIED, PURSUANT TO THE FLORIDA CONTRABAND FORFEITURE ACT, FLORIDA STATUTES § 932.701-932.7062, THAT THE BELOW DESCRIBED PROPERTY HAS BEEN SEIZED BY LAW ENFORCEMENT OFFICERS OF THE BREVARD COUNTY SHERIFF'S OFFICE AND IS BEING HELD IN A WALLET ESTABLISHED BY AND AT 700 SOUTH PARK AVENUE, TITUSVILLE, FL 32780 PENDING CIVIL FORFEITURE ACTION:**

**Cryptocurrency Binance Wallet Address containing the following balance and coinage on 10/27/2022:**

UID 198318266

Estimate Total Balance(BTC)

0.11127382

≈ \$2295.66913492

Currency	Currency Code	Total Balance
USDT	TetherUS	2000.2
USDT	TetherUS	295.5257

ALL PERSONS WHO HAVE AN INTEREST IN THE SUBJECT PROPERTY MAY REQUEST AN ADVERSARIAL PRELIMINARY HEARING IN THE CIRCUIT COURT OF THE EIGHTEENTH CIRCUIT, BREVARD COUNTY, WITHIN FIFTEEN (15) DAYS OF RECEIPT OF THIS NOTICE TO DETERMINE WHETHER PROBABLE CAUSE EXISTS THAT THE PROPERTY HAS BEEN, IS BEING, OR IS INTENDED TO BE USED IN VIOLATION OF THE FLORIDA CONTRABAND FORFEITURE ACT. PURSUANT TO FLA. STAT. § 932.703(3)(a), THE REQUEST FOR AN ADVERSARIAL PRELIMINARY HEARING SHALL BE MADE IN WRITING BY CERTIFIED MAIL, RETURN RECEIPT REQUESTED, AND DIRECTED TO COUNSEL FOR THE BREVARD COUNTY SHERIFF'S OFFICE: **LAURA MOODY, ESQ. and GEORGE C. GASPARD, ESQ., 340 GUS HIPPI BLVD., ROCKLEDGE, FL 32955.** A COURT HEARING WILL BE SET WITHIN TEN (10) DAYS AFTER YOUR REQUEST IS RECEIVED OR AS SOON AS PRACTICABLE THEREAFTER. FAILURE TO REQUEST AN ADVERSARIAL PRELIMINARY HEARING WITHIN THE TIME CONTEMPLATED BY THIS NOTICE WILL RESULT IN THE WAIVER OF YOUR ENTITLEMENT TO AN ADVERSARIAL PRELIMINARY HEARING, HOWEVER YOU MAY STILL HAVE THE RIGHT TO CONTEST THE FORFEITURE ACTION AT A LATER DATE. IT IS ANTICIPATED THAT A COMPLAINT, PURSUANT TO FLA. STAT. § 932.701, ET. SEQ., WILL BE FILED IN THE CIRCUIT COURT OF THE EIGHTEENTH JUDICIAL CIRCUIT IN AND FOR BREVARD COUNTY, FLORIDA, WITHIN FORTY-FIVE (45) DAYS OF THE DATE OF SEIZURE.

Dated this 27<sup>TH</sup> day of OCTOBER, 2022

(Asset Interest Claimant Signature)  
LUA HENG MUN

mun163t@gmail.com

(Address/Telephone Number)

*Agent T. Wood #1104/ECU* *11434*  
(Seizing Deputy Signature / ID# / Unit)  
Brevard County Sheriff's Office  
Attn: SIU Administrative Assistant  
340 Gus Hipp Boulevard  
Rockledge, Florida 32955

RE: Case Report No: 2022-270411

**IN THE CIRCUIT COURT OF THE EIGHTEENTH JUDICIAL CIRCUIT  
IN AND FOR BREVARD COUNTY, FLORIDA**

**CIVIL FORFEITURE**

Agency Case No: 2022-00270411

**IN RE: FORFEITURE OF:**

**CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE  
WALLET(S) NUMBER UID 153035005 REGISTERED TO "YICAI LUO" TO WIT:**

<b>USDT</b>	<b>TetherUS</b>	<b>238830.7437</b>
<b>CAKE</b>	<b>PancakeSwap</b>	<b>14771.75682</b>
<b>ETH</b>	<b>Ethereum</b>	<b>27.73634179</b>
<b>BNB</b>	<b>BNB</b>	<b>89.69501919</b>
<b>SFP</b>	<b>SafePal</b>	<b>60060.07842</b>
<b>BTC</b>	<b>Bitcoin</b>	<b>1.0000034</b>
<b>UNI</b>	<b>Uniswap</b>	<b>2749.764169</b>
<b>ADA</b>	<b>Cardano</b>	<b>38740.48277</b>
<b>DOGE</b>	<b>Dogecoin</b>	<b>140031.784</b>
<b>DOT</b>	<b>Polkadot</b>	<b>960.8127723</b>
<b>ETHW</b>	<b>Ethereum PoW</b>	<b>27.73634179</b>
<b>AAVE</b>	<b>Aave</b>	<b>2.184973</b>
<b>LUNC</b>	<b>Terra Classic</b>	<b>0.00079</b>

**CRYPTOCURRENCIES WITHIN BINANCE HOLDING LTD. D.B.A. BINANCE  
WALLET(S) NUMBER UID 198318266 REGISTERED TO "LUA HENG MUN" TO  
WIT:**

<b>USDT</b>	<b>TetherUS</b>	<b>2000.2</b>
<b>USDT</b>	<b>TetherUS</b>	<b>295.5257</b>

**Defendant Property.**

**EX-PARTE ORDER FINDING PROBABLE CAUSE FOR SEIZURE**

THIS MATTER having come before this Court pursuant to section 932.703(2), Florida Statutes, within ten (10) business days of seizure of the above-described property by the Application of the BREVARD COUNTY SHERIFF'S OFFICE and the Court having reviewed the sworn affidavit of Agent Justin Wood, ID #1434, finds:

1. The seizing agency applied for the probable cause determination within ten (10) business days of the date of the seizure.

2. The requirements specified in paragraph (1)(a) of section 932.703, Florida Statutes, have been satisfied based on the fact that one or more of the following facts exist as indicated below:

A.  The owner of the property was arrested for a criminal offense that forms the basis for determining that the property is a contraband article under section 932.701, Florida Statutes; and/or

**B. EXCEPTION TO OWNER OF PROPERTY ARREST REQUIREMENT EXISTS AS INDICATED:**

Regardless of whether an arrest of the owner of the property was or was not made, the owner of the property cannot be identified after a diligent search or the person in possession of the property denies ownership and the owner of the property cannot be identified by means that were available to the employee or agent of the seizing agency at the time of the seizure;

Regardless of whether an arrest of the owner of the property was or was not made the owner is a fugitive from justice or is deceased;

Regardless of whether an arrest of the owner of the property was or was not made, an individual who does not own the property was arrested for a criminal offense that forms the basis for determining that the property is a contraband article under section 932.701, Florida Statutes, and the owner of the property had actual knowledge of the criminal activity;

Regardless of whether an arrest of the owner of the property was or was not made, the owner of the property agrees to be a confidential informant as defined in section 914.28, Florida Statutes;  
or

Regardless of whether an arrest of the owner of the property was or was not made the property is a monetary instrument.

3. Probable cause exists to seize the above-described property under the Florida Contraband Forfeiture Act.

**THEREFORE, THE COURT HAVING FOUND THAT THE REQUIREMENTS OF FLORIDA STATUTE SECTION 932.703(1)(A) WERE SATISFIED AND THAT PROBABLE CAUSE EXISTS FOR THE SEIZURE, IT IS ORDERED AND ADJUDGED AS FOLLOWS:**

1. The Court authorizes continued seizure of the subject contraband property by the seizing law enforcement agency or an agency or agent on their behalf, pending a determination of title to the property upon the Filing of a Complaint for Forfeiture and pursuant to the procedures defined in the Florida Contraband Forfeiture Act.

2. Pursuant to section 943.704(5)(c), Florida Statutes, any claimant who desires to contest the forfeiture action upon the Filing of a Complaint for Forfeiture by or on behalf of the seizing agency shall file and serve upon the attorney representing the seizing agency any responsive pleadings and affirmative defenses. Therefore, upon the filing of a Civil Complaint for Forfeiture, the seizing Agency shall serve a Certified Copy of the Complaint along with a copy of this Order Finding Probable Cause upon all claimants.

3. Claimants are Notified upon service of this Order and a Complaint for Final Order of Forfeiture of the following: **THAT AS A CLAIMANT OR POTENTIAL CLAIMANT WHO CLAIMS AN INTEREST IN THE SEIZED PROPERTY, YOU HAVE TWENTY (20) DAYS FROM SERVICE OF A COPY OF THE COMPLAINT FOR FORFEITURE AND A COPY OF THIS ORDER FINDING PROBABLE CAUSE, TO FILE IN THIS COURT, ANY RESPONSIVE PLEADING, ANSWER, AND/OR AFFIRMATIVE DEFENSES TO THE COMPLAINT FOR FORFEITURE. SAID PLEADINGS SHALL INCLUDE A SHORT AND PLAIN STATEMENT DEMONSTRATING A VALID PROPERTY INTEREST IN THAT**

WHICH IS CLAIMED, SUFFICIENT TO CONFER STANDING TO APPEAR IN THIS CAUSE.

4. YOU ARE FURTHER COMMANDED TO SERVE A COPY OF SUCH ANSWER OR RESPONSIVE PLEADING WITHIN SAID TIME PERIOD UPON THE ATTORNEY WHO FILED THE COMPLAINT FOR FORFEITURE. FAILURE TO FILE AND SERVE SUCH ANSWER OR PLEADING WITHIN SAID TIME PERIOD SHALL RESULT IN THE ENTRY OF A DEFAULT PURSUANT TO FLORIDA RULE OF CIVIL PROCEDURE 1.500(a), AND A FINAL ORDER OF FORFEITURE.

5. The seizing Agency as described herein is ordered to restrain the seized property by the least restrictive means to protect against disposal, waste, or continued illegal use of such property, pending disposition of the property pursuant to the Florida Contraband Forfeiture Act.

**DONE AND ORDERED** in Chambers at the Harry T. and Harriette V. Moore Justice Center, Viera, Brevard County, Florida, on the 11/4/2022 day of November, 2022.

*David Dugan*  
11/4/2022 1:01:50 PM  
\_\_\_\_\_  
David DUGAN  
Circuit Judge

Copies to:

Laura Moody, Chief Legal Counsel, Brevard County Sheriff's Office via [laura.moody@bcso.us](mailto:laura.moody@bcso.us)

Potential Claimants: Yicai Luo [th863982668\\_mobileuser@binance.com](mailto:th863982668_mobileuser@binance.com) and  
Lua Heng Mun [mun163t@gmail.com](mailto:mun163t@gmail.com)