DECLARATION OF SPECIAL AGENT ANDREW S. JONES

1. I am a Special Agent with the Internal Revenue Service – Criminal Investigation, and have been since December 2022. As a Special Agent, my responsibilities include the investigation of criminal violations of the Internal Revenue Code, the Money Laundering Control Act, the Bank Secrecy Act, and related offenses. I earned a Bachelor of Science in Business Administration and Accounting in 2009 and a Master of Accounting in 2010 from The University of Tennessee at Knoxville. I am a Certified Public Accountant, licensed in the state of Virginia. I worked full-time for the accounting and professional services firm Ernst & Young Global Limited for approximately six years as a consultant and auditor. I also served clients as a consultant sole proprietor offering my accounting and linguistic skills for two years. I was a special agent for the United States Secret Service for approximately three years and three months prior to being employed by the Internal Revenue Service – Criminal Investigation. I completed training at the National Criminal Investigation Training Academy at the Federal Law Enforcement Training Center in Glynco, Georgia. I completed the Criminal Investigator Training Program in December 2019, and the IRS Special Agent Basic Training Program, conducted by the IRS's National Criminal Investigation Training Academy, in April 2023. I completed U.S. Secret Service new agent training in Beltsville, Maryland in September 2020. I received training in conducting financial investigations that involve analyzing books and records of individuals and businesses, such as journals, ledgers, bank accounts, invoices, receipts, and other records evidencing violations of the Internal Revenue Code and other financial crimes. I also received extensive training on laws regarding search and seizure and the execution of search warrants. I am currently assigned to the Cyber Crimes Unit in IRS-CI, and I have received training in cyber operations and in criminal schemes perpetrated via the internet.

2. The facts and information contained in this declaration are based upon my personal observations as well as information from other agents and officers. All observations not personally made by me were relayed to me by the individuals who made them or they were conveyed to me by my review of records, documents, and other evidence obtained during the course of this investigation.

3. This declaration contains information necessary to support a civil complaint for forfeiture in rem of 6.65777556 bitcoin, 423,309.65874752 First Digital USD, 38,797.45285688 TetherUS, and 63,806 The Graph custodied at Binance under User ID 83699030 and email address sedwardjr[@]gmail[.]com ("the Defendant Property"). In total, as of February 19, 2025, the Defendant Property were valued at approximately $1,071,810.43 . I submit that the Defendant Property is property that constitutes proceeds traceable to violations of 18 U.S.C. §§ 1343 and/or 1960, and/or involved in money laundering in violation of 18 U.S.C. § 1957, and therefore is subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), (C), and/or (D).

BACKGROUND CONCERNING VIRTUAL CURRENCIES AND DIGITAL ASSETS

4. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. In contrast to fiat currencies, such as the U.S. dollar, virtual currencies are not issued by any government or bank but are instead generated and controlled through computer software. Bitcoin ("BTC") is the best-known virtual currency in use. Digital assets are a broader category of digital tokens that include virtual currencies but also encompass assets that do not act as currencies—such as "NFTs" (so-called non-fungible tokens, which may purport to prove a property interest in a digital work) or "governance tokens" (digital tokens that allows a bearer to vote on a particular online platform).

5. Virtual currency addresses are the specific virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters. Each virtual currency address is controlled

through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

6. Many virtual currencies publicly record their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred using that blockchain's specific technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

7. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. A user of virtual currency can use multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

8. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

9. USDT (also known as Tether) is a cryptocurrency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is represented to be backed by one U.S. dollar in Tether's reserves, making it what is known as a "stablecoin." USDT is issued by Tether Ltd. USDT is hosted on the Ethereum and Tron blockchains, among others.

10. USDC is a cryptocurrency that resides on multiple blockchains. The value of USDC is tied to the value of the U.S. dollar; therefore, one unit of USDC is represented to be backed by

one U.S. dollar in Circle's reserves, making it what is known as a "stablecoin." USDC is issued by Circle Internet Group, Inc. USDC is hosted on the Ethereum blockchains, among others.

11. First Digital USD ("FDUSD") is a cryptocurrency that resides on multiple blockchains. The value of FDUSD is tied to the value of the U.S. dollar; therefore, one unit of FDUSD is represented to be backed by one U.S. dollar in First Digital's reserves, making it what is known as a "stablecoin." FDUSD is issued by FD121 Limited, a subsidiary of Hong Kong-headquartered financial firm First Digital Limited. FDUSD is hosted on multiple blockchains, including Ethereum and BNB Smart Chain (formerly Binance Smart Chain (BSC)). BNB Smart Chain provides smart contract functionality for Binance.

12. Binance USD (BUSD) is a cryptocurrency that resides on Binance's blockchain network, BNB Smart Chain. The value of BUSD is tied to the value of the U.S. dollar; therefore, one unit of BUSD is represented to be backed by one U.S. dollar in Paxos' reserves, making it what is known as a "stablecoin." BUSD is issued by Paxos Trust Company in partnership with Binance.

13. Bitcoin ("BTC") is a cryptocurrency hosted on the Bitcoin network, the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. Transactions involving BTC are publicly recorded on the Bitcoin blockchain, which allows anyone to track the movement of BTC.

14. Ether ("ETH") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH. The transaction fees associated with ETH transactions and other cryptocurrencies on the Ethereum blockchain are called, "gas."

15. The Graph ("GRT") is an indexing protocol for organizing and accessing data from blockchains and storage networks. The Graph Network is a decentralized data market powered by distributed participants. GRT was developed by The Graph Foundation.

16. Filecoin ("FIL") is a cryptocurrency intended to be a blockchain. It is an open-source cloud storage marketplace and protocol. FIL was developed by the Filecoin Foundation.

BACKGROUND ON CRYPTOCURRENCY INVESTMENT FRAUD

17. I know from my training and experience that investment fraud sometimes involves criminals duping victims into investing money into fraudulent projects, including doing so by making false representations about high yields. A common investment fraud associated with cryptocurrencies is called "pig butchering." Pig butchering scams involve fraudsters gaining the trust of victims, oftentimes via a fictitious romantic relationship, and duping them into making investments into fake cryptocurrency projects. These schemes sometimes begin with a victim receiving an unsolicited message on social media, with the conversation eventually appearing to turn romantic. This can be accomplished by a scammer "spoofing" a social media account associated with a famous person by using slight variations on a legitimate username (i.e. @J0hn_Doe vs. @John_Doe) to fool victims into thinking fake accounts are authentic. The victim will then be convinced to begin transferring money to an alleged cryptocurrency investment opportunity recommended by the scammer. The scammer will eventually highlight seemingly impressive monetary gains from initial investments and encourage the victim to invest increasingly larger amounts. Often, when the victim attempts to withdraw funds from the investment, the scammer purports that the victim must pay more money to the fake project for the purposes of complying with required, "fees," tax-related dues, or other fictious pretenses, ultimately resulting in financial ruin to the victim.

INITIAL INVESTIGATION AND VICTIM INTERVIEW

18. In approximately June 2023, the IRSCI became aware of suspicious activity conducted at Binance by User ID 83699030 through the communications of a Binance.com Internal

Investigations Senior Cryptocurrency Investigator to IRSCI. Binance had already placed a withdrawal restriction on funds held by User ID 83699030 as part of its investigation into the suspicious activity prior to contacting IRSCI. VICTIM 1, an individual located in Madison Heights, Virginia, who initiated transfers of funds of Ethereum that ended in the Binance account held by User ID 83699030, contacted Binance in approximately May 2023 claiming to be a victim of organized scammers whom he had previously believed to be genuine. VICTIM 1 claimed to have transferred more than $1,500,000 of cryptocurrency to addresses associated with the scammers.

19. On February 18, 2025, and May 7, 2025, IRSCI Special Agents Andrew Jones and Andrew Hippler interviewed VICTIM 1 via Microsoft Teams video conferences. VICTIM 1's counsel was also present for the interviews. SA Jones had previously communicated with VICTIM 1 in 2023 and 2024 regarding the IRSCI investigation, and in 2024 and 2025 with VICTIM 1's counsel regarding the investigation and to arrange the February 18, 2025, and May 7, 2025 interviews.

20. During the February 18, 2025 interview, VICTIM 1 told investigators that in 2021 and 2022, he received a loan for approximately $500,000 from the United States government agency, the Small Business Administration (SBA), used the funds to pay off business-related loans, and subsequently sold some of the businesses that he owned. He sold three businesses for approximately $1 million, including convenience stores. VICTIM 1 estimated that he invested approximately $1,547,800 in the investment scheme, Coinance US ("Coinance"). When investigators requested an accounting of funds that were invested into the investment scheme, VICTIM 1 provided a list on approximately July 3, 2025, which included $140,000 of SBA loan funds, and funds related to, "Employee Retention Credit," and, "F941 Employee Credit in

COVID," among other line items. The VICTIM 1-provided accounting of funds invested into the investment scheme is listed here with an investigator-calculated total at bottom:

Description	**Amount**
Sale of convenience store called Best Bet Mini Mart (including inventory)	$480,000
COVID-19 SBA loan amount left over after paying off loans	$140,000
Employee Retention Credit	$66,000
Employee Retention Credit 2	$37,000
Surrendered TradePMR investment in stock and bonds	$150,000
F941 Employee Credit in COVID	$145,000
Sold property at 316 Ragland Rd house	$80,000
Sold 2200 Memorial Ave house	$53,000
Refinanced 275 Ragland Roadhouse	$40,000
Refinanced 168 Mays St house	$80,000
Sold 320 Munford Ave and 886 Brook St homes	$120,000
Cash on hand in personal and business accounts	$200,000
Borrowed from daughter and friend as personal loans	$150,000
Total put in scheme (as calculated by investigators):	**$1,741,000**

21. In approximately July 2025, investigators obtained from SBA an Economic Injury Disaster Loan (EIDL) LoanPay Calculator for Loan 3958259102, titled S.S. SATYA AND PURNIMA CORPORATION with a Process Date of 5/2/2022 and Effective Date of 5/3/2022, indicating a loan principal amount of $500,000.

22. VICTIM 1 confirmed that he converted US Dollars in his personal and business bank accounts into cryptocurrency, which included opening personal accounts at Coinbase and Crypto.com with the intent of investing to generate return on investment during the last 6 months of 2022. VICTIM 1 was looking for ways to generate larger returns with cryptocurrency when he found Coinanceus[.]com, which claimed he could get larger returns. VICTIM 1 did not realize it was a scam. The platform was initially called Coinance[.]com, and later changed to Coinanceus[.]com. VICTIM 1 found Coinance through the social media platform Twitter (now called X) where users were discussing investments. A user spoofing the cryptocurrency social media influencer, Tiffany Fong, using the Twitter handle [@]Tlffany_Fong ("the unidentified scammer(s)"), communicated with VICTIM 1. VICTIM 1 was familiar with the real Tiffany Fong and believed that the user communicating with him was Tiffany Fong. After initially communicating with VICTIM 1 via social media, the unidentified scammer(s) began using WhatsApp to communicate with VICTIM 1. In the WhatsApp communications, the unidentified scammer(s) instructed VICTIM 1 to open an account on the Coinance platform, and to send a copy of his identification. VICTIM 1 was also instructed via WhatsApp to send cryptocurrency to certain wallet addresses to make investments in Coinance, typically in Ethereum. VICTIM 1's initial investment was approximately 4,900 USDC, in or approximately June of 2022, made from his Coinbase account. Within the investment platform, VICTIM 1 was able to view the price of common cryptocurrency assets, his investment balance and watch the investment grow, allegedly. The initial investment appeared to have grown to $7,000 or $8,000 in value within approximately two weeks of initially investing. VICTIM 1 subsequently invested more funds and his total balance grew to $20,000, according to the Coinance platform. VICTIM 1 wanted to withdraw this money around that time, but Coinance required him to deposit additional funds first, to be able to withdraw

afterwards. The amounts and reasons for the payments required to withdraw funds varied over time, including "gas," or "fees," or fees to unlock "keys." VICTIM 1 made at least 31 additional cryptocurrency funds transfers to at the instructions of the unidentified scammer(s) to Coinance in an attempt to withdraw his funds. At one point, Coinbase no longer allowed him to send funds to external wallets. Subsequently, the unidentified scammer(s) instructed VICTIM 1 to use Crypto.com to send funds, which he did. The unidentified scammer(s) also informed VICTIM 1 of other cryptocurrency exchanges where he could open accounts to avoid exchange-imposed waiting periods to be able to transfer funds again. The unidentified scammer(s) also sent a screenshot of a Trust Wallet which showed a total balance of approximately $7.6 million, which VICTIM 1 understood to be the location of his invested funds. VICTIM 1 did not recall being able to withdraw funds he sent to Coinance.

23. VICTIM 1's last communication with the unidentified scammer(s) before the interview was when the scammer(s) attempted to withdraw funds from their Binance wallet, but were unable because Binance had frozen the funds. The unidentified scammer(s) contacted VICTIM 1 and told him they couldn't invest VICTIM 1's money.

24. Binance investigators subsequently asked the unidentified scammer(s) to provide evidence of the source of funds frozen in Binance in their account under User ID 83699030, while also instructing VICTIM 1 as to what to provide to the unidentified scammer(s). The unidentified scammer(s) subsequently provided to Binance what VICTIM 1 had provided to them (at Binance's instruction) indicating that the operator of the Binance account under User ID 83699030 was either the same person(s) that was communicating with VICTIM 1, or was in communication with that person(s). VICTIM 1 has tried texting the unidentified scammer(s) and calling the number via WhatsApp but has not received any response since.

25. VICTIM 1 submitted an Internet Crimes Complaint Center (IC3) complaint form regarding Coinance and contacted his local FBI agent staffed out of the Lynchburg, VA Resident Agency to file a report. He also reported the issue to the Amherst County Sheriff's Office.

26. VICTIM 1 also hired a private company called CNC Intelligence Inc. to investigate and report to him the movement of his invested funds with Coinance. CNC informed VICTIM 1 that his funds had been transferred to a Binance wallet. VICTIM 1 contacted Binance regarding the funds held there.

SOURCE OF THE DEFENDANT PROPERTY

27. VICTIM 1 provided various lists of the transactions that facilitated his investments into Coinance as per the unidentified scammer(s) instructions, including a list in IC3, a list to CNC Intelligence Inc. and information he provided to Binance. Using that information, Investigators traced funds from VICTIM 1 to the account of Binance User ID 83699030. For transactions initiated by VICTIM 1, which ended up in the account of Binance User ID 83699030, there was a pattern of flow of funds: (1) VICTIM 1 deposited funds in the form of U.S. Dollars into a retail user account in his name at the cryptocurrency exchanges Coinbase or Crypto.com; (2) Funds were converted into ether (ETH) and transferred from the respective retail account in the victim's name to smart contract addresses provided by the unidentified scammer(s); (3) Funds were transferred from the receiving smart contract address in step 2 and co-mingled with funds from other smart contract addresses sharing the same code into an aggregator address 0x4cf19…8cedF via transfers; and (4) Funds were transferred into the account of Binance User ID 83699030. Transaction fees on each transaction were incurred, reducing the amount of funds that could be forwarded at each step.

28. Investigators were able to trace the following transaction from VICTIM 1's account at Coinbase as being the primary source of funds for a subsequent deposit into the account of Binance User ID 83699030:

Exchange	Date & Time	TX Hash	ETH Amount	USD Value (time of TX)
Coinbase	Aug 26, 2022 15:06:41	0x4f365…7C3Eb	93.74330002	146,146
		Total	**93.74330002**	**$ 146,146**

29. The above transaction sent VICTIM 1's funds from Coinbase to the smart contract address 0x4f365…7C3Eb. Subsequently, on August 27, 2022, at approximately 04:55 a.m. in transaction 0x83c77…81044, 92.8056 ETH of those funds were sent to the address 0x4cf19…8cedF, which served as an aggregator of funds taken in by the scheme, before ultimately transferring the majority of those funds to the account of Binance User ID 83699030. The below transaction transferred VICTIM 1's August 26, 2022 funds above from the aggregator address 0x4cf19…8cedF to an address at Binance associated with Binance User ID 83699030:

Date & Time	TX Hash	ETH Amount	USD Value (time of TX)
Aug 27, 2022 11:07:08	0xa183c…b07a4	86.297887029	129,566
	Total	**86.297887029**	**$ 129,566**

30. Similarly to the transaction initiated from Coinbase above, investigators were able to trace the following 18 transactions from VICTIM 1's account at Crypto.com as being the primary source of funds for six (6) subsequent transfers, which were made to the account of Binance User ID 83699030 via the aggregator address 0x4cf19…8cedF. The 18 deposits originating from VICTIM 1's account at Crypto.com are:

Exchange	Date & Time	TX Hash	ETH Amount	USD Value (time of TX)
Crypto.com	Sep 1, 2022 02:04:24	0x72cd8…9cb00	31.68995	49,596
Crypto.com	Sep 1, 2022 02:11:13	0x7472e…e9df9	30.67971	48,034
Crypto.com	Sep 6, 2022 21:37:13	0x084a4…f1557	62.47333	98,977

Crypto.com	Sep 15, 2022 06:23:46	0x54c69…98398	18.62329	29,421
Crypto.com	Sep 15, 2022 19:58:11	0x8d458…12e74	1.22736	1,963
Crypto.com	Sep 19, 2022 17:58:37	0xd32da…28afd	43.4664	57,762
Crypto.com	Sep 19, 2022 18:03:13	0x461e1…3ad44	36.8957	48,992
Crypto.com	Sep 20, 2022 12:05:22	0x54334…7e9d7	0.07122	98
Crypto.com	Sep 23, 2022 22:25:39	0x66ad7…5412f	1.99677	2,646
Crypto.com	Sep 23, 2022 22:29:57	0x51c0a…3d0c0	2.2146	2,960
Crypto.com	Oct 3, 2022 18:59:29	0x48b54…00ee0	142	187,425
Crypto.com	Oct 5, 2022 15:47:40	0x9b767…92ff5	3.09865	4,111
Crypto.com	Oct 7, 2022 21:00:12	0x976eb…6ad64	36.82113	49,017
Crypto.com	Oct 12, 2022 13:24:24	0x26cf4…1870a	89.53068996	116,003
Crypto.com	Nov 8, 2022 01:28:15	0x2691e…56f11	61	95,860
Crypto.com	Nov 14, 2022 21:54:01	0x6a978…c6e0a	53.82888048	66,078
Crypto.com	Nov 16, 2022 20:54:44	0x66c16…99de1	43.30131	52,414
Crypto.com	Nov 17, 2022 19:56:13	0x3a35f…8ad90	11.75797	14,184
		Total	**670.6769604**	**$ 925,541**

31. The above 18 transactions sent VICTIM 1's funds from Crypto.com to the smart contract address 0x933C3…34E04. Subsequently, via 23 transactions from September 1 to November 17, 2022, approximately 799.563039 ETH were sent from 0x933C3…34E04 to the aggregator address 0x4cf19…8cedF, the aggregator:

Date & Time	TX Hash	ETH Amount	USD Value (time of TX)
Sep 1, 2022 08:09:00	0xbe907...d333a	61.7380434	95353.79065
Sep 6, 2022 21:49:00	0x084a4...f1557	61.8446367	97771.42305
Sep 8, 2028 02:44:00	0x1f102...833e5	1.7805447	2879.42567
Sep 15, 2022 01:31:00	0x8d458...12e74	1.2111264	1972.18612
Sep 15, 2022 08:18:00	0x54c69...98398	18.4330971	30174.97995
Sep 15, 2022 11:19:00	0x5afef...ee13e	3.6781569	5826.53156
Sep 15, 2022 16:08:00	0x59439...6b10f	10.4148891	15548.49209
Sep 19, 2022 18:07:00	0x461e1...3ad44	36.5227731	48528.17385
Sep 19, 2022 18:10:00	0xd32da...28afd	43.0277463	57171.39679
Sep 20, 2022 00:24:00	0x54334...7e9d7	0.0665478	91.58375
Sep 23, 2022 22:26:00	0x66ad7...5412f	1.9728423	2616.24536
Sep 23, 2022 22:33:00	0x51c0a...3d0c0	2.188494	2902.22755
Oct 3, 2022 20:39:00	0x48b54...00ee0	140.57604	185158.3253
Oct 5, 2022 15:48:00	0x9b767...92ff5	3.0637035	4055.17923
Oct 7, 2022 21:17:00	0x976eb...6ad64	36.4489587	48533.24647

Oct 12, 2022 14:02:00	0x26cf4...1870a	88.631423057703834	115128.6733
Oct 15, 2022 19:47:00	0xe257c...a8a6d	51.475842	66082.11217
Oct 18, 2022 17:28:00	0xa4b93...eea79	7.128	9338.60664
Nov 8, 2022 01:54:00	0x2691e...56f11	60.38604	94327.2215
Nov 14, 2022 14:30:00	0x563c6y...a3584	61.38	77263.3026
Nov 14, 2022 21:56:00	0x6a978...c6e0a	53.286631673482944	64712.35124
Nov 16, 2022 20:55:00	0x66c16...99de1	42.8643369	51745.82751
Nov 17, 2022 19:57:00	0x3a35f...8ad90	11.6364303	14097.53531
	Total	**657.8382492**	**$ 1,091, 279**

32. Ultimately, the majority of those funds originally from VICTIM 1 were transferred to the account of Binance User ID 83699030 via the below six (6) transactions:

Date & Time	TX Hash	ETH Amount	USD Value (time of TX)
Sep 6, 2022 23:43:41	0x87581…0dc6a	0.12799294	211
Sep 7, 2022 2:49:01	0x9af6b…7e1a0	61.71559376	93,285
Sep 15, 2022 09:48:53	0x015d7…e99fa	20.108333648	32,336
Oct 26, 2022 16:44:11	0xfa4b4…3cb5f	160.333493667	250,881
Oct 27, 2022 08:43:33	0xda730…46982	134.563180056	209,522
Nov 25, 2022 17:22:35	0x91ec3…e02aa	236.274166081	281,779
	Total	**613.1227602**	**$ 868,014**

BINANCE USER ID 83699030 ACCOUNT ANALYSIS

33. As of August 26, 2022, Binance User ID 83699030 held no significant asset balances other than 104,128 of Binance USD (BUSD) and 54 USDT. The account held no BTC or ETH. The table below represents the totals, by asset, that were deposited into the account of Binance User ID 83699030 between August 27, 2022 and July 18, 2023. GRT, FIL, and BTC deposits are unrelated to the activities that were investigated:

Asset	Amount
ETH	756.17815118
GRT	63,806
FIL	600

BTC	0.42844609

34. Of these totals, approximately 699.4206472 ETH was primarily derived from VICTIM 1, as follows:

Date & Time (UTC)	TX Hash	ETH Amount	USD Value (time of TX)
Aug 27, 2022 11:07:08	0xa183c…b07a4	86.297887029	129,566
Sep 6, 2022 23:43:41	0x87581…0dc6a	0.12799294	211
Sep 7, 2022 2:49:01	0x9af6b…7e1a0	61.71559376	93,285
Sep 15, 2022 09:48:53	0x015d7…e99fa	20.108333648	32,336
Oct 26, 2022 16:44:11	0xfa4b4…3cb5f	160.333493667	250,881
Oct 27, 2022 08:43:33	0xda730…46982	134.563180056	209,522
Nov 25, 2022 17:22:35	0x91ec3…e02aa	236.274166081	281,779
	Total	**699.4206472**	**$ 997,580**

35. The table below represents the totals, by asset, that were withdrawn from Binance User ID 83699030 between August 27, 2022 and July 18, 2023:

Asset	Amount
BTC	0.7708
USDT	274,996.9000

36. Most withdrawals from the account of Binance User ID 83699030 were attributed to Peer-to-Peer ("P2P") transactions conducted on the Binance platform with other users, in which USDT was exchanged for Nigeria's fiat currency, NGN. Binance User ID 83699030 conducted many trades and conversions in which the ETH was exchanged back and forth for other assets, to include BUSD, USDT, and BTC. As part of this account activity, the ETH was comingled with other funds unrelated to VICTIM 1. Eventually, all the ETH was exchanged for other assets, completely depleting the account of the asset. The resulting account balances consist of the assets listed as Defendant Property above.

37. Those account balances have remained in place per Binance and remain there.

CONCLUSION

38. Based on the foregoing information, I believe probable cause exists to forfeit the Defendant Property pursuant to 18 U.S.C. § 981(a)(1)(A) as property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1957. I further believe probable cause exists to forfeit the Defendant Property pursuant to 18 U.S.C. § 981(a)(1)(C) as proceeds from violations of 18 U.S.C. § 1960. Probable cause also exists to forfeit the Defendant Property pursuant to 18 U.S.C. § 981(a)(1)(D) as proceeds of violations of 18 U.S.C. § 1343.

Andrew Jones

Andrew S Jones
IRSCI Special Agent