DECLARATION OF GEOFFREY PENDRY

I, Geoffrey Pendry, do hereby declare:

Agent Background and Training

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since January 19, 2021. My current assignment is with the Portland Field Office on the Cyber Squad investigating criminal enterprises and cyber-crimes. My training and experience include completion of twenty-one (21) weeks of specialized training received at the FBI Academy in Quantico, Virginia, related to investigative and legal matters. During that time, I was taught the use and practical application of authorized investigative techniques that federal law enforcement officers are allowed to employ. I have received specialized training in the investigation of complex financial crimes, provided by the FBI or DOJ.

Purpose of Declaration

2. This declaration is submitted in support of a complaint for forfeiture. The information contained in this declaration is based on an investigation conducted, which will show cryptocurrencies valued about $2,095,277.18 USD on about March 6, 2024, seized from a Binance exchange account with user ID 98453570, assigned to Abanoub Nady Jamil Khalil (hereinafter "**Binance Account**") was involved in transactions or attempted transactions traceable to money laundering offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions in excess of $10,000), and is property constituting or derived from proceeds obtained, directly or indirectly, from a violation of 18 U.S.C. § 1343 (wire fraud). The cryptocurrency in the **Binance Account** is therefore subject to seizure

pursuant to 18 U.S.C. §§ 981(b) and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) & (C).

3. The balance of cryptocurrency valued at approximately $2,095,277.18 USD included the following cryptocurrency assets at the time Binance transferred the cryptocurrency to an FBI controlled wallet:

- 68,114.80 Algorand (ALGO);
- 0.05818349 Binance Coin (BNB);
- 2.79601316 Bitcoin (BTC);
- 5,814.666 Mines of Dalarnia (DAR);
- 1,938.5475 Filecoin (FIL);
- 3,054,274.0584 Reserve Rights (RSR);
- 21,812.94 The Sandbox (SAND); and
- 1,844,176.191099 Tether (USDT),

(collectively hereinafter "**Defendant Cryptocurrency**").

4. The facts set forth in this declaration are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; FBI forensic accountant; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. This declaration does not set forth each and every fact that I or others have learned during the course of this investigation, only those necessary to establish probable cause to believe the cryptocurrency

described within is subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C).

Background on Cryptocurrency

5. Based on my training and experience, I know cryptocurrency is a decentralized, peer-to-peer, network-based medium of value exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.

Summary of Investigation

6. The Federal Bureau of Investigation (FBI) is investigating computer intrusion, aggravated identity theft, money laundering, and wire fraud by the operator of a subscription-based website known as the Caffeine Store that sold phishing[1] software used to steal log-in credentials, compromise online accounts, and enable theft through account takeovers and business email

[1] "Phishing" is the practice of tricking individuals into disclosing sensitive personal information through deceptive computer-based means. Often, an attacker will send emails appearing to originate from a legitimate organization that ask the recipient to log into their online accounts. The email will direct the recipient to a fraudulent login page controlled by the attacker, and the attacker can then collect any login credentials entered.

compromise[2] (hereinafter "BEC"). Based on the information below, I believe Egypt-based Abanoub Nady Jamil Khalil (hereinafter "Nady") operated the Caffeine Store. Nady sold subscription access phishing kits[3] that were used to compromise accounts, and Nady received subscription fees to the **Binance Account** from people who used the kits to compromise accounts and steal funds. I believe the origins were concealed through the use of private cryptocurrency addresses, some of which Nady used to store and bundle subscription payments prior to transferring to the **Binance Account**. I believe the balance of the **Binance Account,** the **Defendant Cryptocurrency**, consists of proceeds from Nady's involvement in the Target Offenses. The **Defendant Cryptocurrency** was target of previously issued seizure warrant (3:23-mc-991).

Statement of Probable Cause

7. In October 2022, a well-known cyber-security company that investigates cyber-attacks against its customers was likely the first to significantly publicize the Caffeine Store as a "Phishing-as-a-Service" website that offered a subscription-based platform for users to launch customized phishing attacks. The Caffeine Store website was publicly available at the domain[4] www.caffeines.store, and anyone could register using an email address and password. Once users registered, the site offered a basic subscription for $250 USD per month, a professional subscription

[2] "Business email compromise" is a form of phishing where an attacker attempts to trick someone into transferring funds, or revealing sensitive information, often by compromising a trusted business partner's (i.e. a vendor's) email account or creating an email account that looks similar to a trusted contact and requesting action, such as a wire transfer, from the recipient.

[3] A "phishing kit" is a collection of software tools that are assembled to make it simple for someone with little technical knowledge to launch a phishing attack.

[4] A "domain" or "domain name" is a unique address used to access websites, such as google.com.

for $450 USD per three months, and an enterprise subscription for $850 USD per six months. The site accepted cryptocurrency as payment and was shown as "copyrighted" by the moniker MRxC0DER. Investigators confirmed the presence of the website and corroborated several details of the cyber-security company's report.

8. The FBI opened an investigation of the Caffeine Store in October 2022 and identified historical posts showing the Caffeine Store was advertised in online forums as early as September 2021 and was frequently associated to the moniker MRxC0DER. In June 2023, the Caffeine Store appeared to be taken offline, however, investigators continued to observe payments to the suspected operator of the Caffeine Store and several cybersecurity companies have continued to observe the Caffeine Store's phishing infrastructure being used to conduct attacks after June 2023.

Caffeine Store Operator

9. According to records from Cloudflare, the Caffeine Store's proxy service was subscribed to mrxc0der@protonmail.com in May 2021, and billing began in September 2021. As previously discussed, the moniker MRxC0DER claimed to have copyrighted the Caffeine Store website, and the website was discussed in online forums as early as September 2021. The Caffeine Store's Cloudflare proxy service was paid for by a credit card with the billing name Sidney Woods and the billing address 2593 Duplex Rd., Spring Hill, TN. This is a multi-unit apartment complex, and there was no one with that name at that address in law enforcement databases. As discussed later in this affidavit, accounts linked to the operator of the Caffeine Store have used dozens of credit cards with different billing names and addresses across the United States. Based on the number of payment instruments in different names and the lack of any logical connection between

these individuals and the operator of the Caffeine Store, I believe the credit card used to pay for the Caffeine Store's proxy service was likely a compromised account. In fact, several payments to Cloudflare using this credit card appear to have failed.

10. According to records from Cloudflare, payments for the Caffeine Store's proxy service were made from IP addresses assigned to Telecom Egypt. Based on my training and experience, and suspected use of compromised credit cards, I believe the payments' origination IP is likely more indicative of the payer's location than the credit card billing information used to make the payments.

11. Cloudflare also provided records of IPs that accessed Caffeine Store's account between April 2021 and October 2022. One IP was assigned to a proxy service that obscures the true origination IP. The 41 other IPs were assigned to Telecom Egypt. Based on this information, I believe the person managing the Caffeine Store's Cloudflare proxy was likely located in Egypt.

Caffeine Store YouTube Tutorials

12. Investigators identified a YouTube account that, as of October 2023, contained several promotional and instructional videos on using the Caffeine Store platform to launch phishing attacks. Some of the videos appear to show the real-time compromise of email accounts and harvesting of login credentials. According to records from Google, the YouTube account was subscribed to abanoub.nady21@gmail.com, who primarily logged in from IP addresses assigned to Telecom Egypt. The subscriber of the email account used the name "Meth Store" and the Egyptian phone number +201159313898.

13. Investigators served a court order to Google for additional details on abanoub.nady21@gmail.com and received records for its Google Pay payment instruments. One

of the instruments listed the customer's name "Abanoub Nady." Another listed the customer's name "Abanoub Nady Gamil Khalil." Credit cards linked to the account listed several different billing names including Hector Store, Everardo Greenholt, and Amelia Windler. Based on the number of different credit cards and billing names, I believe the user of the Google account likely used or attempted to use compromised credit card information to make payments.

14. The Google account abanoub.nady21@gmail.com was linked to several other Google accounts by the same subscriber phone numbers and cookies. Based on my training and experience, I know cookies are unique pieces of data that Google and other online services use to identify specific devices/computers used to access its accounts. For instance, cookies can show the same cellphone was used to access several different Google accounts. Google linked abanoub.nady21@gmail.com to the following accounts by the presence of the same cookie on the device used to access them; abanoubnady777@gmail.com, mrzcoderii@gmail.com, caffeinestores@gmail.com, mrprincex0@gmail.com, mrzcoder@gmail.com, and mrxc0deriiii@gmail.com. I believe the use of other accounts containing the Caffeine Store name and the moniker of the Caffeine Store operator (MRxC0DER), coupled with the Caffeine Store tutorial videos, show the user of these accounts is likely the operator of the Caffeine Store.

Binance Account

15. "Abanoub Nady Jamil Khalil" (Nady) registered the **Binance Account** in March 2021. Nady uploaded photos of an Egyptian ID card in his name and a photo of himself as identity verification. Nady registered for the account using the email address bebonady73@yahoo.com. According to records from Yahoo, this email account was registered

to "bebo nady," listed the recovery email[5] bnady19@yahoo.com, and listed two verified phone numbers of +201061400117 and +201159313898. The Egyptian phone number +201159313898 was also listed in subscriber records for abanoub.nady21@gmail.com, the Google account that uploaded Caffeine Store tutorial videos to YouTube.

16. I know from my experience that Binance assigns unique identifiers to devices used to access its accounts, like a cookie. According to records from Binance, the same device was used to access the **Binance Account** and additional accounts registered to mrxc0der@yahoo.com and bnady19@yahoo.com. Only the **Binance Account** had significant stored assets, equivalent to about $1,391,000 USD as of October 3, 2023, and increased to $2,095,277.18 USD at the time of the funds were seized in March of 2024. About 99% of the funds entered the **Binance Account** as BTC or USDT, and some of those funds were exchanged for other less common types of cryptocurrencies within the account.

Tracing Deposits to the Binance Account

17. From March 2021 through September 2023, the equivalent of about $1.6 million USD was deposited, and $96,000 USD was withdrawn from the **Binance Account**. These equivalent amounts are based on the estimated conversion rate at the time of the transactions, not the present value. The total USD equivalent in the **Binance Account** as of October 3, 2023, was about $1,391,000 USD. Based on the analysis of the transactions detailed below, I believe there were three categories of deposit activity. From March 2021 to May 2023, the **Binance Account** primarily received smaller deposits averaging between $200-$900 USD, totaling about $240,000

[5] A "recovery email" is a second, or backup, email address a user designates to facilitate access to the primary email account if the user is locked out or forgets their password.

USD. From March 2021 to October 2022, the **Binance Account** received medium-sized deposits averaging about $5,000 USD totaling about $180,000 USD. From March 2023 to September 2023, the **Binance Account** received larger deposits through intermediary bundling addresses averaging about $26,000 USD, totaling about $961,000 USD.

18. According to publicly available blockchain records and records from Binance, from March 2021 to May 2023, the **Binance Account** received about 700 deposits of BTC and USDT in nearly round dollar amounts equivalent to $200-$900 USD. These deposits originated from private and anonymous addresses. Deposits in this range during this period totaled about the equivalent of $240,000 USD. When coupled with possible fluctuations in historical subscription fees and cryptocurrency valuation, I believe payments to the **Binance Account** between 2021 and early 2023 correspond to the Caffeine Store's fees of $250 to $850 USD. I believe the payment amounts, coupled with information that Nady operates the Caffeine Store and owns the **Binance Account**, indicate Nady received Caffeine Store-related payments to the **Binance Account** between 2021 and early 2023 totaling about $240,000 USD.

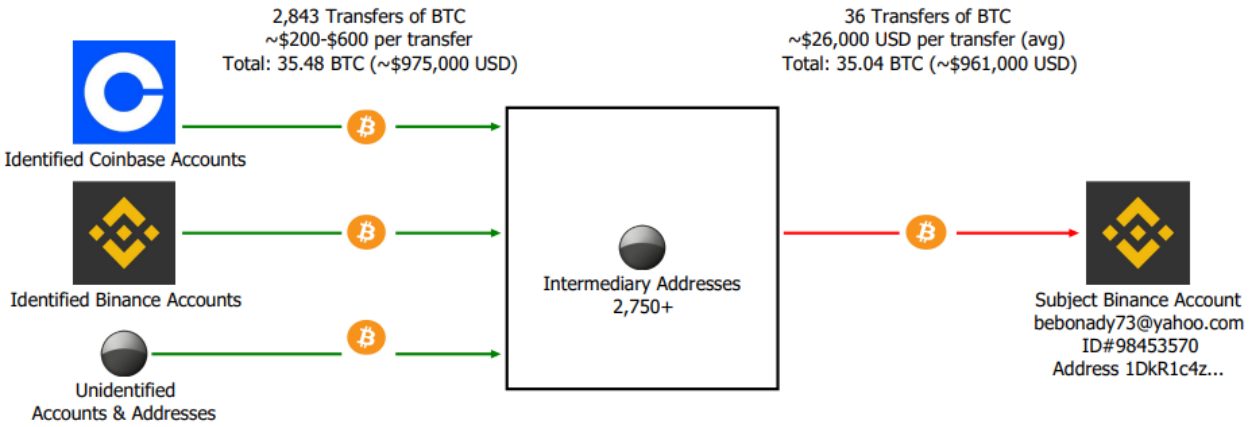
19. According to publicly available blockchain records and records from Binance, from March 2021 to October 2022, the **Binance Account** also received 36 USDT deposits over $1,000 USD, averaging the equivalent of $5,000 USD. Deposits in this range during this period totaled about the equivalent of $180,000 USD. These deposits originated from private and anonymous addresses.

20. Based on my knowledge and experience with criminal investigations involving cryptocurrency, I know successfully tracing the origin of cryptocurrency payments often depends on the proximity of those payments to an originating exchange service. Several large exchange

services collect customer data including email addresses, phone numbers, and identification documents that can be used to associate cryptocurrency addresses with their owners. A user could alternatively avoid linking their funds to an exchange and retain anonymity. Prior to March 2023, the **Binance Account** largely received funds from private and anonymous addresses.

21. According to publicly available blockchain records and records from Binance, beginning around March 2023, the **Binance Account** began to receive larger deposits averaging about $26,000 worth of USD from private cryptocurrency addresses. These private addresses received funds, stored them, and then funded transfers to the **Binance Account**. Because nearly the entire balance of these addresses was transferred to the **Binance Account**, I believe these addresses were controlled by the owner of the **Binance Account** and used to bundle funds. From March 2023 through September 2023, the **Binance Account** received the equivalent of about $961,000 USD from these intermediary addresses, as shown in the chart below.

Flow of Funds Through Intermediary Addresses to Subject Binance Account
March 2023 to September 2023



22. The FBI has access to a proprietary software tool that analyzes financial transactions on blockchains and attributes cryptocurrency addresses found on blockchains with service providers, such as exchange services. This tool allowed the FBI to link many originating transfers to Coinbase and Binance exchanges. Investigators requested records from Coinbase and Binance for transactions originating from their services to the intermediary addresses and identified 214 individual account holders, who were almost all Nigerian nationals. According to Coinbase and Binance records, the account holders logged into their accounts from many of the same Nigeria-based IP addresses at around the same times, and groups of depositors used many of the same devices to do so. Additionally, most of the account holders listed home addresses in or near Lagos, Nigeria. Some lived within blocks of each other. Based on these records and the information below linking several of the account holders to phishing and BECs, I believe these individuals are part of a coordinated organization that sends Caffeine Store subscription fees to the **Binance Account**.

Depositors to the Binance Account Linked to Phishing and BECs

23. Based on an analysis of the evidence, I believe a Nigeria-based organization purchased phishing services from the Caffeine Store and paid subscription fees to the **Binance Account**. The depositors paid in relatively consistent and round-dollar amounts mostly between $200 and $600 USD, which are roughly equivalent to the Caffeine Store's documented subscription fees of $250, $450, and $850 USD. Many of the 214 depositors have been linked to phishing and BEC-related cybercrimes by existing FBI investigations. Some of these depositors are shown below, and their links to cybercrimes are then explained in further detail.

Selected BTC Deposits to Intermediary Addresses Funding the **Subject Binance Account**		
Name[6]	**Deposit Date**	**Approx. USD Equivalent**
POI-1	3/15/2023	$300
POI-2	4/27/2023	$500
POI-3	5/15/2023	$450
POI-4	5/16/2023	$300
POI-5	5/16/2023	$600
POI-6	5/17/2023	$300
POI-7	5/17/2023	$400
POI-8	5/18/2023	$300
POI-9	5/21/2023	$300
POI-10	5/23/2023	$500
POI-11	6/6/2023	$450
POI-12	6/12/2023	$300
POI-13	7/19/2023	$400
POI-14	7/25/2023	$400
POI-15	7/26/2023	$200
POI-16	7/26/2023	$400
POI-17	8/1/2023	$400
POI-18	8/21/2023	$400
POI-19	9/5/2023	$400

24. The email address used to register POI-1's Coinbase account was identified in a separate FBI investigation in a seized customer list of a website known to sell phishing tools to its customers.

25. POI-2 and POI-19 were identified in a separate FBI investigation of a BEC resulting in a loss of over $5 million USD from a Colorado-based victim in 2021. Funds from the victim were traced to several sources including about $2.5 million USD to a Kraken exchange account that

[6] The Persons of Interest, or "POIs," identities are known to me but omitted from this affidavit to protect their identities should this affidavit become unsealed or released to the public.

sent about $780,000 USD worth of BTC to unattributed private addresses. These private addresses sent about $575,000 USD worth of BTC to POI-2's Binance account and about $1000 USD worth of BTC to POI-19's Binance account.

26. POI-3 was identified in a separate FBI investigation as the recipient of cryptocurrency from a romance scam subject who defrauded elderly people in the United States.

27. The email address used to register POI-4's Binance account was identified in a separate FBI investigation as in contact with a subject selling personally identifiable information (hereinafter "PII") and stolen credit card data. The email address used to register POI-16's Binance account appeared in logs seized by the FBI for the website used to sell the PII and stolen credit card data.

28. The Binance account held by POI-5 was identified in a separate FBI investigation after a BEC resulted in a loss of about $1.5 million from a Minnesota-based school in February 2023. The school's Chief Financial Officer's email account was compromised resulting in fraudulently directed wire transfers totaling $226,000 to a person's bank account. That same day, the person transferred $223,000 from their bank account to their cryptocurrency exchange account and sent about $100,000 USD worth of BTC through three unattributed private addresses to POI-5's Binance account.

29. The email address used to register POI-6's Binance account appeared in contact information obtained by the FBI pursuant to a court order in 2019 of a suspected client of a subject who sold domain names to be used for BECs.

30. The Binance account held by POI-7 was identified in a separate FBI investigation as linked to the proceeds of a BEC resulting in the loss of about $2 million from a Minnesota-based company in 2021.

31. POI-8 and POI-10 were identified in a separate FBI investigation after their Binance accounts were linked to payments towards a domain name used in a BEC resulting in the theft of about $10 million from a California-based company in October 2022.

32. The email address used to register POI-9's Binance account was identified in a separate FBI investigation as linked by cookies to an email account used to file suspected fraudulent COVID-related unemployment claims totaling over $3 million dollars since 2020.

33. POI-11 was indicted in the Southern District of New York in September 2022 for wire fraud and conspiracy to commit computer intrusion after a separate FBI investigation identified their involvement in a BEC resulting in the loss of over $1 million from a New York-based victim.

34. The email address used to register POI-12's Coinbase account was reported to the FBI in 2020 as registering "typo-squatter" domain names. The domain names resembled legitimate website addresses but had slightly different characters, or typos, that would direct a user to a fraudulent site. Based on my training and experience, I believe these domain names were likely used to facilitate phishing and BECs.

35. The email addresses used to register POI-13, POI-15, POI-17, and POI-14's Binance accounts appear in transaction logs seized by the FBI in 2020 from an online marketplace that sold remote access to compromised computers.

36. The email address used to register POI-18's Binance account was identified in a separate FBI investigation as a recovery email address added to a Google account. The FBI identified dozens of phishing websites designed to send stolen credentials to this Google account.

37. According to records from Binance, several of the depositors to intermediary addresses funding the **Binance Account** used the same physical devices to log into their accounts, as shown in the table below. While the FBI does not maintain derogatory information on all 214 known depositors to intermediary addresses funding the **Binance Account**, investigators believed the links by IPs, devices, home addresses, deposit amounts, and deposit timeframe show the depositors are part of a coordinated group with significant links to cybercrime.

Selected BTC Deposits to Intermediary Addresses Funding the **Binance Account** (Highlighted sections depict accounts using the same device)

Name	**Deposit Date**	**Approx. USD Equivalent**
POI-20	4/17/2023	$300
POI-21	5/8/2023	$400
POI-20	5/16/2023	$300
POI-21	6/3/2023	$500
POI-20	8/1/2023	$400
POI-22	8/10/2023	$600
POI-23	6/2/2023	$350
POI-23	6/2/2023	$50
POI-24	6/7/2023	$300
POI-23	8/2/2023	$400
POI-25	4/5/2023	$400
POI-25	5/8/2023	$400
POI-25	8/25/2023	$400
POI-25	8/25/2023	$400
POI-26	5/7/2023	$300
POI-27	8/3/2023	$300
POI-27	8/5/2023	$100

POI-28	5/30/2023	$450
POI-29	9/7/2023	$400
POI-30	5/8/2023	$275
POI-31	6/12/2023	$300

IP Overlap Between the Caffeine Store and Nady's Accounts

38. Investigators received IP login records for the Caffeine Store's proxy service and several accounts linked to Nady, including the **Binance Account.** Investigators identified a separate Binance account that was registered to bnady19@yahoo.com, which was the recovery email address for the **Binance Account**'s registered email address bebonady73@yahoo.com. The bnady19@yahoo.com Binance account shared many of the same login IPs and was accessed by several of the same physical devices as the **Binance Account**. The bnady19@yahoo.com Binance account was registered to Roumani Nady Jamil Khalil, who shares the same last name as Nady (Nady Jamil Khalil), submitted an Egyptian ID card to Binance listing the same Egyptian home address as Nady, is less than two years younger than Nady, and submitted an identity verification photo that appears to have the same light-green wall color as the verification photo submitted by Nady (photos included below). Based on this information, investigators believed Roumani Nady Jamil Khalil is Nady's brother and lived at the same residence in Egypt.

///

///

///

Abanoub Nady Jamil Khalil (Identity Document Submitted for the **Binance Account)**	Roumani Nady Jamil Khalil (Identity Document Submitted for the bnady19@yahoo.com Binance Account)
	

39. Based on my training and experience analyzing IP records, I believe the level of overlap shown in the table below shows the owner of the **Binance Account** is same person operating Caffeine Store's proxy service. I believe the use of the same IPs to access the bnady19@yahoo.com Binance account shows the IPs were assigned to a common location, such as a residence, used by Nady and his brother to access the internet. Based on the significant IP overlap, use of common devices, and link by recovery email to the **Binance Account**, I believe it's also possible the bnady19@yahoo.com Binance account is operated by Nady despite being registered to his suspected brother.

///

Common IPs used to access the Caffeine Store and Binance Accounts associated to Nady			
IP Address (Telecom Egypt)	Caffeine Store Cloudflare Proxy Account	**Subject Binance Account**	Bnady19@yahoo.com Binance account
154.183.179.197	5/3/21 at 18:18 UTC	5/3/21 at 15:32 UTC	5/3/21 at 15:39 UTC
154.183.171.94	9/26/21 at 00:28 UTC	9/26/21 at 00:34 UTC	
197.54.215.22	11/19/21 at 19:14 UTC	11/19/21 at 19:18 UTC	
154.179.49.188	12/18/21 at 16:34 UTC	12/18/21 at 19:01 UTC	
197.54.173.58	4/8/22 at 15:52 UTC		4/8/22 at 22:38 UTC
197.54.132.234	4/11/22 at 04:08 UTC		4/10/22 at 21:53 UTC
156.210.153.193	6/4/22 at 03:00 UTC		6/3/22 at 23:49 UTC
156.210.171.72	7/2/22 at 11:53 UTC	7/2/22 at 16:40 UTC	
197.54.166.53	8/30/22 at 02:16 UTC		8/29/22 at 21:20 UTC
197.54.174.220	9/19/22 at 16:52 UTC		9/19/22 at 15:23 UTC
156.210.162.246	10/12/22 at 23:36 UTC	10/12/22 at 19:28 UTC	
156.210.184.2	10/13/22 at 19:40 UTC		10/13/22 at 15:25 UTC
156.210.135.242	10/18/22 at 16:33 UTC		10/18/22 at 15:12 UTC

40. The table above shows IPs used to access the Caffeine Store's Cloudflare account and are presumably all logins by the person operating the account. In addition, investigators obtained a pen register/trap & trace court order to collect all IPs handled by the Cloudflare proxy to the Caffeine Store website domain caffeines.store. This data includes all IP traffic to and from

the Caffeine Store website through its Cloudflare proxy and is not limited to the operator's logins to the administrative Cloudflare account. For instance, if anyone was to access www.caffeines.store using a web browser, their IP was likely logged by Cloudflare during this period because its servers handled traffic to the website domain. Investigators obtained this traffic data from about December 9, 2022, to January 29, 2023, which yielded about 10,000 unique IPs. Based on my knowledge and experience analyzing website data, I believe these IPs likely include those used by the operator and customers of the website.

41. As shown in the table below, many of the same IPs used to access the **Binance Account** were also used to access caffeines.store through its Cloudflare proxy at about the same times. Coupled with more limited access logs to the administrative Cloudflare proxy account, I believe this data further demonstrates the person holding the **Binance Account** is also accessing and operating the Caffeine Store.

Common IPs in caffeines.store website traffic and the **Binance Account**		
IP Address (Telecom Egypt)	Caffeines.store website traffic	**Binance Account**
197.54.170.82	12/26/22 at 09:14 to 12/27/22 at 13:56 UTC	12/31/22 at 09:02 UTC
156.210.172.10	1/4/23 from 10:23 to 10:41 UTC	1/4/23 at 21:28 UTC
156.210.186.250	1/5/23 from 14:17 to 17:57 UTC	1/5/23 at 14:24 UTC
197.54.163.211	1/6/23 at 07:31 to 1/8/23 at 08:01 UTC	1/7/23 at 12:02 UTC
156.210.189.238	1/9/23 at 18:20 to	1/9/23 at 23:08 UTC

	1/10/23 at 06:47 UTC	
197.54.143.217	1/22/23 at 05:01 UTC	1/22/23 at 13:48 to 1/23/23 at 00:32 UTC
197.54.129.163	1/24/23 at 09:14 to 1/25/23 at 04:55 UTC	1/23/23 at 12:20 to 1/25/23 at 22:38 UTC
197.54.186.90	1/28/23 from 18:44 to 19:52 UTC	1/29/23 from 04:19 to 13:11 UTC

Seizure Warrant

42. On November 15, 2023, the FBI obtained a seizure warrant signed by United States Magistrate Judge Jeffrey Armistead commanding the seizure of "all cryptocurrency contained in Binance exchange account with user ID 98453570, associated with email address: bebonady73@yahoo.com, assigned to Abanoub Nady Jamil Khalil." The warrant was executed on November 16, 2023, as it was served to Binance via the online portal under Binance case number BNB-62840. Binance confirmed receipt on November 18, 2023, and completed the transfer of the crypto to a government-controlled wallet on March 6, 2024.

43. FBI confirmed receipt of the crypto on March 22, 2024. The cryptocurrency balances at the time of execution varied from the actual amounts seized. Binance told investigators that the user had set a spot trade between USDT and BTC some time ago, which was executed automatically when the price was hit. The execution occurred between the test transfer date and the remaining balance transfer date, resulting in the balance change. Consequently, about 20.26 BTC was converted to USDT, an increase of about 1,111,000 USDT, between the time of the last account review, on about October 3, 2023, and the time that Binance transferred the funds to government control on March 6, 2024.

Conclusion

44. Based on the information above, I have probable cause to believe, and do believe, that the **Defendant Cryptocurrency** is subject to seizure pursuant to 18 U.S.C. § 981(b) and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) & (C), as monies involved in transactions or attempted transactions or traceable to money laundering offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions in excess of $10,000), and is property constituting or derived from proceeds obtained, directly or indirectly, from a violation of 18 U.S.C. § 1343 (wire fraud).

I declare under penalty of perjury that the foregoing is true and correct pursuant to 28 U.S.C. §1746.

Executed this 27th day of February 2026.

/s Geoffrey Pendry
GEOFFREY PENDRY
Special Agent
Federal Bureau of Investigation