

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Seizure of)
)
ALL FUNDS FROM ONE CRYPTOCURRENCY) Case No. 24-sz-27
ACCOUNT PURSUANT TO 18 U.S.C. §§ 981, 982,)
AND 28 U.S.C. § 2461(c))

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under 18 U.S.C. §§ 981, 982, AND 28 U.S.C. § 2461(c)

(describe the property):

SEE ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, HEREBY INCORPORATED BY REFERENCE.

‡ Continued on the attached sheet.

Applicant's signature

_____, Special Agent

Printed name and title

Attested to by the applicant in according with the requirements of Fed. R. Crim. P. 41 by telephone.

Date: 06/21/2024

City and state: District of Columbia

 2024.06.21
12:39:53 -04'00'

Judge's signature

Robin M. Meriweather, United States Magistrate Judge

Printed name and title

AO 109 (Rev. 12/09, modified by USAO-DC) Warrant to Seize Property Subject to Forfeiture by Telephone

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of)
)
ALL FUNDS FROM ONE CRYPTOCURRENCY) Case No. 24-sz-27
ACCOUNT PURSUANT TO 18 U.S.C. §§ 981, 982,)
AND 28 U.S.C. § 2461(c))

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE BY TELEPHONE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the jurisdiction of the District of Columbia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

ONE CRYPTOCURRENCY ACCOUNT, FURTHER DESCRIBED IN ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before July 5, 2024
(not to exceed 14 days)

☐ in the daytime – 6:00 a.m. to 10:00 p.m.

☒ at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.


An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge Robin M. Meriweather

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 06/21/2024


Judge's signature

2024.06.21

12:40:35 -04'00'

City and state: District of ColumbiaRobin M. Meriweather, United States Magistrate Judge

Printed name and title

AO 109 (Rev. 12/09) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.:
24-sz-27

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEIZED

The property to be seized includes all virtual currency, funds, monies, and other things of value stored in or accessible at Binance Cryptocurrency Exchange associated with User ID [REDACTED] and associated with the email address [REDACTED], and in the name of [REDACTED]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEIZURE OF ALL
FUNDS FROM ONE CRYPTOCURRENCY
ACCOUNT PURSUANT TO 18 U.S.C. §§ 981,
982, AND 28 U.S.C. § 2461(c)

Case No. 24-sz-27

Filed Under Seal

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Internal Revenue Service's Criminal Investigation division ("IRS-CI"), and I have been so employed since March 2019. As an IRS-CI Special Agent, my responsibilities include the investigation of criminal violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code), the Bank Secrecy Act (Title 31, United States Code), and related offenses. I am currently assigned to IRS-CI's Cyber Crimes Unit, which is tasked with complex investigations involving virtual currency. I have conducted several complex national security investigations including into violations of U.S. economic sanctions and virtual currency money laundering. Prior to my employment with IRS-CI, I was a Special Agent with the [REDACTED] Office of Inspector General for approximately five years. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

2. The facts in this affidavit come from my personal observations, my training and experience, review of records and documents, and information obtained from other law enforcement officials, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter. The dates listed in the affidavit should be read as “on or about” dates.

PROPERTY TO BE SEIZED

3. This affidavit is made in support of a seizure warrant for all assets, virtual currency, funds, monies, and other things of value (“**SUBJECT ASSETS**”) stored in or accessible via the account at Binance Cryptocurrency Exchange (“Binance”) bearing User ID [REDACTED], associated with the email address [REDACTED] and in the name of [REDACTED], which translates to [REDACTED], hereinafter “[REDACTED]” Open-source translation of the name provided in Binance records provides an alternative spelling of his last name, [REDACTED].” [REDACTED]’s Binance account is the “**SUBJECT ACCOUNT.**” On or about January 9, 2024, Binance froze the **SUBJECT ACCOUNT.** There is currently a sum of 6,360.45 Solana virtual currency tokens (SOL) remaining in the **SUBJECT ACCOUNT.**¹ As of on or about June 7, 2024, one SOL was worth approximately \$171.60. Solana is volatile and subject to significant value changes, including significant value fluctuation daily. As of on or

¹ Binance initially froze 10,034.79 SOL in the **SUBJECT ACCOUNT** on or about January 9, 2024, but on or about April 4, 2024, a foreign law enforcement agency seized 3,673 SOL that was traceable to a non-U.S. victim. As such, the **SUBJECT ASSETS** available for seizure are 6,360.45347340 SOL, which excludes the portion already seized by foreign law enforcement.

about June 7, 2024, the value of the assets in the **SUBJECT ACCOUNT** was approximately \$1,091,453.22.

LEGAL AUTHORITY FOR SEIZURE

4. I have probable cause to believe that the **SUBJECT ACCOUNT** is subject to seizure and forfeiture because it is proceeds of a specified unlawful activity – namely, fraud and related activity in connection with computers, in violation of 18 U.S.C. § 1030, and wire fraud, in violation of 18 U.S.C. § 1343 -- and/or involved in money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i) -- and as such is subject to civil forfeiture, pursuant to 18 U.S.C. § 981(a)(1)(A) and (C) and subject to criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1) and (2)

5. 18 U.S.C. § 1343 (wire fraud) prohibits, in pertinent part, whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

6. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such financial transaction which in fact involves the proceeds of specified unlawful activity knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

7. 18 U.S.C. § 981(a)(1)(A) (forfeiture for violations of 18 U.S.C. § 1956) provides for the forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 as well as any property traceable to such property.

8. 18 U.S.C. § 981(a)(1)(C) (forfeiture for specified unlawful activities) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity (“SUA”), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA, including a violation of Section 1030. Section 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the United States Code. Section 1961(1) references violations of 18 U.S.C. § 1343.

9. 18 U.S.C. § 982(a)(1) provides for the criminal forfeiture of any property, real or personal, involved in or traceable to a violation of 18 U.S.C. § 1956, 1957, and 1960.

10. 18 U.S.C. § 982(a)(2)(A) and (B) provide for the criminal forfeiture of any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of an offense in violation of 1343(A) or 1030(B), among other offenses.

11. A restraining order would be inadequate to preserve the cryptocurrency for forfeiture. Based on my training and experience, I know that restraining orders served on banks sometimes fail to preserve the property for forfeiture because the bank representative receiving the restraining order fails to put the necessary safeguards in place to freeze the money in time to prevent the account holder from accessing the funds electronically or fails to notify the proper personnel as to the existence of the order. The risk of such problems is higher, not lower, with virtual currency. In contrast, a seizure warrant guarantees that the funds will be in the

government's custody upon execution of the warrant and, thus, preserved for forfeiture. A Binance official initially told IRS-CI that Binance would freeze the SUBJECT ACCOUNT temporarily. IRS-CI later formally requested that Binance freeze the account. IRS-CI does not know for how long Binance will preserve the assets for forfeiture.

12. This Court has the authority to issue seizure warrants for assets located in a foreign jurisdiction pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that a seizure warrant may be issued by a "judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)] and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement." 18 U.S.C. § 981(b)(3). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located in a foreign jurisdiction.²

Background on Ransomware Attacks and Virtual Currency Terminology

13. **Ransomware:** Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through virtual currency, in exchange for a key to decrypt

² Binance Holdings Limited ("Binance") claims that it is a non-U.S. company and, therefore, is not subject to U.S. jurisdiction and cannot be compelled by U.S. process. Binance has further indicated, however, that it is willing to voluntarily freeze the SUBJECT ACCOUNT, and transfer cryptocurrency to the United States with a seizure warrant issued by a federal judge.

the files and restore victims' access to systems or data. Ransomware actors often launder the virtual currency payments they receive through a series of obfuscating transactions.

14. **Virtual Currency:** Virtual currencies, or “cryptocurrencies,” are forms of digital currencies that are circulated over the internet as a form of value. Virtual currencies are typically not backed by a government, which distinguishes them from electronic forms of fiat currency (currency that derives its value from government regulation or law, such as the U.S. dollar). For instance, fiat currency stored in an electronic bank account is not considered virtual currency. There are numerous virtual currencies. Individual units of virtual currencies are often referred to as tokens or coins. For example, bitcoin is a type of virtual currency token.

15. **Bitcoin:** Bitcoin (BTC) is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin was not issued by any government, bank, or company, but rather was generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

16. **Solana:** Solana (SOL) is another type of virtual currency, circulated over the Internet as a form of value. Like Bitcoin, Solana was not issued by any government, bank, or company, but rather was generated and controlled through computer software operating via a decentralized, peer-to-peer network.

17. **Tether:** Tether is a decentralized virtual currency or token that, like Bitcoin and Solana, is circulated over the Internet, supported by a peer-to-peer network, and not backed by a government. However, unlike BTC, the Tether is known as a “stable coin” because it was designed to keep a stable price. According to its developers, Tether’s price is “tethered” to the value of fiat

currency, for example the U.S. dollar, because the value of all outstanding tokens is backed by collateral equivalent to the market capitalization of the token.

18. **Virtual Currency Exchanges or Exchangers:** Virtual currency exchanges (“VCE”) are trading and/or storage platforms for virtual currencies such as BTC, Solana and Tether. Many VCEs also store their customers’ virtual currency in virtual currency wallets. These wallets can hold multiple virtual currency addresses associated with a user on a VCE’s network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., Know Your Customer (“KYC”) checks) and to have anti-money laundering (“AML”) programs in place (to the extent they operate and service customers in the United States).

19. **Virtual Currency Address:** Virtual currency addresses are the particular virtual locations to which virtual currencies are sent and from which they are received. An address is analogous to a bank account number and is represented as a string of letters and numbers.

20. **Private Key:** Each address is controlled using 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.

21. **Virtual Currency Wallet:** 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.

22. **Blockchain:** Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. Some virtual currencies focus on privacy and portions of their blockchains are not visible online to everyone. There are different blockchains for different types of virtual currencies. For example, BTC and Solana exist and are recorded on different Blockchains that are referred to as the "Bitcoin blockchain" and "Solana blockchain," respectively.

23. **Blockchain Analysis:** It is virtually impossible to look at a sole transaction on a blockchain and immediately ascertain the identity of the individual behind said transaction. That is because blockchain data generally only consists of alphanumeric strings and timestamps. That said, law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To do so, law enforcement can use blockchain explorers, as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools, which are hereinafter referred to as "blockchain tools," to be reliable.

24. Because a blockchain serves as a searchable public ledger of every transaction utilizing a specific virtual currency, through the use of blockchain analysis, investigators are in certain instances able to trace transactions to VCEs. And because VCEs often collect identifying information about their customers, appropriate legal process submitted to these VCEs can, in some instances, reveal the true identity of the individual responsible for the transaction.

25. For instance, although the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular address by analyzing the blockchain. These analyses can also reveal additional addresses controlled by the same individual or entity. “For example, when an organization creates multiple [virtual currency] addresses, it will often combine its [virtual currency] addresses into a separate, central [virtual currency] address (i.e., a “cluster”). It is possible to identify a ‘cluster’ of [virtual currency] addresses held by one organization by analyzing the [virtual currency] blockchain's transaction history. Opensource tools and private software products can be used to analyze a transaction.” *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

26. In this investigation investigators have relied on anti-money laundering software offered by private blockchain analytics companies that is used by financial institutions and law enforcement organizations worldwide including to help perform financial investigations and compliance and/or risk mitigation functions. This software has supported many investigations and has been the basis for numerous search and seizure warrants, and as such, has been found to be reliable. Law enforcement has been able to verify the reliability of this software by ex-post analysis on numerous occasions. For example, in an unrelated case, such software directed the government to over 50 customers of a darknet child pornography site. *See United States v. Twenty-Four*

Cryptocurrency Accounts, 473 F. Supp. 3d 1 (D.D.C. 2020). In each one of the 50 subsequent law enforcement actions, the software's data was corroborated by statements and search warrant returns from the targets' devices. In sum, this software has correctly analyzed data on the blockchain in hundreds of investigations, and I have assisted or been briefed on many of these investigations.

27. Blockchain analysis has repeatedly been presented in testimony at trial and has withstood scrutiny by defense counsel. *See, e.g., United States v. Ologeanu et al*, 5:19-cr-00010 (E.D.Ky.) (defendant Iossifov was convicted at trial following testimony regarding blockchain analysis; multiple other defendants pleaded guilty in advance of trial); *United States v. Dove*, 8:19-cr-33 (M.D. Fla.) (defendant pleaded guilty mid-trial following testimony regarding blockchain analysis); *United States v. Felton*, No. 20-cr-347 (N.D. Ga.) (defendant pleaded guilty mid-trial to multiple counts of wire fraud, securities fraud, and money laundering, following blockchain analysis testimony); *United States v. Ulbricht*, 14-cr-68 (S.D.N.Y.) (administrator of Silk Road darknet market convicted at trial that included blockchain analysis testimony) (upheld in *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017)); *United States v. Costanzo*, No. 2:17-cr-00585 (D. Ariz.) (defendant found guilty of money laundering at trial following testimony regarding blockchain analysis) (upheld in *United States v. Costanzo*, 956 F.3d 1088 (9th Cir. 2020)).

28. In addition, I am advised that blockchain analysis has repeatedly been considered by judges in issuing search and seizure warrants. For example, in assessing the reliability of blockchain analysis in an opinion published February 2022 in the District of Columbia, Magistrate Judge Zia Faruqi observed: "The unprecedented rate of prior success, lack of incentive or capacity to lie, and incredible level of detail (the software draws out each transaction block-by-block that

comprises a cluster), make the clustering software a reliable foundation for probable cause that is beyond compare.” *In the Matter of Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956*, 2022 WL 406410, at *13 (D.D.C. Feb. 8, 2022).

29. **Cluster:** A cluster is a collection of addresses that can be attributed to one person or entity through various means, including co-spending,³ in order to determine the number of virtual currency tokens held by an individual. In other words, a cluster is an estimate of all of the virtual currency addresses (and its virtual currency content) contained in a user’s wallet or wallets. Because the blockchain records every address, and maintains records of every transaction, and all the known balances for each address, forensic computer experts are able to create clustering algorithms that examine the entire history of virtual currency transactions recorded on the blockchain and make logical connections between different addresses.

30. **Virtual Currency Mixers:** Virtual currency mixers, sometimes referred to as “tumblers,” are service businesses that consolidate virtual currency from several different sources and then redistribute those funds for the purpose of obscuring the source and destination of funds. Mixers typically use algorithms to obscure the output from the input. For instance, some mixers give users the options to delay receiving payment or to break the output up into several smaller payments. Blockchain analytical companies have analyzed clusters of addresses, which they label in their respective tools as likely belonging to mixers. Law enforcement in combination with these companies have developed reliable methods of tracing funds through some mixers. This process is referred to as “de-mixing.”

³ Co-spending refers to the practice of using smaller transactions originating from multiple sources to fund a larger transaction.

31. **Darknet Markets:** Darknet markets (DNMs) are website marketplaces that promote anonymity of customers and are frequently used to sell illicit items and services. DNMs are only accessible through a special network browser on the internet known as The Onion Router (“Tor”). Tor conceals DNM users’ true IP addresses, which allows users to mask their true identities, and thereby provides relative anonymity. DNM consumers register accounts on the website to conduct transactions and utilize virtual currencies to trade for these illicit goods and services. DNM market administrators and customers often utilize mixers to obscure the source and destination of funds being sent to DNMs.

FACTS SUPPORTING PROBABLE CAUSE

Investigation Background

32. IRS-CI and Homeland Security Investigations (HSI) (“investigative team”) are investigating a ransomware scheme by a Russian ransomware group known as the Royal Ransomware Group (“Royal”). Royal is a ransomware threat actor that is believed to have been operating since approximately September 2022. According to a public service announcement released by the Federal Bureau of Investigation (FBI) and the U.S. Cyber Security Infrastructure Agency (CISA),⁴ Royal gains access to victims’ networks, disables antivirus software, and exfiltrates large amounts of data before ultimately deploying the ransomware and encrypting the systems. Royal actors have targeted numerous critical infrastructure sectors including, but not limited to, Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and

⁴ <<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a>> Accessed March 26, 2023.

Education. Royal victims are typically required to pay ransoms in BTC by accessing a darknet website.

33. As discussed in detail below, this affidavit discusses one line of investigation into an individual who received and laundered virtual currency from a New Jersey-based Royal Victim (“Victim 1”). On or about April 4, 2023, Victim 1 paid a ransom of 49.3120227 BTC, which was worth \$1,445,454.86 at the time of the transaction. A portion of those proceeds were repeatedly deposited and withdrawn into the SUBJECT ACCOUNT until the funds were frozen by Binance on or about January 9, 2024.

34. The SUBJECT ACCOUNT was opened using the driver’s license of a Ukrainian national named [REDACTED], hereinafter [REDACTED]). [REDACTED] used the email address [REDACTED] when opening the Binance account (hereinafter, the **SUBJECT ACCOUNT**).

35. Based on analysis of the blockchain and the SUBJECT ACCOUNT, which is summarized in detail below, there is probable cause to believe that [REDACTED] launders ransomware funds originating from Royal and other ransomware actors through his account. Furthermore, there is probable cause that the funds currently in the SUBJECT ACCOUNT, namely 6,360.45347340 of the virtual currency Solana (SOL), the “SUBJECT ASSETS,” are laundered ransomware funds that [REDACTED] used as part of a money laundering scheme.

36. The SUBJECT ASSETS were transferred into the SUBJECT ACCOUNT in six different transactions between December 15, 2023, and January 9, 2024, and originally totaled 10,034.79 SOL before a foreign law enforcement agency seized 3,673 SOL that was traceable to a non-U.S. victim. As such, the SUBJECT ASSETS available for seizure are 6,360.45347340

SOL, which excludes the portion already seized by foreign law enforcement. The SUBJECT ASSETS were originally valued at \$506,894.12 when first deposited into the SUBJECT ACCOUNT but have since increased in value to approximately \$1,091,453.22. Investigators note that the price of Solana is volatile.

37. The source of the SUBJECT ASSETS is still under investigation but, as described in detail below, there is probable cause to believe that 3,673 SOL, currently valued at \$630,286.80, originated from Victim 1's ransom payment. Furthermore, there is probable cause to believe that the remainder of the SOL in the SUBJECT ACCOUNT that cannot be traced directly to the Victim 1 payment, namely 2,687.45 SOL (this amount has been reduced by the amount seized by the foreign law enforcement agency), was used as facilitating property in furtherance of [REDACTED]'s money laundering scheme. As such, the U.S. seeks to seize and forfeit the entire amount of the SUBJECT ASSETS within the SUBJECT ACCOUNT.

I. The SUBJECT ACCOUNT Received Funds Originating, in Part, from a Ransom Paid by Victim 1 to Royal Ransomware

38. On April 14, 2023, HSI obtained information related to ransomware payments paid to Royal between April 1, 2023, and April 12, 2023 from a confidential source (CS-1) that is a business that has a history of providing accurate information to the government. CS-1 assists ransomware victims in purchasing virtual currency and paying ransoms. According to CS-1, on or about April 4, 2023, CS-1 facilitated a ransom payment for a victim based in New Providence, New Jersey. CS-1 provided HSI with a copy of the ransomware note left on the victim's network in which Royal claims responsibility for the ransomware attack and directs the victim to a known Royal dark web site to engage in negotiations. This is consistent with the ransomware note Royal

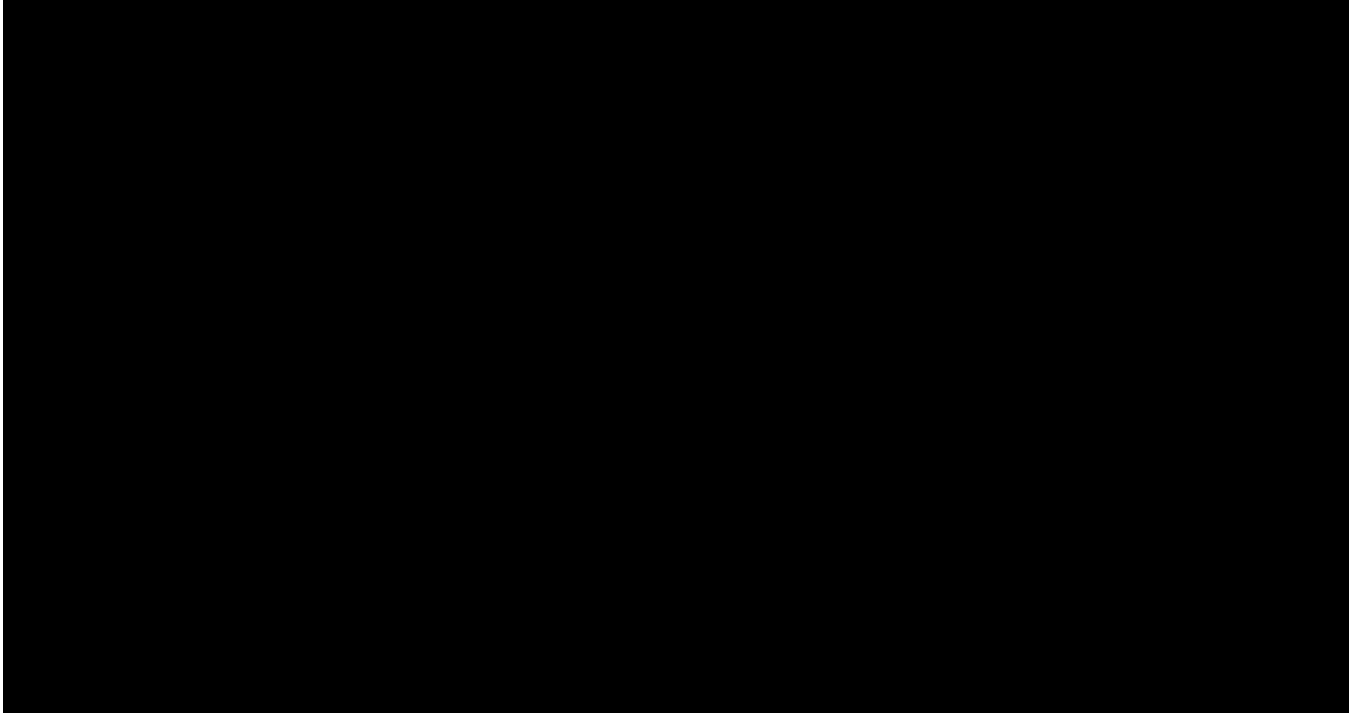
leaves on its victims' networks. CS-1 indicated they (CS-1) facilitated a transaction on behalf of Victim 1 on April 4, 2023 for 49.3120227 BTC (approximately \$1,445,454.86 at the time) to the address provided by Royal ([REDACTED]). [REDACTED] is hereinafter referred to as the "Ransom Address."

39. Between the original payment on April 4, 2023, and August 29, 2023, an approximately five-month period, the Victim 1 ransom was commingled with approximately 7.7 BTC and split into two separate transactions before being recombined into a single address cluster that includes the address [REDACTED] (hereinafter, the "[REDACTED] Cluster").

40. The route traveled by the Victim 1 ransom is summarized in the below graphic. The ransom paid by Victim 1 is on the left side of the graphic and the path of those funds is shown in red traveling to the "[REDACTED] Cluster" on the right side of the graphic. Investigators note that the Victim 1 ransom was commingled with two unknown sources (notated with "?" icons) and portions of the funds were routed two separate ways on August 16, 2023, before being recombined into the [REDACTED] Cluster. The first portion (11.7 BTC), which is represented on the bottom path within the chart, was sent directly into the [REDACTED] Cluster. The second portion was sent through the SUBJECT ACCOUNT, represented on the top branch of the chart, before being withdrawn from the SUBJECT ACCOUNT and combined into the [REDACTED] cluster in three separate transactions.⁵ Notably, the unknown sources that were commingled are small

⁵ Investigators note that one payment from [REDACTED]'s Binance account to the [REDACTED] cluster occurred on August 14, 2023 ([REDACTED]), which was two

(only 1.73 BTC and 5.976 BTC totaling approximately 7.7 BTC) when compared to the 34.67 BTC ransom proceeds originating from Victim 1. The source of those 34.67 Victim 1 ransom proceeds, prior to being commingled with the unknown 7.7 BTC, have been highlighted in the graphic below.



41. Based on training and experience, I recognize the above-depicted transaction patterns as being consistent with money laundering. More specifically, routing the Victim 1 ransom payment two separate directions after commingling them with outside funds is a technique commonly used to obscure the volume, source, and destination of funds. Consequently, there is probable cause to believe that all funds that were commingled with the Victim 1 ransom proceeds

days before the Victim 1 ransom was deposited into [REDACTED]'s Binance account of August 16, 2023. These funds have been included in the chart to portray the total source of funds deposited into the [REDACTED] Cluster and because there is probable cause to believe, based on the activity within [REDACTED]'s Binance Account, that those funds were intended to obscure the volume, source and destination of the Victim 1 ransom payments that were ultimately deposited into the [REDACTED] Cluster.

in the above chart were funds intended to facilitate the money laundering scheme. In total, 42.9566432 in BTC were deposited into the [REDACTED] cluster including 34.67 BTC that originated directly from Victim 1 proceeds.

42. There is probable cause to believe that the [REDACTED] cluster is controlled by a ransomware threat actor, or their associate, who has affiliation with several different ransomware groups based on the deposits into that cluster. The chart below summarizes the source of BTC deposited into the [REDACTED] cluster, which was comprised of 78% from ransomware-related funds including 56% from the Victim 1 Payments (including funds that were commingled with the Victim 1 payment that were used in an attempt to conceal the ransomware proceeds), 17% from funds directly traceable to three other Royal victims⁶, and 4.5% from addresses that are likely

⁶ Investigators traced approximately 13.2 BTC deposited into cluster [REDACTED] originating from three different Royal Ransomware victims attributed by Blockchain Tool 1. While the identities of these victims are unknown, based on training and experience, and reliability of blockchain analytics described in the background on virtual currency section above, there is probable cause to believe this information is credible. These victims sent funds to the following addresses between January 28, 2023, and March 17, 2023: [REDACTED] (01/28/2023 00:04), [REDACTED] (02/26/2023 01:33), [REDACTED] (03/17/2023 16:57)

controlled by other Ransomware affiliated groups called Alpha-V Blackcat and Biban.⁷ All the lines listed below are ransomware-related funds except for line 5 labeled “other.”⁸

Line	Source of Funds Deposited into Ransomware Cluster	BTC Received	USD Equivalent	% of Total Deposits (BTC)
1	Victim 1 Ransom (Direct)	11.70380477	\$ 340,796.19	15.38%
2	Victim 1 Ransom (Indirect Through [REDACTED] Binance Account)	31.2566432	\$ 833,410.92	41.07%
3	Unknown Royal Victims Identified Through Blockchain Tools	13.2190392	\$ 386,262.63	17.37%
4	Addresses Controlled Biban/AlphaV Ransomware	3.49478135	\$ 90,990.00	4.59%
5	Unknown Sources	16.42320817	\$ 464,148.90	21.58%
6	Total BTC Deposited	76.09747669	\$ 2,115,608.64	100.00%
7	Total Funds Traceable to Victim 1 Ransom Payment (Line 1 + 2)	42.96044797	\$ 1,174,207.11	56.45%
8	Total BTC Traceable to Ransomware-Related Funds (Sum: Lines 1,2,3,4)	59.67426852	\$ 1,651,459.74	78.42%

43. Based on the above-described money laundering activity, there is probable cause to believe that BTC from unknown sources were commingled with the illicit funds to conceal the volume of illicit activity, as well as the source and destination of the illicit funds. As such, 100%

⁷ Cluster [REDACTED] received 3.49 BTC (\$461,148) from an address cluster that contains 14 addresses including [REDACTED]. This cluster sent 57% of its deposited funds directly to a cluster of addresses controlled by organizations that are labeled as ransomware affiliates in Blockchain Tool 1 including Biban ([REDACTED]) and AlphV Blackcat ([REDACTED]). The fact that this address cluster sent funds to AlphV Blackcat is notable. According to a press release by the U.S. DOJ, “the Blackcat ransomware group — also known as ALPHV or Noberus — has targeted the computer networks of more than 1,000 victims and caused harm around the world since its inception, including networks that support U.S. critical infrastructure.” <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant>

⁸ The 21% of funds deposited into the Cluster [REDACTED] that is categorized as “unknown” originated from seven different addresses or clusters that are not attributed in Blockchain Tool 1. Those addresses include [REDACTED],

[REDACTED] Investigators note that [REDACTED] is part of a three-address cluster that, according to Blockchain tool 1, received 30% of its funds indirectly from clusters associated with a ransomware actor called “Hive.”

of the deposits into the [REDACTED] cluster (76.09 BTC) were funds used in the ransomware money laundering scheme. This is important because all those funds would later be deposited into the SUBJECT ACCOUNT, as discussed below.

44. On September 18, 2023, the 76.09747669 BTC in the [REDACTED] cluster, which was 100% of the deposits in that cluster, were withdrawn to the SUBJECT ACCOUNT in a single withdrawal of 76.0971157 BTC, which was valued at \$2,036,549.81. This payment had a transaction hash of [REDACTED]. A portion of these funds would later be used to purchase a portion of the SUBJECT ASSETS, as discussed in the next section.

II. The SUBJECT ACCOUNT Further Laundered the Ransomware Funds Before Using those BTC to Purchase a Portion of the SUBJECT ASSETS

45. On September 18, 2023, the SUBJECT ACCOUNT received the 76.09 in laundered ransomware proceeds from the [REDACTED] cluster that were discussed in the section above. Within five minutes of the funds being deposited, [REDACTED] sold those BTC and received \$2,068,542.85 in another virtual currency, Tether (USDT). Approximately 6 hours after that, [REDACTED] sold 2,066,474.37 in USDT and received 77.04837 BTC. Based on training and experience, this rapid conversion of BTC to USDT and back to BTC is consistent with a money laundering technique designed to make the funds more difficult for law enforcement to trace.

46. Also, on September 18, 2023, and several days later on September 25, 2023, [REDACTED]'s Binance account received approximately 1.04 BTC from unknown sources in two separate transactions.⁹ In total, the current balance of [REDACTED]'s Binance account was at least

⁹ [REDACTED]'s Binance account also received .25 tokens of a different virtual currency called Ether

77.8 BTC and investigators note that the amount of BTC received from unknown sources was small compared to the amount deposited from the [REDACTED] Cluster. However, investigators note that the exact balance of [REDACTED]'s Binance account is difficult to determine based on his rapid conversion between currencies. Based on the above-described laundering patterns, the entirety of virtual currency in [REDACTED]'s Binance account, which is believed to have equaled approximately 77.8 BTC, either originated from ransomware or originated from funds that were used to conceal the ransomware proceeds in furtherance of the money laundering scheme. These approximately 77.8 BTC are hereinafter the "laundered ransomware funds."

47. Between September 21, 2023, and September 28, 2023, [REDACTED] withdrew all of the laundered ransomware funds from his Binance account (77.8 BTC) and the funds traveled through several unhosted addresses. The recipient of those funds, likely [REDACTED],¹⁰ moved almost all of those funds between three different BTC addresses, and re-deposited approximately the same amount of funds (77.436 BTC) into [REDACTED]'s Binance account on September 28, 2023.

48. Between September 28, 2023, and September 30, 2023, approximately half (38.32 BTC) of the laundered ransomware funds were converted to USDT and withdrawn to an unknown address that appears to be controlled by an unknown service.¹¹ The remainder of the BTC

(ETH) on September 18, 2023, which was valued at approximately \$417.00. Investigators note that this was a small amount compared to the laundered ransom funds present at the time from the [REDACTED] Cluster.

¹⁰ As discussed in the virtual currency background section, there is no "know your customer" or other identifying information about the individual who owns or controls unhosted addresses. However, investigators believe that [REDACTED] or his close associate likely controlled many of the unhosted addresses discussed throughout this affidavit because the funds were repeatedly deposited and withdrawn from his Binance account.

¹¹ On September 30, 2023, approximately 1,391.276829 USDT were also withdrawn from the

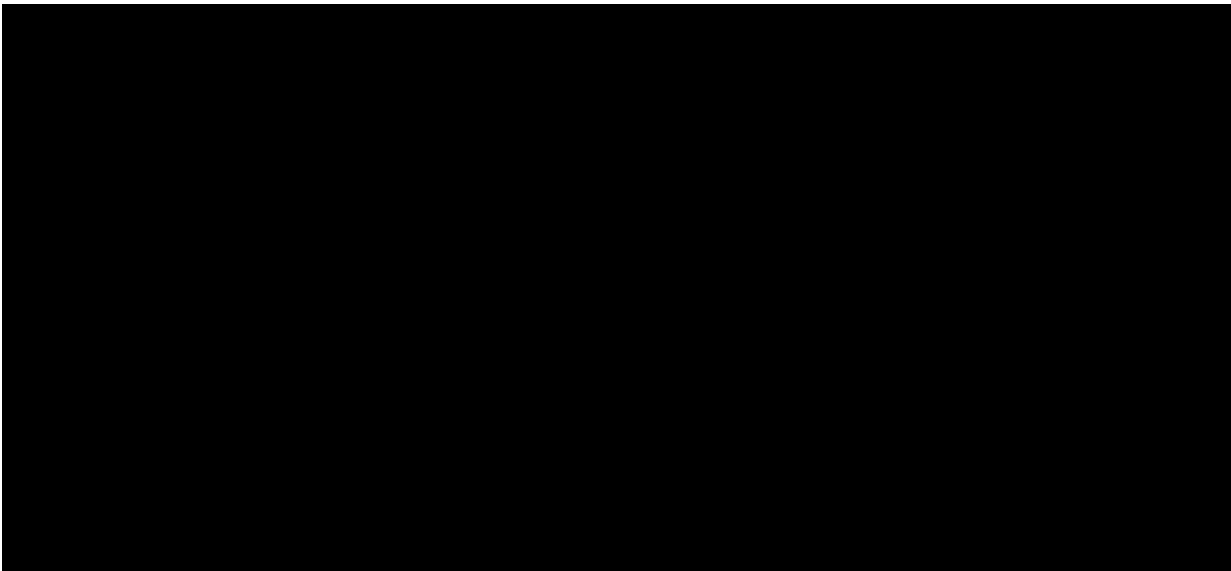
(approximately 37.9907 BTC) stayed in [REDACTED]'s Binance account and are hereinafter referred to as the "remaining laundered funds." The remaining laundered funds are important because a portion of them would later be used to purchase some of the SUBJECT ASSETS, as discussed in detail below.

49. Between October 1, 2023, and October 6, 2023, [REDACTED] withdrew the remaining laundered ransomware funds (37.9907 BTC) to an unhosted address, [REDACTED], and then redeposited that entire amount less fees (37.9906 BTC) back into his Binance account on October 6, 2023. Once deposited, [REDACTED] used the same conversion from BTC to USDT to BTC laundering technique as he had used previously on September 18, 2023 (*See generally* para. 43).

50. Between October 9, 2023, and October 16, 2023, [REDACTED] again withdrew the remaining laundered ransomware funds (38.301296 BTC) to a new unhosted address, [REDACTED], and then redeposited that entire amount less fees (38.301275 BTC) back into his Binance account on October 16, 2023.

SUBJECT ACCOUNT to an account at the Bitget virtual currency exchange that was opened using the same email that was used to open the SUBJECT ACCOUNT [REDACTED]. This transaction, which was valued at only \$1,391.27, has been excluded from the body of the affidavit due to the small size. However, the fact these funds were withdrawn to this Bitget account is notable because a portion of the Victim 1 ransom proceeds were traced to that Bitget account (discussed in detail later in the affidavit).

51. Paragraphs 43 through 48 are depicted in the graphic below where 100% of BTC in the [REDACTED] cluster (76.097 BTC) were withdrawn from the [REDACTED] cluster on the left side of the graphic and moved through several unhosted addresses before being deposited back into the SUBJECT ACCOUNT on September 28, 2023. A day later, those funds were split and half were sent to an unknown service while the “remaining laundered funds” (highlighted in yellow) were withdrawn from the SUBJECT ACCOUNT and shortly thereafter deposited back into the SUBJECT ACCOUNT on October 6, 2023. Those same BTC (approximately 38 BTC) were then withdrawn from the SUBJECT ACCOUNT and redeposited into the SUBJECT ACCOUNT approximately a week later on October 16, 2023.



52. Based on training and experience, the above-described transactions wherein [REDACTED] withdrew and then redeposited the same amount of funds in his Binance account, repeatedly, is a technique commonly used by criminals to launder virtual currency. More specifically, removing the funds and then redepositing them repeatedly makes it more difficult to trace the source and destination of the funds using blockchain tools because investigators need to

obtain records from the virtual currency exchange, in this case Binance, to continue tracing to the destination of the funds.

53. Between October 17, 2023, and October 26, 2023, the 38.301275 BTC of remaining laundered ransomware funds in [REDACTED]'s Binance account were repeatedly sold for USDT and then repurchased, which is the same laundering technique that [REDACTED] used previously on September 28, 2023. In further substantiation that this activity is indicative of money laundering, during this time, [REDACTED] made withdrawals to parties that had exposure to ransomware, mixers, and darknet markets, as summarized below.

a. On October 22, 2023, at approximately 16:53:42, [REDACTED]'s Binance account withdrew 1.009 BTC (\$30,290.59) to address [REDACTED] (Address [REDACTED]). According to Blockchain Tool 1, Address [REDACTED] is part of a cluster of 21 addresses that received a total of approximately \$86,508 in BTC including 21% of funds from illicit sources including ransomware, darknet markets, mixing services, and OFAC-sanctioned entities including Hydra, Garantex, Sinbad.io, and Blender.io.

b. On October 23, 2023, at approximately 17:24:08 [REDACTED]'s Binance account withdrew 0.04894000 BTC (\$1,618.45) to address [REDACTED] (“Address [REDACTED]”). According to Blockchain Tool 1, Address [REDACTED] is part of a cluster of 8 Addresses that received 39% of its funds from mixers, including most prominently from a mixer called SamuraiWallet.com.

54. On October 27, 2023, and November 5, 2023, [REDACTED] withdrew 27.927 BTC of the remaining laundered proceeds to an unhosted address starting with “[REDACTED]” through another unhosted address starting with “[REDACTED].”¹² Investigators note that the amount of remaining laundered proceeds was reduced by the above-described illicit withdrawals, as well as several other withdrawals that occurred during this time.

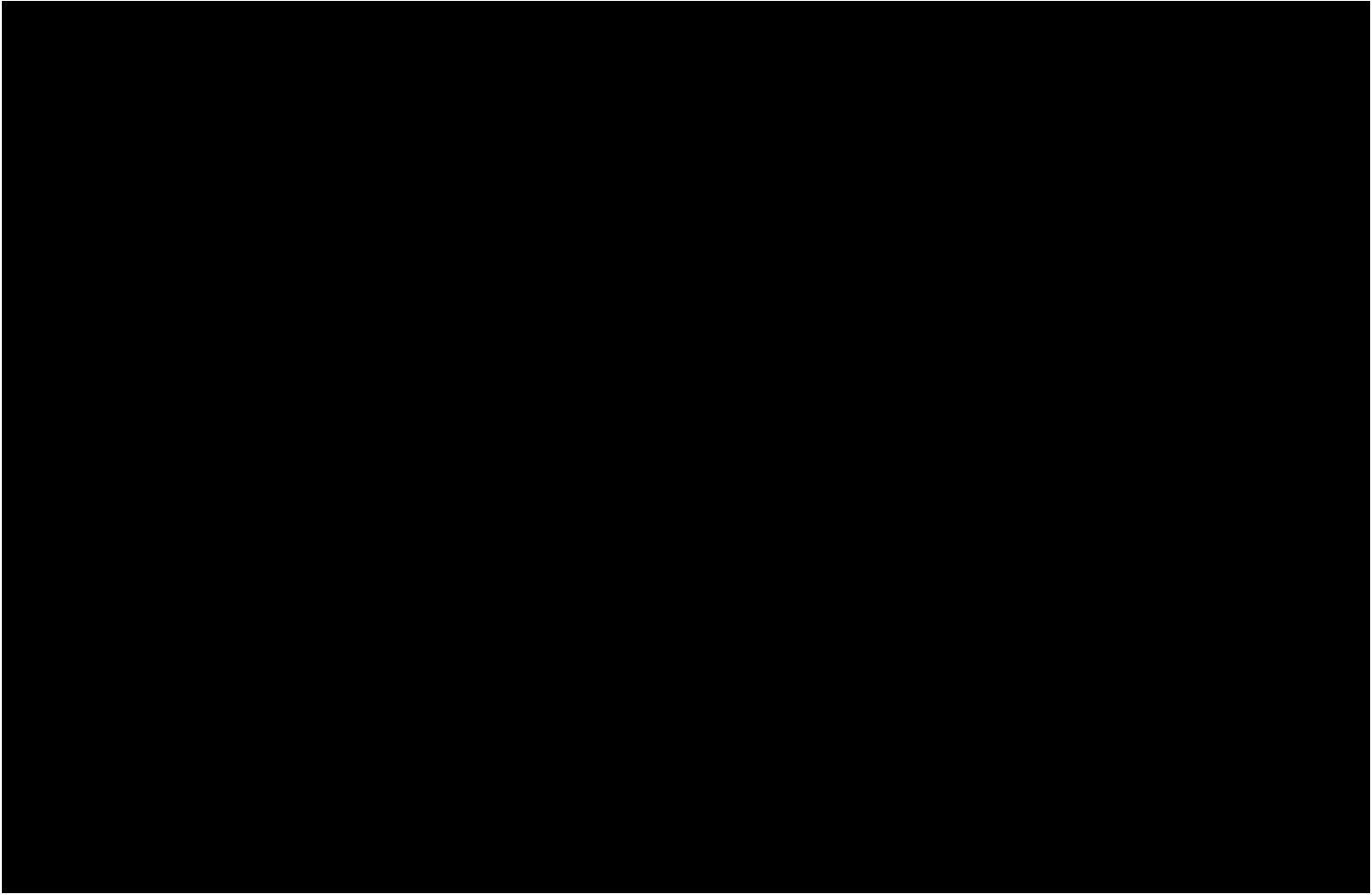
55. On December 4, 2023, [REDACTED] withdrew 4.8226 BTC of the remaining ransom proceeds from [REDACTED] to an account at the Bitget virtual currency exchange (Bitget) with user ID [REDACTED], while the remainder were transferred to an unknown account at Bybit and to an unhosted address that, as of now, has not been spent or transferred.¹³

56. Paragraphs 52 through 53 are summarized in the graphic below wherein 33.62 BTC were withdrawn from the SUBJECT ACCOUNT and divided along two separate routes. The first route, which is depicted on the lower path, resulted in 4.8266 BTC being deposited into the Bitget account (this transaction is highlighted for emphasis) while the remaining funds (represented on the upper branch) resulted in 21.1 BTC that were traced, in part, to the Bybit virtual currency exchange. The BTC traced to Bitget are important because investigators were able to trace the funds through Bitget to the SUBJECT ACCOUNT where they were used to purchase a portion of the SUBJECT ASSETS.¹⁴

¹² Full addresses: [REDACTED]

¹³ The funds traced to Bybit are discussed in detail later in this affidavit. Additionally, the Investigative Team traced 17.55 BTC to address [REDACTED] (“Address [REDACTED]”) where the funds are currently residing.

¹⁴ The Investigative Team was unable to trace the laundered ransomware funds through the Bybit exchange. However, circumstantial evidence that those Bybit funds were re-deposited into the SUBJECT ACCOUNT is discussed in the next section.



57. This Bitget account that received 4.8266 BTC of the laundered ransom funds, described and depicted above, was opened using the same email address that [REDACTED] used to open the SUBJECT ACCOUNT, [REDACTED]. However, the identification documentation used to open the account was not [REDACTED]'s but rather the passport photo and selfie photograph of a female named [REDACTED] which translates to [REDACTED] [REDACTED]. Based on training and experience, I know that money launderers often use false KYC photo identification or the KYC information from friends, associates, or relatives but often re-use the same email accounts to maintain control of the account, which I believe occurred in this instance. In further substantiation that [REDACTED] controlled this Bitget Account, the funds

deposited into the Bitget Account were later transferred back to the SUBJECT ACCOUNT, which belongs to [REDACTED]. As such, this Bitget Account is referred to as [REDACTED]'s Bitget account.

58. On December 4, 2023, after receiving the 4.8226 BTC into his Bitget account, [REDACTED] sold that BTC and received 3,231.39 tokens of a different virtual currency called Solana. Based on the facts above, there is probable cause to believe this Solana was purchased with the laundered ransomware funds and was worth approximately \$235,891 on the date of the transaction.

59. On December 19, 2023, [REDACTED]'s Bitget account withdrew approximately 3,231.39 SOL to the SUBJECT ACCOUNT where the funds were frozen by foreign law enforcement authorities.

60. Between December 19, 2023, and the date of this writing (June 7, 2024), the U.S. dollar price for Solana increased from \$73.00 to \$171.60. As a result, the value of the 3,231.39 Solana traceable to the remaining ransomware laundered funds increased from \$235,891 to \$554,506.52.

61. In summary, based on the above facts, there is probable cause to believe that [REDACTED] purchased 3,231.39 SOL, which is currently valued at approximately \$554,506.52, with the laundered ransom funds.

62. The remainder of the SUBJECT ASSETS, namely 6,803 SOL (a portion of which have already been seized by foreign law enforcement agencies as discussed previously), were purchased using funds that are not directly traceable to the laundered ransomware funds. However, based on the money laundering techniques repeatedly observed on the blockchain and within [REDACTED]'s account discussed above, there is probable cause to believe that the remainder of the

SUBJECT ASSETS were funds used to facilitate money laundering and to obfuscate the source, destination, and volume of transactions originating from the laundered ransomware funds. As such, the untraceable portion of the SUBJECT ASSETS are hereinafter referred to as the “facilitating property.” Probable cause that the facilitating property was used in furtherance of the money laundering scheme is detailed below.

III. Probable Cause that the Untraceable Solana within the SUBJECT ACCOUNT Was Used to Facilitate Money Laundering

63. Between December 15, 2023, and January 9, 2024, [REDACTED]’s Binance account received deposits of the SUBJECT ASSETS that were not directly traceable to the laundered ransomware funds. This Solana originated from Bybit and was deposited into the SUBJECT ACCOUNT over five transactions totaling 6,803 Solana, which was worth approximately \$563,785,884.38 at the time of the transactions.

64. Law enforcement has not been able to obtain records from Bybit to confirm the source of those funds. However, based on the money laundering techniques used by [REDACTED] and his associates discussed throughout this affidavit, there is probable cause to believe that these Solana deposits from Bybit were facilitating property. Furthermore, there is circumstantial evidence that provides probable cause to believe that the SOL deposits from Bybit were made in furtherance of the money laundering scheme, as discussed below.

65. Based on training and experience, the fact that the deposits from Bybit were deposited in the Solana token is significant because Solana was the same token to which the laundered ransomware funds (traceable to Victim 1) were ultimately converted prior to being deposited into the SUBJECT ACCOUNT. Based on training and experience, commingling

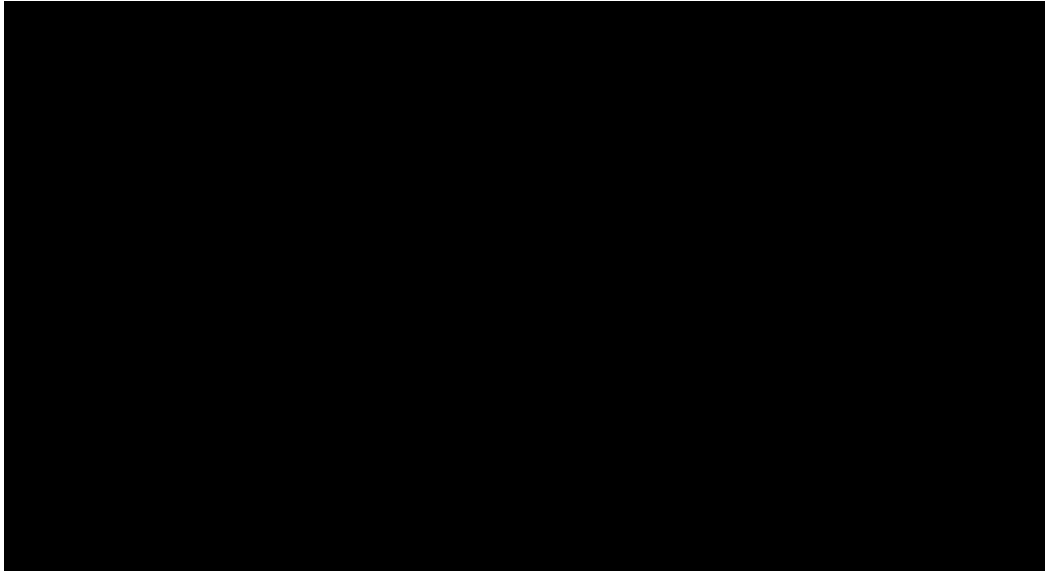
purportedly “clean” funds with illicit funds, and specifically using funds of the same token, is a technique used by money launderers to obfuscate the volume, source, and destination of funds.

66. Also notable, the Solana from Bitget, which originated from the laundered ransom proceeds as discussed above, was deposited into [REDACTED]’s Binance account on December 19, 2023, which occurred in the middle of the deposits of the facilitating property, which were deposited between December 15, 2023, and January 9, 2024. Based on training and experience, the synchronization of deposits of illicit funds with other funds is a technique used by money launders to obscure the source of funds and volume of illicit funds.

67. Finally, while law enforcement was unable to trace the exact source of the facilitating property, including whether it originated from the laundered ransom funds, the fact that the facilitating property originated from Bybit is notable because a portion, and more specifically 7 BTC valued at approximately \$299,458 of the laundered ransom proceeds were traced to Bybit around the same time that approximately the same amount (\$261,048.53) of Solana were deposited into the SUBJECT ACCOUNT from Bybit. This is potentially important because, based on the timing of the transactions, it is possible that the laundered ransom funds traced to Bybit were the same funds withdrawn from Bybit to the [REDACTED] Binance account after they were converted to Solana at Bybit (or at another exchange enroute to being transferred to Bybit).

68. This timing is depicted in the below graphic where the dotted line at the top of the graphic represents Bybit records that are unavailable to law enforcement to determine whether the Bybit account that received the laundered ransomware proceeds in BTC converted a portion of them to Solana and then withdrew them to [REDACTED]’s Binance account. The similar amounts and timing of the transactions have been highlighted for emphasis. Investigators note that

conversion of the laundered ransomware proceeds from BTC to Solana, if it occurred within the unknown Bybit account, would have been a similar process to the known process used by [REDACTED] to convert BTC to Solana within the Bitget account.



CONCLUSION

69. Based on the foregoing, as well as my training, education, and experience, I submit that there is probable cause to believe that all of the funds held in the **SUBJECT ACCOUNT**, in any form, are proceeds of, or traceable to proceeds of violations of 18 U.S.C. §§ 1030 (fraud and related activity in connection with computers) and/or 1343 (Wire Fraud), and/or are involved in violations of 18 U.S.C. § 1956(a)(1)(B)(i) (Concealment Money Laundering), and therefore subject to criminal and civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), (C) and 982(a)(1), (2). Binance has further indicated, in response to an inquiry specific to this case, that it is willing to voluntarily freeze the **SUBJECT ACCOUNT**, and transfer cryptocurrency to the United States with a seizure warrant issued by a federal judge.

Respectfully submitted,

[REDACTED]

[REDACTED], Special Agent
Internal Revenue Service – Criminal
Investigation

Attested to me in accordance with the requirements of Fed. R. Crim. P. 4.1 via telephone
on June 21, 2024.



2024.06.21

12:41:18 -04'00'

Honorable Robin M. Meriweather
United States Magistrate Judge