

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.

UNITED STATES OF AMERICA,

Plaintiff,

v.

APPROXIMATELY 919.30711258 ETHER COINS
SEIZED FROM ETHEREUM WALLET ADDRESS
0x71949d87258c4ca6827730c337f80907d73c7800;

APPROXIMATELY 2.65995166 BITCOINS
FORMERLY HELD IN BITCOIN WALLET ADDRESS
16qq4DGd2R9vcK5xmV5nRQmoZn2WZVSYK1; AND

ALL VIRTUAL CURRENCY SEIZED ON OR
ABOUT JUNE 16, AND 19, 2017, AND FORMERLY
HELD IN BITCOIN WALLET ADDRESS
12EZr5x8mFpxS6ypNobhPXmyj4BbRkm6GW,
INCLUDING, BUT NOT LIMITED TO,
APPROXIMATELY 640.26804512 BITCOINS;
APPROXIMATELY 640.2716098 BITCOIN CASH;
APPROXIMATELY 640.2715428 BITCOIN GOLD;
AND APPROXIMATELY 640.2716043 BITCOIN SV,

Defendants *In Rem*.

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff, the United States of America (the “United States”), by and through its undersigned counsel, to allege upon information and belief as follows:¹

I. NATURE OF THE ACTION

1. This is a civil action *in rem*, pursuant to 18 U.S.C. § 981(a)(1)(A) and (C), and the procedures set forth in Rule G of the Supplemental Rules for Admiralty or Maritime Claims and

¹ All dates and amount referenced in this Complaint are approximate.

Asset Forfeiture Actions, and the Federal Rules of Civil Procedure, to forfeit the following property, currently valued at approximately \$47 million, that constitute proceeds of computer fraud in violation of 18 U.S.C. § 1030, property involved in money laundering transactions in violation of 18 U.S.C. § 1956, and/or property traceable to such property (collectively, the “Defendant Virtual Currency”):

- a) Approximately 919.30711258 ether coins seized on or about May 16, 2017, from Ethereum wallet address 0x71949d87258c4ca6827730c337f80907d73c7800;
- b) Approximately 2.65995166 bitcoins seized on or about June 30, 2017, and formerly held in Bitcoin wallet address 16qq4DGd2R9vcK5xmV5nRQmoZn2WZVSYK1;
and
- c) All virtual currency seized on or about June 16, and 19, 2017, and formerly held in Bitcoin wallet address 12EZr5x8mFpxS6ypNobhPXmyj4BbRkm6GW, including, but not limited to, approximately 640.26804512 bitcoins, approximately 640.2716098 Bitcoin Cash, approximately 640.2715428 Bitcoin Gold, and approximately 640.2716043 Bitcoin SV.

II. JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1345 and 1355 and 18 U.S.C. § 981(a)(1).

3. This Court has *in rem* jurisdiction over the Defendant Virtual Currency pursuant to 28 U.S.C. § 1355.

4. Venue for this action is proper in this District because acts or omissions giving rise to the forfeiture occurred in the Southern District of Florida, and the Defendant Virtual Currency was seized in Parkland, Florida, which is within this District. *See* 28 U.S.C. §§ 1355(b)(1), 1395.

III. FACTUAL ALLEGATIONS

A. Overview of The Onion Router Network, the Dark Web, and Virtual Currency

5. Devices directly connected to the internet are identified by unique numbers called Internet Protocol (“IP”) addresses used to route information. Generally, when one device contacts a second device, the two connected devices (for instance, a home computer and the www.google.com website server) know each other’s IP address to communicate information. In addition, publicly available databases can be easily searched to obtain the IP address for any known Uniform Resource Locator (“URL”)² and the registered owner and location of any IP address.

6. The Onion Router (“TOR”) network is a special network of computers distributed around the world designed to conceal the true IP addresses of the users of the network. Every communication sent through the TOR network is directed through numerous relays within the network and wrapped in a layer of encryption at each relay, such that the end recipient of the communication has no way of tracing the communication back to its true originating IP address.

7. In order to access the TOR network, anyone can download the TOR network browser software and access the internet by inputting a website IP address or URL into the TOR network browser. The TOR network browser automatically encrypts and routes the communication through several relays so that the destination website can only see the IP address of the last (or “exit”) relay and not the IP address of the device actually connecting to the destination website. Although the IP address of the user would remain hidden from the destination website, the user must know the URL or IP address of the website in order to have directed a connection to it through the TOR network.

²A URL is colloquially termed a web address.

8. Thus, the TOR network on its own achieves only one-way anonymity. To achieve two-way anonymity, the TOR network enables websites to operate inside the network in a manner that conceals the true IP address of the computer server that is hosting the website. Such “hidden services” operating on TOR network have complex web addresses which are generated using a computer algorithm, and these hidden service websites end in “.onion[.]” Also, unlike a standard URL, there is no way to retrieve a website server’s true IP address from its “.onion” TOR network address alone.

9. This network of anonymous users and hidden service websites is known as the “Dark Web.” Criminal actors have taken advantage of the Dark Web to create websites with online marketplaces designed to promote the anonymous sale of illegal items, such as hacked online account information and narcotics. Dark Web marketplaces are specifically designed to facilitate illegal commerce by working to ensure the anonymity of its administrators, as well as of the buyers and sellers who participate in commerce on the website.

10. Dark Web marketplaces’ escrow services further promote anonymity, as purchases are made primarily in virtual currency, such as bitcoin,³ that are “tumbled” or “mixed” by the marketplaces’ participation in the transaction (i.e., a buyer transfers funds to the Dark Web marketplace, and the Dark Web marketplace subsequently transfers the funds to the seller upon satisfaction of the terms of sale). By providing escrow services, along with tumbling services, Dark Web marketplaces scramble multiple buyer-seller virtual currency transactions in order to conceal the virtual currency payments from buyer to seller or commission payments to the administrator.

³In accordance with accepted practice, “Bitcoin” here refers to the protocol, software, and community, and “bitcoin” (with a lowercase letter b) refers to units of the virtual currency.

11. Most virtual currencies log each transaction as part of their “blockchain,” generally a decentralized public ledger that records all transactions. For example, the Bitcoin blockchain includes every address that has ever received a bitcoin and maintains public records of every transaction for each address. Some virtual currencies, for example bitcoin and ether, are not issued by any government, bank, or company, but rather are generated and controlled through computer software operating via a decentralized, peer-to-peer network.

12. Bitcoin and Ethereum⁴ are two protocols of the many varieties of virtual currency, circulated over the internet as a form of value. Bitcoins and ether coins are sent to and received from “addresses” or “wallets,” which are somewhat analogous to bank account numbers and are represented by a string of letters and numbers that are 26-to-35-characters long and case sensitive. Each wallet is controlled through the use of a unique private key, a cryptographic equivalent of a password or pin needed to access the wallet’s address. The address and the private key by themselves rarely reflect any personal identifying information. As a result, little-to-no personally identifiable information about the payor or payee is transmitted in a transaction as only the address of the receiving party and the sender’s private key are needed.

B. Undercover Dark Web Transactions with Moniker 1

13. From at least in or around October 2015, a vendor using an online alias (“Moniker 1”) was involved in the selling of illicit items and hacked online account information on several Dark Web marketplaces, some of which that are no longer in operation.

⁴Similar to Bitcoin, “Ethereum” refers to the protocol, and “ether” refers to the currency in this Complaint.

14. In or around January 2017, agents reviewed Moniker 1's Dark Web marketplace sales feedback (which operates similarly to that of customer feedback reviews on other consumer websites), which indicated that Moniker 1 conducted over 100,000 Dark Web transactions.

15. Among these transactions were several purchases of hacked online account information from Moniker 1 made by undercover law enforcement agents in or around 2016 and 2017, including, but not limited to:

- i. On or about January 29, 2016, an undercover law enforcement officer purchased ten (10) Netflix accounts usernames and passwords from Moniker 1 on a Dark Web marketplace for approximately 0.00132443 bitcoins;
- ii. On or about April 20, 2016, an undercover law enforcement officer purchased one (1) World Wrestling Entertainment account username and password from Moniker 1 on a Dark Web marketplace for approximately 0.01134 bitcoins;
- iii. On or about September 14, 2016, an undercover law enforcement officer purchased sixty (60) Uber accounts usernames and passwords from Moniker 1 on a Dark Web marketplace for approximately 0.0824 bitcoins;
- iv. On or about March 7, 2017, an undercover law enforcement officer purchased three (3) Xfinity accounts usernames and passwords from Moniker 1 on a Dark Web marketplace for approximately 0.040 bitcoins; and
- v. On or about March 13, 2017, an undercover law enforcement officer purchased one (1) HBOGO account username and password and one (1) Showtime account username and password from Moniker 1 on a Dark Web marketplace for approximately 0.0118 bitcoins.

16. Law enforcement agents contacted some of the relevant online service providers, such as Netflix and Uber, and confirmed that the accounts purchased from Moniker 1 appeared to belong to real and unrelated individuals.

17. Law enforcement agents then contacted some of the subscribers and confirmed that they did not know that access information to their online accounts had been sold by Moniker 1 on Dark Web marketplaces.

C. Identification of the Individual 1

18. In or around 2016, law enforcement agents identified two residences in Florida linked to Moniker 1 after Moniker 1 provided the addresses as the shipping address when he or she previously purchased narcotics from Dark Web marketplaces.

19. Through investigative means, agents determined that the individual associated with the two Florida addresses was, at the time, currently residing in Parkland, Florida (the “Parkland Residence”).

20. The occupant of the Parkland Residence (“Individual 1”) was subsequently identified.

21. A Comcast IP address was associated with the Parkland Residence, which is within the Southern District of Florida. Internet traffic to and from the Comcast IP address between in or around December 2016 and March 2017 revealed numerous internet connections from the Parkland Residence on the TOR network. In addition, the internet traffic data showed correlations between when the TOR network was accessed at the Parkland Residence and when messages were received from Moniker 1 by the law enforcement officer(s) making the undercover purchases identified in paragraph 15 above.

22. Surveillance of Individual 1 and the internet traffic to and from the Parkland Residence confirmed that Individual 1 was the individual controlling the online alias Moniker 1.

23. Individual 1 had bank accounts at PNC Bank, including a personal checking account ending in 0929 that was opened on or about November 13, 2014. According to PNC records, Individual 1 was the authorized signer on this account and was self-employed when the account was opened.

24. From in or around April to November 2016, the following cash transactions occurred in Individual 1's PNC Bank account ending in 0929:

Date	Deposit/Withdrawal	PNC Branch	Amount
April 5, 2016	deposit	Penn Plaza, NY	\$3,408.16
April 6, 2016	withdrawal	N SR 7, FL	\$3,400.00
April 19, 2016	deposit	Penn Plaza, NY	\$6,653.83
April 21, 2016	withdrawal	N SR 7, FL	\$6,650.00
April 27, 2016	deposit	Penn Plaza, NY	\$4,757.77
April 29, 2016	withdrawal	N SR 7, FL	\$300.00
April 29, 2016	withdrawal	N SR 7, FL	\$2,700.00
May 19, 2016	deposit	Penn Plaza, NY	\$3,423.09
May 20, 2016	withdrawal	N SR 7, FL	\$4,000.00
June 13, 2016	deposit	Grove St., NJ	\$2,480.00
June 14, 2016	withdrawal	N SR 7, FL	\$1,500.00
July 5, 2016	deposit	Westgate Dr., NC	\$4,400.00
July 8, 2016	withdrawal	N SR 7, FL	\$3,000.00
October 3, 2016	deposit	Century Corners	\$1,960.00
October 4, 2016	withdrawal	N SR 7, FL	\$1,900.00
October 27, 2016	deposit	W 47th St., IL	\$3,000.00
October 31, 2016	withdrawal	N SR 7, FL	\$2,200.00
November 25, 2016	deposit	Penn Plaza, NY	\$2,500.00
November 28, 2016	withdrawal	N SR 7, FL	\$2,500.00

25. Surveillance photos confirm that Individual 1 conducted the cash withdrawals from PNC Bank account ending in 0929.

26. Persons who are involved in the commerce of hacked online account information on the Dark Web convert virtual currencies to, and from, standard currencies such as U.S. dollars through a variety of methods, including by anonymously selling the virtual currency on

LocalBitcoins.com, a website which facilitates peer-to-peer virtual currency exchange transactions, in exchange for individuals who make third-party deposits into a vendor's bank account.

27. The cash transaction activity in Individual 1's PNC Bank account ending in 0929 was consistent with that of a Dark Web vendor converting virtual currency into cash using LocalBitcoins.com.

D. Seizure of the Defendant Virtual Currency Involved in Money Laundering

28. On or about May 16, 2017, law enforcement agents executed a federal search warrant for the Parkland Residence.

29. Following the search, Individual 1 confirmed his or her online use of Moniker 1.

30. From in or around May 2017 onwards, the Defendant Virtual Currency was seized by law enforcement with Individual 1's consent and cooperation and transferred to Government custody from the following virtual currency wallets:

- a) On or about May 16, 2017, approximately 919.30711258 ether coins were seized from Ethereum wallet address 0x71949d87258c4ca6827730c337f80907d73c7800 (the "Ethereum 7800 Wallet");
- b) On or about June 30, 2017, approximately 2.65995166 bitcoins formerly held in Bitcoin wallet address 16qq4DGd2R9vcK5xmV5nRQmoZn2WZVSYK1 (the "Bitcoin SYK1 Wallet") were seized;
- c) On or about June 19, 2017, approximately 418.51177 bitcoins were seized from Bitcoin wallet address 12EZr5x8mFpxS6ypNobhPXmyj4BbRkm6GW (the "Bitcoin m6GW Wallet").

d) On or about June 16, 2017, approximately 221.76 bitcoins formerly held in the Bitcoin m6GW Wallet were also seized.

31. Individual 1 confirmed to law enforcement agents that the Ethereum 7800 Wallet, the Bitcoin SYK1 Wallet, and the Bitcoin m6GW Wallet belonged to him or her and held commingled proceeds of computer fraud in violation of 18 U.S.C. § 1030, property involved in money laundering transactions in violation of 18 U.S.C. § 1956, and/or property traceable to such property.

i. Virtual currency formerly held in the Bitcoin m6GW Wallet

32. Bitcoin m6GW Wallet was used by Individual 1 as a passthrough, virtual currency wallet to obscure the true origins of his or her Dark Web computer fraud proceeds.

33. Between on or about October 4, 2014 and May 5, 2017, Individual 1 conducted approximately 3,370 transactions using the Bitcoin m6GW Wallet, receiving a total of approximately 1,399 bitcoins and sending a total of approximately 1,398 bitcoins during this time period.

34. Blockchain analysis of the bitcoins received in the Bitcoin m6GW Wallet showed that approximately ninety-six (96) percent of the bitcoins received came from addresses associated with Dark Web marketplaces or exchanges. Over fifty (50) percent of outgoing transfers were made to peer-to-peer exchanges, including to LocalBitcoins.com.

35. After law enforcement seized approximately 640.26804512 bitcoins from the Bitcoin m6GW Wallet in or around June 2017, a number of “forks” took place in the Bitcoin protocol, which created new derivative virtual currencies.

36. Similar to the proverbial “fork in the road,” a fork in the blockchain of a virtual currency is essentially a change to a network’s protocol. The changes, which are typically initiated

by developers or members of the virtual currency's community, are done in order to add new features and/or improve the ecosystem of that virtual currency. This change creates a "fork" in the blockchain: one path follows the new, upgraded blockchain, and the other path continues along the old path.

37. The developers of Bitcoin Cash, Bitcoin Gold, and Bitcoin SV created new networks from the Bitcoin protocol, and any individuals owning bitcoins prior to the fork are entitled to receive an equivalent amount in the new derivative virtual currency. Because Bitcoin is decentralized, it continues to operate using the original protocol. Further, each derivative virtual currency created has a "legacy address" that corresponds to the Bitcoin wallet address from which it is derived.

38. Blockchain data confirms that approximately 640.2716098 Bitcoin Cash, approximately 640.2715428 Bitcoin Gold, and approximately 640.2716043 Bitcoin SV are all derived from the same legacy Bitcoin wallet address, the Bitcoin m6GW Wallet.

ii. Approximately 919.30711258 ether coins seized from the Ethereum 7800 Wallet

39. Pursuant to the search warrant, law enforcement agents also recovered Individual 1's laptop computer from the Parkland Residence. Through an analysis of the laptop, agents learned that Individual 1 owned the Ethereum 7800 Wallet, which contained approximately 919.30711258 ether coins.

40. Individual 1 told law enforcement agents that he or she obtained the ether in the Ethereum 7800 Wallet by converting bitcoins earned from unlawful online Dark Web transactions involving the sale of hacked online account information. Individual 1 converted the bitcoins to ether using a virtual currency exchange ("Virtual Currency Exchange 1") that did not require users to provide personal identifying information until in or around 2019, thus, providing an additional

layer of anonymity.

41. By exchanging bitcoin for ether, which obscures blockchain tracing analysis, Individual 1 utilized the “chain hopping” technique to further disguise and conceal the nature, location, source, ownership, and control of the illicit proceeds derived from computer fraud.

42. Law enforcement agents were able to confirm that Individual 1 exchanged bitcoins obtained from Dark Web marketplaces to the ether held in the Ethereum 7800 Wallet through an analysis of the blockchain history for both the Ethereum 7800 Wallet and Bitcoin m6GW Wallet, the transactional activity at Virtual Currency Exchange 1, and historical exchange rates for the transaction dates.

43. A review of the Ethereum blockchain history showed that approximately 919.30711258 ether was deposited into the Ethereum 7800 Wallet via nine (9) transactions between on or about March 16 and 17, 2017. These deposits traced back to a known Ethereum address associated with Virtual Currency Exchange 1.

44. Further, a review of the blockchain Bitcoin history showed that approximately thirty-two (32) bitcoins were sent via nine (9) transactions from the Bitcoin m6GW Wallet to other Bitcoin addresses, and from those addresses, transfers were made to Virtual Currency Exchange 1.

45. When these blockchain histories were compared with historical exchange rates, the same transfer amounts for the nine (9) transactions were shown on each respective blockchain, further confirming that bitcoins from the Bitcoin m6GW Wallet were converted to the ether coins eventually seized from the Ethereum 7800 Wallet.

iii. Approximately 2.65995166 bitcoins formerly held in the Bitcoin SYK1 Wallet

46. In addition, Individual 1 was a known vendor on AlphaBay, an online Dark Web marketplace. Individual 1 told law enforcement agents that he or she only sold hacked online account information on AlphaBay.

47. AlphaBay vendors had access to a virtual wallet within the marketplace to store the proceeds from their sales. With cooperation from Individual 1, law enforcement agents “cashed out” his or her AlphaBay account that contained computer fraud proceeds, and Individual 1’s illicit proceeds were pooled in Bitcoin SYK1 Wallet.

48. Later, approximately 2.65995166 bitcoins formerly held in the Bitcoin SYK1 Wallet were seized by law enforcement.

IV. BASIS FOR FORFEITURE

49. Pursuant to 18 U.S.C. § 981(a)(1)(A), “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of [a federal money laundering offense, 18 U.S.C. § 1956], or any property traceable to such property” is subject to forfeiture to the United States.

50. Pursuant to 18 U.S.C. § 981(a)(1)(C), “[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of . . . any offense constituting ‘specified unlawful activity’ . . . , or a conspiracy to commit such offense” is subject to forfeiture to the United States.

51. A “specified unlawful activity” is defined in 18 U.S.C. § 1956(c)(7) to include, among other things, computer fraud in violation of 18 U.S.C. § 1030.

52. Pursuant to 18 U.S.C. § 1030(a)(6)(A), it is unlawful to, knowingly and with intent to defraud, traffic in any password or similar information through which a computer may be accessed without authorization if such trafficking affects interstate or foreign commerce.

FIRST CLAIM
Computer Fraud Proceeds
(18 U.S.C. § 981(a)(1)(C))

53. The factual allegations in paragraphs 1 to 52 are re-alleged and incorporated by reference herein.

54. As set forth above, the Defendant Virtual Currency constitutes or was derived from proceeds traceable to a federal computer fraud offense in violation of 18 U.S.C. § 1030.

55. Accordingly, the Defendant Virtual Currency is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

SECOND CLAIM
Property Involved in Money Laundering
(18 U.S.C. § 981(a)(1)(A))

56. The factual allegations in paragraphs 1 to 52 are re-alleged and incorporated by reference herein.

57. As set forth above, the Defendant Virtual Currency was involved in money laundering transactions or attempted transactions in violation of a federal money laundering offense, 18 U.S.C. § 1956, and/or constitute property traceable to such property.


58. Accordingly, the Defendant Virtual Currency is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

WHEREFORE, Plaintiff, the United States of America, requests that the Clerk of the Court issue a warrant for the arrest of the Defendant Virtual Currency; that notice of this action be provided to persons known or thought to have an interest in or right against the Defendant Virtual

Currency; that the Defendant Virtual Currency be forfeited and condemned to the United States of America; and for such other and further relief as this Court may deem just, necessary and proper.

Respectfully submitted,

JUAN ANTONIO GONZALEZ
ACTING UNITED STATES ATTORNEY

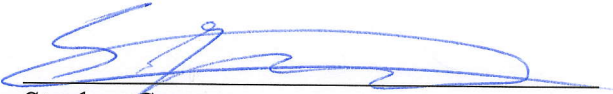
By: 
Mitchell Hyman
Assistant United States Attorney
Florida Bar No. 125405
U.S. Attorney's Office
99 Northeast Fourth Street, 7th Floor
Miami, Florida 33132-2111
Telephone: (305) 961-9283
Email: Mitchell.Hyman@usdoj.gov

VERIFICATION

I, Stephan George, hereby verify and declare, under penalty of perjury, that I am a Special Agent with the Internal Revenue Service Criminal Investigation (“IRS-CI”), and that the foregoing factual allegations are true and correct to the best of my knowledge and belief.

The sources of my knowledge and information and the grounds of my belief are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent of the IRS-CI.

Executed on this 18th of October 2021.


Stephan George
Special Agent, IRS-CI

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.) NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.

I. (a) PLAINTIFFS

UNITED STATES OF AMERICA

DEFENDANTS

APPROXIMATELY 919.30711258 ETHER COINS SEIZED FROM ETHEREUM WALLET ADDRESS 0x71949d87258c4ca6827730c337f80907d73c7800, et al.,

(b) County of Residence of First Listed Plaintiff (EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys (Firm Name, Address, and Telephone Number) AUSA Mitchell Hyman, 99 NE 4 Street, Miami, FL 33132 Telephone: 305-961-9283

Attorneys (If Known) David Howard, Attorney at Law, 25 SE 2nd Ave, Suite 1105, Miami, FL 33131, Telephone: 786-350-6056

(d) Check County Where Action Arose: MIAMI-DADE MONROE BROWARD PALM BEACH MARTIN ST. LUCIE INDIAN RIVER OKEECHOBEE HIGHLANDS

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff Federal Question (U.S. Government Not a Party)
2 U.S. Government Defendant Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State Citizen of Another State Citizen or Subject of a Foreign Country
Incorporated or Principal Place of Business In This State Incorporated and Principal Place of Business In Another State Foreign Nation

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Grid of categories: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, PERSONAL INJURY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, LABOR, IMMIGRATION, FORFEITURE/PENALTY, SOCIAL SECURITY, FEDERAL TAX SUITS, BANKRUPTCY, OTHER STATUTES.

V. ORIGIN

- 1 Original Proceeding 2 Removed from State Court 3 Re-filed (See VI below) 4 Reinstated or Reopened 5 Transferred from another district (specify) 6 Multidistrict Litigation Transfer 7 Appeal to District Judge from Magistrate Judgment 8 Multidistrict Litigation - Direct File 9 Remanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S)

(See instructions): a) Re-filed Case YES NO b) Related Cases YES NO JUDGE: DOCKET NUMBER:

VII. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause (Do not cite jurisdictional statutes unless diversity):

18 U.S.C. § 981(a)(1)(A) and (C) Forfeiture in Rem Action LENGTH OF TRIAL via 5 days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23 DEMAND \$ CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

DATE 10/21/2021 SIGNATURE OF ATTORNEY OF RECORD Mitch Hyman

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.

UNITED STATES OF AMERICA,

Plaintiff,

vs.

APPROXIMATELY 919.30711258 ETHER COINS
SEIZED FROM ETHEREUM WALLET ADDRESS
0x71949d87258c4ca6827730c337f8090
7d73c7800

APPROXIMATELY 2.65995166 BITCOINS
FORMERLY HELD IN BITCOIN WALLET ADDRESS
16qq4DGd2R9vcK5xmV5nRQmoZn2WZVSYK1; AND

ALL VIRTUAL CURRENCY SEIZED ON OR
ABOUT JUNE 16, AND 19, 2017, AND FORMERLY
HELD IN BITCOIN WALLET ADDRESS
12EZr5x8mFpxS6ypNobhPXmyj4BbRkm6GW,
INCLUDING, BUT NOT LIMITED TO,
APPROXIMATELY 640.26804512 BITCOINS;
APPROXIMATELY 640.2716098 BITCOIN CASH;
APPROXIMATELY 640.2715428 BITCOIN GOLD;
AND APPROXIMATELY 640.2716043 BITCOIN SV,

Defendants *In Rem*.

WARRANT OF ARREST IN REM

**TO: FEDERAL BUREAU OF INVESTIGATION, INTERNAL REVENUE SERVICE,
OR ANY OTHER AUTHORIZED FEDERAL LAW ENFORCEMENT OFFICER**

WHEREAS, on October 21, 2021 the United States of America filed a Verified
Complaint for Forfeiture *In Rem* against the above-captioned defendant property; and

WHEREAS, according to said Complaint, the defendant property is in the Government's
possession, custody or control; and

WHEREAS, Supplemental Rule G(3)(b)(i) provides that “the clerk must issue a warrant to arrest the property if it is in the government’s possession, custody or control.”

NOW THEREFORE, you are hereby commanded to take the defendant property into your possession for safe custody. If the character or situation of the defendant property is such that the taking of actual possession is impracticable, you shall execute this process by affixing a copy thereof to the property in a conspicuous place and by leaving a copy of the Complaint and process with the person having possession or his agent.

YOU ARE FURTHER commanded to cite and admonish the owner and/or possessor of the defendant property and any person or firm known to claim any interest therein, to file, **no later than 35 days from the date notice was sent**, a Verified Claim in accordance with Rule G(5) of the Supplemental Rules for Certain Admiralty and Maritime Claims; to therewith or within twenty (20) days thereafter file an Answer or other responsive pleading to the Complaint, a copy of which Complaint you shall supply with this Warrant; to file the Claim and Answer or other responsive pleading with the **Clerk of the Court**, United States District Court, 299 East Broward Boulevard #108, Fort Lauderdale, FL 33301 and to send a copy of said Claim, Answer or responsive pleading, to **Mitchell Hyman, Assistant United States Attorney** 99 N.E. 4th Street, 7th Floor, Miami, Florida 33132; the Claim must identify the specific property claimed, identify the claimant and state the claimant’s interest in the property and be signed by the claimant under penalty of perjury, and that upon the failure of the owner, possessor or any party claiming an interest in the Defendant property to comply with Supplemental Rule G, the Defendant property may be forfeited to the United States by default and without further notice or hearing.

[Intentionally Left Blank]

AND YOU ARE FURTHER commanded to make due and prompt return of this Warrant to this Court upon its execution.

ANGELA E. NOBLE, CLERK
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

DATED: _____

By: _____
DEPUTY CLERK

cc: AUSA Mitchell Hyman

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.

UNITED STATES OF AMERICA,

Plaintiff,

vs.

APPROXIMATELY 919.30711258 ETHER COINS
SEIZED FROM ETHEREUM WALLET ADDRESS
0x71949d87258c4ca6827730c337f8090
7d73c7800, *et al.*,

Defendants *In Rem.*


CIVIL COMPLAINT COVER SHEET

1. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to August 9, 2013 (Mag. Judge Alicia Valle)? Yes No
2. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to August 8, 2014 (Mag. Judge Shaniek Maynard)? Yes No
3. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to October 3, 2019 (Mag. Judge Jared Strauss)? Yes No

Respectfully submitted,

JUAN ANTONIO GONZALEZ
ACTING UNITED STATES ATTORNEY

By:



Mitchell Hyman
Assistant United States Attorney
Florida Bar No. 125405
U.S. Attorney's Office
99 Northeast Fourth Street, 7th Floor
Miami, Florida 33132-2111
Telephone: (305) 961-9283
Email: Mitchell.Hyman@usdoj.gov