UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, U.S. Attorney's Office 555 Fourth Street, NW Washington, D.C. 20530, Plaintiff, v. 482 BITCOINS SEIZED FROM VIRTUAL CURRENCY EXCHANGE A ACCOUNT ENDING IN 6594 -- and -- 1,721,868 USDT SEIZED FROM VIRTUAL CURRENCY EXCHANGE A ACCOUNT ENDING IN 6594 Defendants In Rem.	Civil Action No. 20-2064

VERIFIED COMPLAINT FOR FORFEITURE *IN REM* AND CIVIL COMPLAINT

COMES NOW, Plaintiff, the United States of America, by and through the United States Attorney for the District of Columbia, and brings this verified complaint for forfeiture in a civil action *in rem* against 482 bitcoins seized from Virtual Currency Exchange A ("VC-A") account ending in 6594 ("Defendant Funds 1") and 1,721,868 tether seized from VC-A account ending in 6594 ("Defendant Funds 2") (collectively the "Defendant Funds"), and alleges as follows:

NATURE OF ACTION AND THE PARTIES

1. This action arises out of an investigation by the U.S. Secret Service ("USSS") of a Ponzi scheme named the Banana Fund, which was operated by a foreign national who currently resides outside the United States ("Person 1").

2. Between approximately December 2016 and March 2018, Person 1 devised and carried out a scheme to defraud using interstate wires. Person 1 represented to potential investors that he was creating a company to facilitate other startup companies through crowdfunding investment and crowdsourcing ideas, represented that investors would receive large multiples of their initial investment as a return on their investment, and represented that earlier investors would realize larger returns. Person 1 advertised his purported business on public internet sites associated with virtual currency and solicited investments in virtual currency.

3. Once Person 1 received funds from investors, he did not use them to create a business as promised. Instead, he used the funds to trade in other virtual currencies for personal profit. In January and March 2018, he offered refunds to investors in an amount far below what he had received and falsely represented that there were no other funds available to repay investors. Shortly thereafter, he attempted to withdraw funds traceable to investors from his virtual currency account for the purpose of purchasing a house.

4. This action relates to the seizure and forfeiture of virtual currency from Person 1's account at a U.S.-based virtual currency exchange, VC-A, which are proceeds of Person 1's scheme to defraud.

5. These transfers were in violation of the wire fraud statute, codified at 18 U.S.C. § 1343, and the federal money laundering statute, codified at 18 U.S.C. § 1956(a)(2)(A).

6. The Defendant Funds are subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 18 U.S.C. § 981(a)(1)(A).

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1345, and 1355.

8. Venue is proper pursuant to 28 U.S.C. § 1395(c) because the Defendant Funds are currently held in the District of Columbia.

DEFINITION OF TERMS

I. BITCOIN

9. Bitcoin[1] is a type of virtual currency, circulated over the Internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

10. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the funds associated with a Bitcoin address. Only the holder of an address' private key can authorize transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time and may use a unique Bitcoin address for each and every transaction.

11. To acquire bitcoin, a typical user purchases them from a virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual

[1] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities.

12. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to-peer Bitcoin network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflects any identifying information about either the sender or the recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

13. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can often use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to, among other recipients, Bitcoin exchangers. Because Bitcoin exchangers generally collect identifying information about their customers, subpoenas or other appropriate legal process submitted to exchangers can, in some instances, reveal the true identity of an individual responsible for a Bitcoin transaction. For this reason, many criminal actors who use bitcoin to facilitate illicit transactions online (*e.g.*, to buy and sell drugs or other illegal items or services) look for ways to gain greater anonymity.

II. TETHER

14. Like Bitcoin, tether (USDT) is a blockchain-based virtual currency, circulated over the Internet. However, unlike Bitcoin, tether is a stablecoin (*i.e.*, is designed to minimize the volatility of its price) backed by tether's reserves in fiat currency. According to its website, Tether is pegged to the dollar (*i.e.*, 1 tether is always valued by Tether at $1).

III. BLOCKCHAIN ANALYSIS

15. As previously stated, it is possible for law enforcement to identify the owner of a particular Bitcoin address by analyzing the blockchain. This analysis can also reveal additional addresses controlled by the same individual or entity. For example, a business owner may create multiple Bitcoin addresses to receive payments from different customers. Then, when the business owner wants to use the bitcoin that he or she has received (*e.g.*, to exchange bitcoin for other currency or to purchase goods or services), the business owner may group those Bitcoin addresses together into a single transaction.

16. While investigating suspicious virtual currency transactions, law enforcement officers frequently use commercial services offered by several different blockchain-analysis companies. These private companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these private companies create large databases that group transactions into "clusters" based on patterns and a variety of heuristics.

III. FACTUAL ALLEGATIONS

A. ESTABLISHMENT OF BANANA FUND SCHEME

17. A white paper is commonly used to show investors the details of an investing scheme.

18. The creator of the Banana Fund published a white paper (the "White Paper"), outlining the fund's mission and business model. The White Paper was available at the official Banana Fund website, www.bananafund.com, which had a link to view and download the White Paper at https://banana.fund/pages/proposal.html.

19. The White Paper contained, among others, the following statements describing the Banana Fund's business and investing model:

> Banana Fund is:
>
> A platform for users to post business projects, and for our crowd to brainstorm, and collaborate with the entrepreneur (for a reward!), to develop the idea, it's documentation, and settings / terms. Aiming to provide complete transparency for all parties, and to create an 'instruction book' for how Banana Fund should build & run the project on behalf of the crowd.
>
> An equity crowdfunding platform, using Bitcoin to finance user projects.
>
> An online marketplace for users to buy/sell their (hopefully) dividend paying positions in user projects, in real-time.
>
> A communications platform, for project managers to share near real-time accounts, and updates, aiming to provide unprecedented levels of operational transparency to their backers. And for the crowd to continually make suggestions, and feedback.
>
> A crowd control platform, where backers have established procedures to vote on any desired changes / evolutions to the businesses, to overrule/change the assigned project manager. It's your business. You're in control! We work for you."
>
> Banana Fund is a business development and management company. We assign each project a manager, and using the project documentation and rules as an instruction book, along with the funding from the crowd - we make that business happen! Contracting Banana Fund staff / expertise where possible, and hiring additional staff specific to requirements of each individual business.

> We basically do all the work, so that the entrepreneur and the crowd don't have to. Yet, they're both still in control. They just delegate the day to day operations / leg work to the assigned project manager (Banana Fund)"
>
> Every project is it's [sic] own completely separate, and registered company; with Banana Fund holding all the actual physical equity by default (as we're the ones that register each business on behalf of the crowd / entrepreneur). Tokens serve as "discount coupons" that can be used to buy (and take delivery of) the equity in your project, for a nominal sum.
>
> The tokens that are listed for sale, as part of the Initial Token Offering, are broken up into 20 blocks. The number of available tokens for sale in each block, are priced as shown in the table above. (Users can buy fractions of a token, rendering the unit prices unimportant). The sum of all tokens sold, equals the funding goal.
>
> Needless to say, the strategy with Initial Token Offerings is to bid as soon as you're able. As the block 1 price is 1/20th of the Block 20 price. Thereby, if you get a $10 bid into block 1, the project funds successfully, and the subsequent marketplace holds its price. [sic] You'll have made 20x your money back ($200) right there. Before the project is even built, or really even started construction!
>
> Any action, or service involving Banana Fund central staff (e.g. HR, project management, design, programming, legal, accounting), will be billed to the project's financing at cost +15%. Hourly rates will be adjusted periodically, to keep up with evolving overheads, etc.

20. The White Paper claimed that investors would, at all times, be able to review the details of their projects in as close to real time as possible. The White Paper also claimed—without proof—that the Banana Fund offered a safety net for circumstances when a project failed or did poorly as a result of financial problems.

21. On December 5, 2016, the Banana Fund platform opened for investments of $10.00.

22. Archived copies of the Banana Fund website confirmed that the Banana Fund was set up to be a crowdfunding platform, providing the first 10,000 users that signed up a pre-bid and option to buy a stake in the Banana Fund platform.

23. According to the White Paper, the more quickly a person bought in, the less expensive the position was. The token marketplace was scheduled to start in January 2017. The White Paper also indicated that the price would then fluctuate according to supply and demand, and individuals would be able to list their tokens for sale at market rates.

24. A review of the Banana Fund website revealed that no such token marketplace started in January 2017, or in the subsequent months.

25. VC-A records revealed a cluster of Bitcoin addresses that received funds from Banana Fund victims. Person 1 transferred the victims' funds to another VC-A account ending in 6594 (the "Subject Account").

26. Person 1 registered the Subject Account to a residential address in Toledo, Spain. The know-your-customer information for the Subject Account contained Person 1's email address, a scanned copy of Person 1's passport, and a photograph of Person 1 holding the passport.

27. Publicly available website registration data revealed that the Banana Fund website was registered to Person 1, under the same residential address in Toledo, Spain that Person 1 provided VC-A when registering the Subject Account.

28. On January 14, 2017, Person 1 posted the following publicly available statement to a virtual currency forum:

> The website is all under construction…it's not pre-launch for nothing. Read the whitepaper, and see what we're actually working towards. If you don't believe in the project, or me, then fine. Watch others earn. I will hit a 20 million valuation this year, and anyone buying into the initial offering should be good for 20x their money back. Mark my words, even if you have no intention of acting on them.

29. On January 18, 2017, Person 1 responded to several posts where people challenged the legitimacy of the Banana Fund platform and labeled it a scam. Person 1 responded:

> the money exits, but what difference does it make, you say they don't exist, so you wont invest, you call me a scammer, so even if they exist, you wont invest. If

> you're all so smart….why not click on one of the transactions shown on the stats page and follow the money on the blockchain. It all ends up in just a handful of cold storage wallets. Why do you need me to tell you? The blockchain is there for a reason. Public record. You're all focusing on such silly things…you should be reading the whitepaper and scrutinizing the actual business model. And check out my facebook to see who I am, and the following I have. And you'll see what people are backing me.

30. On January 20, 2017, Person 1 posted a message on the same forum stating:

> here are the bulk of the funds: 346.89 BTC https://blockchain.info/address/13xKsaZxS597SJorAxATBmqu9tzLzrps88. There's another 34 BTC on my exchange account. Some scraps in hot wallet. And the remainder has applied already…once the website is built, you'll be able to see all the invoices billed against dev funding.

The website link in the post directed viewers to Blockchain.info, a publicly available site for viewing Bitcoin transactions on the blockchain.

31. On January 20, 2017, the Bitcoin address viewable at the provided Blockchain.info link received its first deposit of 346 bitcoins, which indicates that Person 1 made the transfer in response to people questioning him about the legitimacy of the project.

32. On January 25, 2017, Person 1 posted in the forum that the same Bitcoin address was at "642 BTC and rising!" A USSS financial analyst reviewed the blockchain and observed that this Bitcoin address had a value of approximately 547 bitcoins.

33. A review of transactional activity for the Subject Account revealed that it was funded primarily via incoming transfers from several Bitcoin clusters. One of these clusters (the "Primary Banana Fund Cluster") was mostly active between December 2016 and April 2017, when it received approximately 500 bitcoins.

34. Despite having significant investment funds in 2017, bank records and virtual currency transactions indicate that Person 1 did not appear to spend those funds on business endeavors for a year, after which he publicly announced that investors would receive limited

refunds that were well below the total value of currency that Person 1 had received. In other words, investors would have netted greater wealth by simply holding onto their bitcoins, which steadily increased in value during the period of the fraud scheme.

B. PERSON 1 LAUNDERED THE VICTIMS' FUNDS

35. Blockchain analytical tools indicated that the Primary Banana Fund Cluster was funded via multiple different sources, including victims at various Bitcoin exchanges.

36. Records from another U.S.-based virtual currency exchange ("VC-B") confirmed that multiple victims contributed to the Primary Banana Fund Cluster. VC-B allowed users to provide "tags" for payments, that is, notes or comments in VC-B's systems regarding individual transactions. Several VC-B customers tagged their payments to the Primary Banana Fund Cluster with variations of the Banana Fund name.

37. The user in control of the Primary Banana Fund Cluster liquidated its holdings at various points and frequently laundered funds to four different locations:

a. Approximately 94 bitcoins to a cluster labeled "Funnel Cluster #1";

b. Approximately 58 bitcoins to a cluster labeled "Funnel Cluster #2" which forwarded approximately 57 bitcoins to "Funnel Cluster #1";

c. Funnel Cluster #1, Funnel Cluster #2, and two other sources combined to send approximately 206 bitcoins to "Funnel Cluster #3," which subsequently received another approximately 283 bitcoins; and

d. Approximately 30 bitcoins to BTC-e, an exchange that catered to cybercriminals and was shut down by law enforcement in mid-2017.

38. Funnel Cluster #3 was primarily funded by bitcoin that originated from the Primary Banana Fund Cluster, which in turn was funded by victims who invested in the Banana Fund.

39. Person 1 liquidated the entire balance of Funnel Cluster #3 as follows:

a. On March 5, 2017, Person 1 transferred approximately 200 bitcoins from Funnel Cluster #3 to the Subject Account; and

b. On March 17, 2017, Person 1 transferred approximately 360 bitcoins from Funnel Cluster #3 to the Subject Account.

40. In March 2017, Person 1 began trading victims' funds across at least seven different kinds of virtual currencies via the Subject Account at VC-A.

a. In approximately two weeks of trading in March, Person 1 generated approximately $540,000 in profit from this virtual currency trading/speculation.

b. Person 1 engaged in such trading largely to enrich himself using the victims' funds as capital for his virtual currency trading/speculation.

c. Between March 2017 and February 2018, Person 1 conducted approximately 40,000 trades of virtual currency as part of this self-enrichment scheme.

d. The balance of the Subject Account appreciated as Person 1 conducted such trades; however, the victims generally did not receive the benefit of this increased value.

C. THE REFUND SCHEME

41. On or about January 2, 2018, www.bananafund.com began redirecting to a "Google Docs" page – that is, a document hosted by Google and associated with a particular Google account whose owner can share access with others – which noted that the Banana Fund had failed. The page directed victims to input their information in order to receive a refund of their original investment. Person 1 stated that due to the increased value of bitcoin, investors would receive more than their initial investment in U.S. dollars, although, realistically, they would all still lose money because of the increased value of bitcoin.

a. For example, if a victim invested one bitcoin in the Banana Fund on X date, when one bitcoin was worth $1,000, Person 1 was now promising a refund on Y date of up

to $4,000, even though one bitcoin was worth $10,000 at that time. Thus, victims suffered substantial losses, while Person 1 was trading on the increased value of bitcoin to enrich himself.

42. Person 1 stated that the rate of return for the refund would depend on how many victims drew from the pool of "$1.73 million" that Person 1 claimed to have on hand. Person 1 promised victims that:

> Refunds will then be paid asap (from the first week of March). Depending on how many there are, it may take me a while to send all the payments. But I'll keep you updated every step of the way; and post all the proofs of payment.
>
> All the funds are presently in Payeer (USD) and USDT (Tether). So it doesn't matter what Bitcoin does in the meantime. The refunds are now set.

43. VC-A records revealed, however, that in the weeks and months leading up to placing funds into USDT, Person 1 was actively buying and selling multiple coins with investor funds for personal gain. For example, following the deposits of 559 bitcoins that were traced to victims investing in the Banana Fund, Person 1 began executing thousands of buy and sell orders.

44. Person 1 falsely claimed that he only had $1,730,000 available to refund investors, when, in fact, the Subject Account had a balance of approximately $11,000,000. Larger refunds were therefore available for victims to the scheme; however, Person 1 concealed this from them.

45. In February 2018, shortly after promising to refund money to the Banana Fund victims, Person 1 contacted VC-A customer service to request approval to withdraw over 100 bitcoins from the Subject Account so that he could purchase a house.

46. By March 2018, the above-referenced Google Docs page had been updated and stated that the deadline to submit refund requests was "extended by 1 week," and that "$1,730,000 USD are available for refunds, and will be divided between all valid requests." Person 1 admitted that this would not "be a full bitcoin for bitcoin refund, as funds were spent, and that money just

isn't there. However; it should work out to something like 4x what you originally invested in dollars."

47. Person 1 promised to begin paying victims "as fast as i'm [sic] able," which would "average out at $50,000+ or so per week."

48. Person 1 failed to repay the vast majority of victims.

D. THE DEFENDANT FUNDS

49. Person 1 publicly stated that all 557 bitcoins in the Subject Account were Banana Fund investor proceeds.

50. As a result, law enforcement seized all available bitcoins from the Subject Account that were traceable to the Banana Fund scheme.

51. At the time of that seizure, Person 1 had drawn the balance down in VC-A to 482 bitcoins, which represents Defendant Funds 1.

52. Person 1 also publicly stated that he held $1,730,000 in victim funds, which he was supposed to refund to Banana Fund victims. As a result, law enforcement seized 1,721,868 USDT from the Subject Account, all of which was traceable to the Banana Fund scheme. These funds represent Defendant Funds 2.

IV. COUNTS

COUNT ONE -- FORFEITURE
(18 U.S.C. § 981(a)(1)(C))

53. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 52 as if fully set forth herein.

54. Person 1 knowingly executed a scheme or artifice to defraud or obtain money or property by means of false or fraudulent pretenses, representations, or promises via wire communications in violation of 18 U.S.C. § 1343.

55. As such, the Defendant Funds are subject to forfeiture, pursuant to 18 U.S.C. § 981(a)(1)(C), as property which constitutes or is derived from proceeds traceable to violations of the wire fraud statute.

COUNT TWO -- FORFEITURE
(18 U.S.C. § 981(a)(1)(A))

56. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 52 above as if fully set forth herein.

57. Person 1 transmitted and transferred the Defendant Funds to a place inside the United States from or through a place outside the United States and from a place outside the United States to or through a place inside the United States, with the intent to promote the carrying on of violations of 18 U.S.C. § 1343 (relating to wire fraud), in violation of 18 U.S.C. § 1956(a)(2)(A)).

58. As such, the Defendant Funds are subject to forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(A), as property involved in transactions in violation of 18 U.S.C. § 1956(a)(2)(A) and (h), or as any property traceable to such property.

V. PRAYER FOR RELIEF

WHEREFORE, the United States of America prays as follows:

A. that notice issue on the Defendant Funds as described above;

B. that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed;

C. that a warrant of arrest *in rem* issue according to law;

D. that judgment be entered declaring that the Defendant Funds be forfeited to the United States of America for disposition according to law; and

E. that the United States of America be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

MICHAEL R. SHERWIN
Acting United States Attorney, N.Y. Bar No. 4444188

By: _____*/s/Zia M. Faruqui*_____
Zia M. Faruqui, D.C. Bar No. 494990
Jessi Brooks, CA Bar No. 283055
Assistant United States Attorneys
555 Fourth Street, N.W.,
Washington, DC 20530; (202) 252-7566 (main line)

C. Alden Pelker, MD Bar
Jessica Peck, NY Bar 5188248
U.S. Department of Justice, Criminal Division
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005; (202) 514-1026 (main line)

Dated: July 29, 2020

Attorneys for the United States of America

VERIFICATION

I, Andrew Foss, a Special Agent with the U.S. Secret Service, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 29TH day of July, 2020.

/s/ Andrew Foss
Andrew Foss
Special Agent
U.S. Secret Service