

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

_____)	
UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
v.)	
)	
113 VIRTUAL CURRENCY ACCOUNTS,)	Civil Action No. 20-606
)	
-and-)	
)	
33 VIRTUAL CURRENCY ACCOUNTS,)	
)	
Defendants.)	
_____)	

AFFIDAVIT IN SUPPORT OF ISSUANCE OF WARRANT OF ARREST *IN REM*

I, Christopher Janczewski, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I make this affidavit in support of an application for a Warrant of Arrest *in Rem* for the defendant properties in this action (further described in Attachment A), pursuant to Rule G(3)(b)(ii) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions of the Federal Rules of Civil Procedure (“Supplemental Rules”). The defendant properties are: 113 virtual currency accounts and 33 virtual currency accounts (collectively the “Defendant Properties”). There is probable cause to believe that the Defendant Properties are subject to seizure and forfeiture as described herein.

2. I am a Special Agent with the Internal Revenue Service Criminal Investigation Division (“IRS-CI”), and have been so employed since September 2009. As a 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. Prior to my employment as a special agent, I was a revenue agent in the Examination division of the IRS for three years. My education includes a Bachelor's Degree in Accounting from Central Michigan University in Mt. Pleasant, Michigan. As a special agent, I attended approximately 26 weeks of special agent training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, in various aspects of criminal investigations dealing specifically with criminal law, criminal tax law, money laundering, wire fraud, seizure, and various financial investigative techniques. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of arrest and search warrants. I am currently assigned to the Cyber Crimes Unit of the IRS-CI, have received training in criminal schemes perpetrated via the internet, and I hold a Global Information Assurance Certification of Information Security Fundamentals.

3. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who have been involved in this investigation, on materials that I have reviewed, and on my training and experience. Where I have reported statements made by others or from documents that I have reviewed, those statements are reported in substance and in part, unless otherwise indicated.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Because this affidavit is being submitted for a limited purpose, I have not set forth all of the information known to me concerning this investigation. Instead, I have set forth information that I believe to be sufficient to establish probable cause in support of the government's application for a warrant to seize the Defendant Properties.

5. Specifically, based on the facts set forth in this affidavit, there is probable cause to believe that the subjects committed, and conspired to commit, the hacking and theft of virtual currencies in violation of 18 U.S.C. 1343 (relating to wire fraud) and 18 U.S.C. § 1349 (conspiracy to commit the same).

6. Wire fraud is a specified unlawful activity as defined by 18 U.S.C. § 1956(c)(7)(D) and as such, probable cause also exists that the subjects laundered the wire fraud proceeds in violation of 18 U.S.C. § 1956(a)(2)(A) (the international promotional money laundering statute) and operated of an unlicensed money service business in violation of 18 U.S.C. § 1960.

7. Therefore, probable cause exists that the Defendant Properties are subject to forfeiture, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C), as proceeds of the above violations and as property involved in such violations.

8. There is also probable cause to believe that the Defendant Properties are foreign assets or sources of influence of the Democratic People's Republic of Korea (hereinafter, "North Korea"), a state sponsor of terrorism, which has engaged in planning and perpetrating federal crimes of terrorism as defined in 18 U.S.C. § 2332b(g)(5), and is therefore subject to seizure and forfeiture under 18 U.S.C. § 981(a)(1)(G)(i).

II. STATUTORY BACKGROUND

A. Money Transmission Business Regulatory Framework

9. Federal law requires money transmitting businesses to be registered with the Financial Crimes Enforcement Network ("FinCEN"), which is located in the District of Columbia. The failure to register with FinCEN is a federal felony offense.

10. Federal law bars money transmitting businesses from transmitting funds that were known to be derived from a criminal offense or intended to be used to promote unlawful activity.

11. In March of 2013, FinCEN issued guidance “to clarify the applicability of the regulations implementing the Bank Secrecy Act (‘BSA’) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.” March 2013 Guidance at 1, available at <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

12. The March 2013 Guidance confirmed that “[t]he definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies.” *Id.* at 3. “Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.” *Id.*

13. The March 2013 Guidance sets forth the types of virtual currency businesses that must register under the BSA regulations. In particular, it states that an “exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person.” *Id.* at 3. The Guidelines define an “exchanger” as “a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.”

B. Money Laundering

14. 18 U.S.C. § 1956(a)(2)(A) (the international promotional money laundering statute) criminalizes, *inter alia*, transporting, transmitting, and transferring, and attempting to transport, transmit, and transfer a monetary instrument or funds to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity. The funds involved in this international transportation of funds are not required to be proceeds of unlawful activity.

15. Pursuant to 18 U.S.C. § 1956(c)(7)(D), the term “specified unlawful activity,” includes a violations of the wire fraud statute.

16. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

C. Forfeiture

17. This application seeks a seizure warrant under both civil authority, because the Defendant Properties could easily be placed beyond process if not seized by warrant. The Defendant Properties are virtual currencies that could be easily transferred to other parties to elude legal process.

18. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction, in violation of 18 U.S.C. § 1960, or any property traceable to such property is subject to civil forfeiture.

19. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction, in violation of 18 U.S.C. § 1956, or any property traceable to such property is subject to civil forfeiture.

20. On November 20, 2017, the President designated North Korea a state sponsor of terrorism. In so doing, the President noted that, “[i]n addition to threatening the world by nuclear devastation, North Korea has repeatedly supported acts of international terrorism, including assassinations on foreign soil.”

- a. Pursuant to 18 U.S.C. § 981(a)(1)(G)(i), all assets, foreign or domestic, of an organization engaged in planning or perpetrating any federal crime of terrorism (as defined in 18 U.S.C. § 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, are subject to civil forfeiture, as are all assets,

foreign or domestic, affording any person a source of influence over any such entity or organization.

- b. “§ 981(a)(1)(G)(i) covers all property ‘foreign or domestic.’ That is, the statute empowers the government to seek the forfeiture of property outside the United States, which may have never touched the United States. The broad expanse of this language is for forfeiture actions to reach all property of terrorist organizations. This court is the sole jurisdiction where such litigation is properly lodged. 28 U.S.C. § 1355(b)(2).” United States v. One Gold Ring with Carved Gemstone, No. 16-CV-02442-TFH, 2019 WL 5853493, at *1 (D.D.C. Nov. 7, 2019).

21. These money laundering and terrorism forfeiture authorities apply to a larger class of property than just illegally obtained proceeds. Specifically:

- a. Money-laundering based forfeitures are not limited to the proceeds of the crime. Money laundering forfeiture encompasses all property “involved in” the crime, which can include so-called “clean” or “legitimate” money that is comingled with “tainted” money derived from the specified unlawful activity; and
- b. Terrorism-based forfeitures cover the broadest categories of property, as it includes *all* property foreign and domestic, irrespective if the property has any nexus to the crime or the United States.

22. Pursuant to 28 U.S.C. § 1355(b)(1)(A), this Court has venue and jurisdiction over Defendant Properties, because acts or omissions giving rise to the forfeiture occurred in this district, to wit, the subjects of the investigation failed to obtain a money transmitting business license from the Financial Crimes Enforcement Network (“FinCEN”), which is located in the District of Columbia, D.C.

23. Pursuant to 28 U.S.C. § 1355(b)(2), this Court has default venue and jurisdiction over property subject to civil forfeiture that is located in a foreign country or been detained by a foreign authority.

III. PROBABLE CAUSE STATEMENT

24. As demonstrated below, the Defendant Properties are virtual currencies, which were obtained illegally through hacking virtual currency exchanges and finance institutions:

A. Bitcoin and Ethereum

25. Bitcoin (BTC) and Ether (ETH) are pseudonymous virtual currencies. Although transactions are visible on a public ledger, each transaction is referenced by a complex series of numbers and letters (as opposed to identifiable individuals) involved in the transaction. The public ledger containing this series of numbers and letters is called a blockchain. This feature makes BTC and ETH pseudonymous; however, it is often possible to determine the identity of an individual involved in BTC and ETH transactions through several different tools. For this reason, many criminal actors who use BTC and ETH to facilitate illicit transactions online (*e.g.*, to buy and sell drugs or other illegal items or services) look for ways to make their transactions even more anonymous.

26. BTC/ETH addresses are unique tokens; however, BTC/ETH are designed such that one person may easily operate many such accounts. Like an email address, a user can send and receive BTC/ETH with others by sending BTC/ETH to a BTC/ETH address. People commonly have many different addresses, and an individual could theoretically use a unique address for every transaction in which they engage.

27. To spend BTC/ETH held within a BTC/ETH address, the user must have a private key, which is generated when the BTC/ETH address is created. Similar to a password, a private

key is shared only with the BTC/ETH-address key's initiator and ensures secured access to the virtual currency. Consequently, only the holder of a private key for a BTC/ETH address can spend BTC/ETH from the address. A BTC user can also spend from multiple BTC addresses in one transaction; for example, five addresses each holding five BTC can collectively send 25 BTC in a single transaction.

28. Although generally, the owners of BTC/ETH addresses are not known unless the information is made public by the owner (for example, by posting the address in an online forum or providing the BTC/ETH address to another user for a transaction), analyzing the public transaction ledger can sometimes lead to identifying both the owner of an address and any other accounts that the person or entity owns and controls.

29. BTC/ETH are often transacted using a virtual currency exchange, which is a virtual currency trading and storage platform. An exchange typically allows trading between the U.S. dollar, other foreign currencies, BTC, ETH, and other virtual currencies. Many virtual currency exchanges also store their customers' virtual currencies. These exchanges act as money services businesses and are legally required to conduct due diligence of their customers and have anti-money laundering checks in place. Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq.*, and must collect identifying information of their customers and verify their clients' identities.

B. Blockchain Analysis

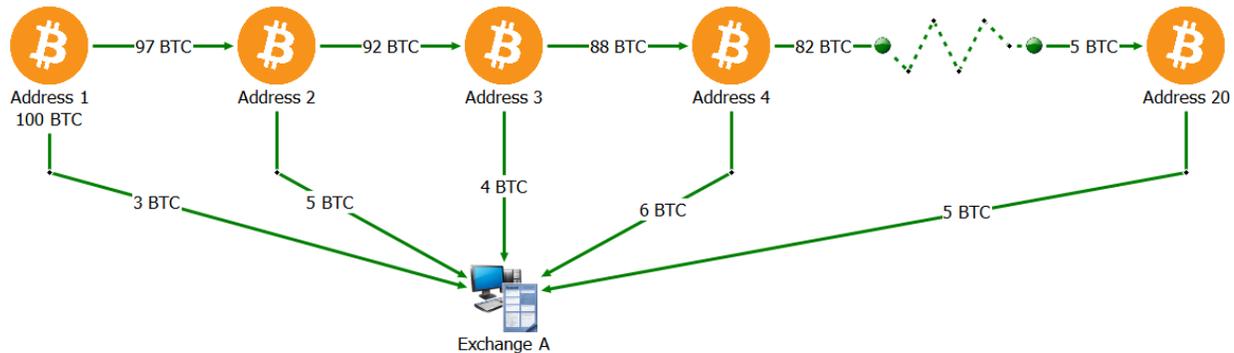
30. While the identity of the BTC/ETH address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular BTC/ETH address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business

may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into “clusters” through analysis of data underlying the virtual currency transactions.

C. Peel Chains

31. A “peel chain” occurs when a large amount of BTC sitting at one address is sent through a series of transactions in which a slightly smaller amount of BTC is transferred to a new address each time. In each transaction, some quantity of BTC “peel off” the chain to another address – frequently to be deposited into a virtual currency exchange – and the remaining balance is transferred to the next address in the chain.

32. The chart below illustrates a simple peel chain example in which a subject seeking to deposit 100 BTC into Exchange A uses a peel chain to make the transaction difficult to track. From left to right, the subject forwards 100 BTC through a series of transactions with 20 peels in inconsistent amounts, ultimately depositing the final five BTC into an exchange, at which point all 100 BTC are deposited.



33. The above chart is a relatively simple example of a peel chain. In practice, sophisticated criminals often use peel chains of hundreds of transactions to obfuscate the path of funds on the blockchain.

D. North Korea’s Hacking of Virtual Currency Exchanges to Create a Source of Influence

34. In its August 2019 report, the Panel of Experts established by the United Nations Security Council to investigate compliance with sanctions against North Korea (“Panel of Experts”) noted how the North Korean government has “used cyberspace to launch increasingly sophisticated attacks to steal funds from financial institutions and cryptocurrency exchanges to generate income.” 2019 Report of the Panel of Experts, at 4.

35. The Panel of Experts investigated:

the widespread and increasingly sophisticated use by the Democratic People’s Republic of Korea of cyber means to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges, launder stolen proceeds and generate income in evasion of financial sanctions. In particular, large-scale attacks against cryptocurrency exchanges allow the Democratic People’s Republic of Korea to generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector. Democratic People’s Republic of Korea cyber actors, many operating under the direction of the Reconnaissance General Bureau, raise money for the country’s weapons of mass destruction programmes, with total proceeds to date estimated at up to \$2 billion.

Id.

36. Based on information provided by member countries and open source reports, the Panel of Experts undertook investigations of at least 35 reported instances of North Korean actors attacking financial institutions, cryptocurrency exchanges, and mining activity designed to earn foreign currency.

37. “With regard to the foreign currency earned through cyberattacks, according to one Member State, ‘These activities contribute to the DPRK’s WMD programme.’ Implementing such attacks is low risk and high yield, often requiring minimal resources (e.g., a laptop and Internet access).” *Id.* at 27. The Panel of Experts further noted that,

Democratic People’s Republic of Korea cyber actors steal cryptocurrency, use it to launder proceeds in evasion of financial sanctions and mine it through cryptojacking attacks for the purposes of revenue generation. According to a Member State, cryptocurrency attacks allow the Democratic People’s Republic of Korea to more readily use the proceeds of their attacks abroad. In order to obfuscate their activities, attackers use a digital version of layering in which they create thousands of transactions in real time through one-time use cryptocurrency wallets. According to that Member State, stolen funds following one attack in 2018 were transferred through at least 5,000 separate transactions and further routed to multiple countries before eventual conversion to fiat currency, making it highly difficult to track the funds.

Id.

38. The Panel of Experts noted that North Korea mostly targets South Korean cryptocurrency exchanges, and launches such hacking campaigns from within North Korea. The Panel of Experts concluded that North Korea’s “cyberattacks on Republic of Korea [South Korean] targets have been increasing in number, sophistication and scope since 2008, including a clear shift in 2016 to attacks focused on generating financial revenue. In 2019, Democratic People’s Republic of Korea cyber actors shifted focus to targeting cryptocurrency exchanges. Some cryptocurrency exchanges have been attacked multiple times.” *Id.*

39. The facts giving rise to this complaint involve the theft of virtual currency by North Korean co-conspirators from four virtual currency exchanges (“The Exchange 1,” “The Exchange

2,” “The Exchange 3,” and “The Exchange 4”), three of which were based in South Korea, and the related laundering of the proceeds.

40. On March 2, 2020, the Department of Treasury’s, Office of Foreign Assets Control, designated the two subjects of this investigation for having provided material support to the Lazarus Group, a North Korean state-sponsored malicious cyber group responsible for North Korea’s malicious cyber activity on critical infrastructure. The designation further noted that North Korea’s malicious cyber activity, which includes cyber intrusions targeting virtual currency exchanges, is a key revenue generator for the regime, and that this revenue allows the North Korean regime to continue to invest in its illicit ballistic missile and nuclear programs.

41. Based on the above facts, there is probable cause to believe that North Korea’s state-sponsored malicious cyber activity, which generates revenue by hacking virtual currency exchanges, and then laundering proceeds, provides a “source of influence” for the regime, including for funding its weapons proliferation program.

E. Money Transmission Business Regulatory Framework

42. Federal law requires money transmitting businesses to be registered with FinCEN. The failure to register with FinCEN is a federal felony offense.

43. Federal law bars money transmitting businesses from transmitting funds that were known to be derived from a criminal offense or intended to be used to promote unlawful activity.

44. In March of 2013, FinCEN issued guidance “to clarify the applicability of the regulations implementing the Bank Secrecy Act (‘BSA’) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.” March 2013 Guidance at 1, available at <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

45. The March 2013 Guidance confirmed that “[t]he definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies.” *Id.* at 3. “Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.” *Id.*

46. The March 2013 Guidance sets forth the types of virtual currency businesses that must register under the BSA regulations. In particular, it states that an “exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person.” *Id.* at 3. The Guidelines define an “exchanger” as “a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.”

F. Hacking and Money Launderings Campaigns

i. Phase One: The Intrusion and Theft

47. In late 2018, IRS-CI’s Cyber Crimes Unit learned that The Exchange 1 had been hacked. The perpetrators of the hack stole nearly \$250 million worth of virtual currencies (as detailed below). The intrusion and subsequent laundering involved numerous electronic communications made in furtherance of the scheme, including e-mail messages and other wire communications related to the intrusion and the submission of false Know-Your-Customer information to various virtual currency exchanges. These communications include wire communications that transited through the United States.

48. In mid-2018, an employee of The Exchange 1 communicated with a “potential client” via email. While communicating with the “potential client,” the employee unwittingly downloaded malware which attacked The Exchange 1.

49. On or about the same day that The Exchange 1 was hacked, a co-conspirator in North Korea researched The Exchange 1 and its CEO. This research, much of which was in Korean, referenced:

- a. Hacking;
- b. Gmail hacker extension;
- c. How to conduct phishing campaigns; and
- d. How to exchange large amounts of ETH to BTC.

50. Ultimately, the malware unwittingly downloaded by The Exchange 1 employee provided remote access to The Exchange 1 and unauthorized access to private keys controlling wallets to multiple virtual currencies.

51. With control of The Exchange 1's private keys, the North Korean co-conspirators stole the following virtual currencies:

<u>Currency</u>	<u>Est. Amount</u>	<u>Est. Dollar Value</u>
BTC	10,777.94	\$94,145,839.41
ETH	218,790	\$131,005,511.85
Zcash (ZEC)	3,783	\$1,020,809.45
Dogecoin (DOGE)	99,999,000	\$560,944.39
Ripple (XRP)	3,043,268	\$2,660,100.78
Litecoin (LTC)	11,000	\$1,639,699.05
Ethereum Classic (ETC)	<u>175,866</u>	<u>\$3,304,763.96</u>
	Total	\$234,337,668.88

52. The North Korean co-conspirators withdrew approximately 10,777.94 BTC from The Exchange 1. Generally speaking, a single deposit of over 10,000 BTC would be easy to trace as it would generate multiple "red flags" for the exchange that received the deposit. Additionally, the exchange receiving the large deposit could freeze the account and leave the hackers with no recourse. Thus, to obfuscate the BTC trail and decrease scrutiny, the North Korean co-conspirators

engaged in hundreds of automated transactions with new BTC addresses as “peel chains” to four different exchanges.

53. The North Korean co-conspirators failed to conduct a peel chain for the LTC they stole from The Exchange 1. Instead they transferred all 11,000 LTC to LLzTJFu3UcwXRrwaq2gLKnJaWWt3oGHVMK (Defendant Property 81).

ii. Initial Laundering of the Proceeds of Phase One via Peel Chains

54. Analysis of the blockchain and additional investigation revealed that over 10,500 of the BTC stolen from The Exchange 1 was deposited primarily into accounts at four virtual currency exchanges (“VCE1,” “VCE2,” “VCE3,” and “VCE4”).

55. Further analysis revealed that a substantial amount of other virtual currencies stolen from The Exchange 1 was also deposited into accounts at VCE1, VCE2, VCE3, and VCE4. In particular, one account at VCE1 (Defendant Property 64) directly received nearly all DOGE and XRP stolen from The Exchange 1.

56. The account at VCE4 into which the funds were laundered controlled the addresses listed as Defendant Properties 98 through 111. This account was the same account that received proceeds from approximately \$30 million worth of virtual currency stolen by North Korean co-conspirators from The Exchange 4, a South Korea-based virtual currency exchange, in or about the summer of 2018.

57. The main account at VCE1 (Defendant Property 64) was registered using an email account from a South Korean engineering company, whose email accounts were compromised by North Korean co-conspirators. In addition to the approximately 5,600.42737261 BTC (\$39,765,175.16), the account received approximately 600.1 ETH, 99,998,987 DOGE, 3,043,200

XRP, and 1,500 ZEC, which were converted to BTC and withdrawn. The South Korean engineering firm was unaware that its infrastructure was being used for this purpose.

58. In an attempt to circumvent VCE1's Know-Your-Customer ("KYC") program, the North Korean co-conspirators submitted two fraudulent identification photos. As depicted below in KYC Photo 1, one photo is of what appears to be an Asian male sitting in a chair holding his South Korean government-issued photo ID in front of his face with two hands. Behind the individual is a computer monitor displaying an encrypted web browser which conceals IP addresses. Metadata from the photo revealed that it was altered.



KYC Photo 1

59. Another account at VCE1 (Defendant Property 63) received approximately 112.047 ETH and converted it to BTC. North Korean co-conspirators also submitted two

fraudulent photos for this account as well, in a continued attempt to circumvent VCE1's KYC policy. As demonstrated below in KYC Photo 2, one photo is of what appears to be a Caucasian male standing behind a computer monitor holding a German government-issued photo ID in front of his face with two hands. The face in the photo is noticeably altered. There are publicly available versions of the photo depicting this person, one of which was used in this photo. The white t-shirt with black writing being worn by the individual is the exact same t-shirt being worn in the photo submitted for the other account. That is, the North Korean co-conspirators used the exact same photo of the body, but added in different photos of the faces when submitting KYC documents.



KYC Photo 2

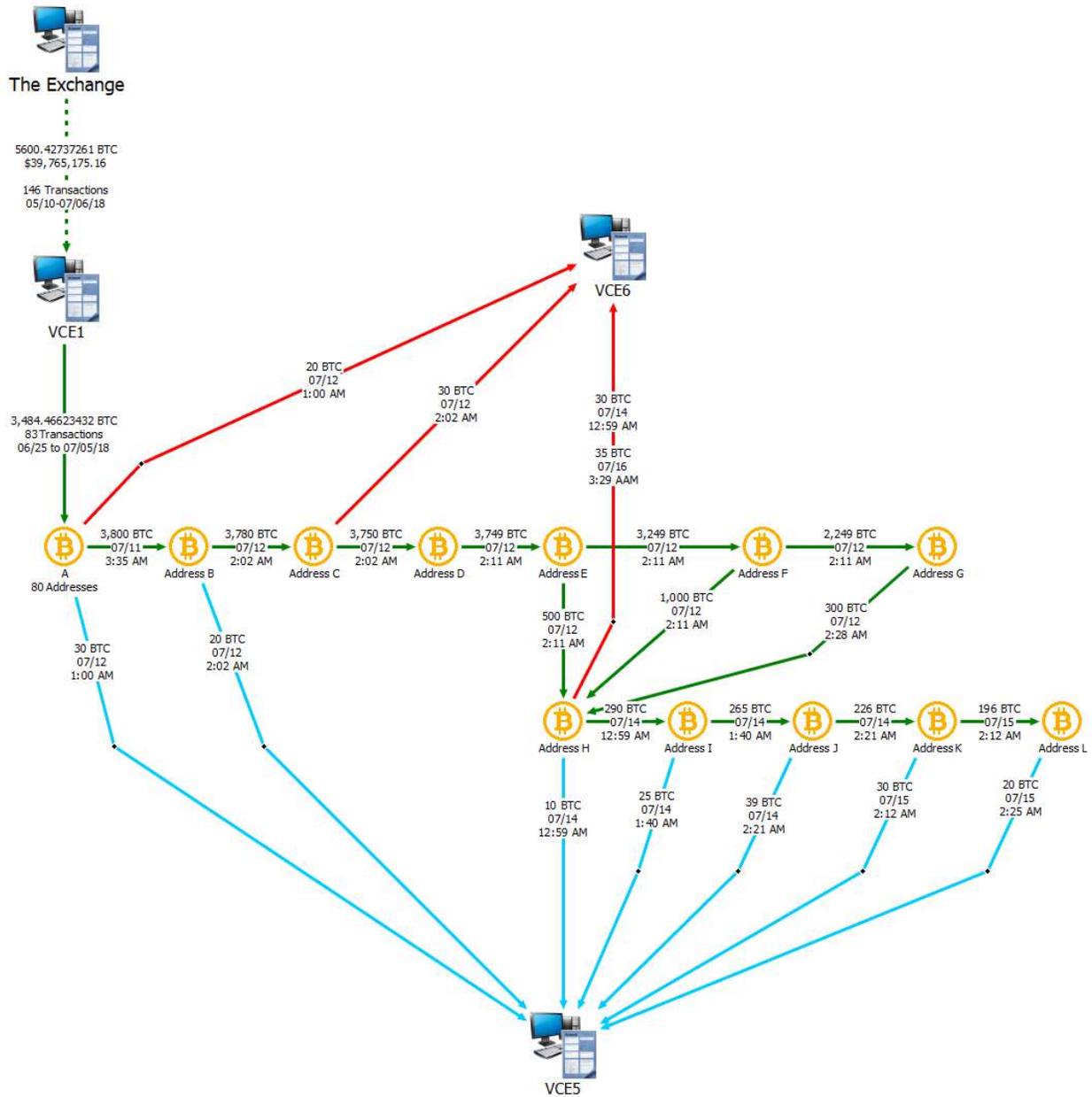
60. The account at VCE3 receiving the 264.454103 BTC (\$1,818,972.13) (which included Defendant Properties 50 through 52) also involved altered KYC photos. One photo is a Caucasian male holding a sheet of paper with the name of VCE3 and the date written on it in one

hand and an Australian passport open to the photo page in the other hand. The face in the photo was noticeably altered. Ultimately, VCE3 was not satisfied with the image and requested a video conference with the account holder, which the account holder refused.

61. An account at VCE2 (Defendant Property 112) received approximately 406.095468 BTC (\$3,408,849.46). This account at VCE2 was linked to the account at VCE4 (which included Defendant Properties 98 through 111) that received BTC from The Exchange 1 and the summer 2018 theft from The Exchange 4. In total, the VCE4 account received approximately 6,138.10855889 BTC (\$46,461.524.35).

62. The BTC received by the accounts was then withdrawn from the four exchanges, and again the North Korean co-conspirators reconstituted the funds by conducting hundreds of transactions with new BTC addresses and multiple peel chains. During this period, additional BTC was included in the layering.

63. Included below as Exhibit 1 is a diagram that details a sample of the larger peel chain that IRS-CI's Cyber Crimes Unit analyzed in the course of the investigation.



64. Exhibit 1 reflects that:

- After The Exchange 1 was hacked, 5,600.42737261 BTC was laundered into an account at VCE1 (Defendant Property 64) via 146 transactions from May 10, 2018 to July 6, 2018.
- The North Korean co-conspirators then laundered 3,484.46623432 BTC (of the approximately 5,600 BTC) to 80 BTC addresses via 83 transactions from June 25,

2018 to July 6, 2018.

July 11, 2018

- On July 11, 2018, at 3:35 am, the subjects then had all 80 addresses transfer 3,800 BTC to Address B.
 - o That is, a review of the blockchain shows the 80 addresses sent the BTC as part of a single transaction to Address B.
 - o Such transactions typically occur when a user storing BTC in software on their computer creates a single transaction to transfer the funds to an exchange so that the user can begin the process of cashing out the BTC for fiat currency.
- The subjects began peeling off bitcoin from this large address and sent it in small transactions to two other virtual currency exchanges (“VCE5” and “VCE6”). Accounts at VCE5 (Defendant Properties 65-70) and VCE6 (Defendant Properties 55-62) received the bulk of the laundered funds from the hack of The Exchange 1. An example of how the funds were laundered into VCE5 and VCE6 is as follows:

July 12, 2018

- At 1:00 am, the subjects laundered 20 BTC from Addresses A to an account at VCE6 (Defendant Property 59).
- At 1:00 am, the subjects laundered 30 BTC from Addresses A to an account at VCE5 (Defendant Property 68).
- At 2:02 am, the subjects peeled off 20 BTC from Address B and laundered it to an account at VCE5 (Defendant Property 68).
- At 2:02 am, the subjects laundered the remaining 3,780 BTC from Address B to Address C.

- At 2:02 am, the subjects peeled off 30 BTC from Address C and laundered it to an account at VCE6 (Defendant Property 59).
- At 2:02 am, the subjects laundered the remaining 3,750 BTC from Address C to Address D.
- At 2:11 am, the subjects peeled off 1 BTC from Address D and laundered it to another address.
- At 2:11 am, the subjects laundered the remaining 3,749 BTC from Address D to Address E.
- At 2:11 am, the subjects peeled off 500 BTC from Address E and laundered it to Address F.
- At 2:11 am, the subjects laundered the remaining 3,249 BTC from Address E to Address G.
- At 2:11 am, the subjects peeled off 1,000 BTC from Address G and laundered it to Address F.
- At 2:11 am, the subjects laundered the remaining 2,249 BTC from Address G to Address H.
- At 2:28 am, the subjects peeled off 300 BTC from Address H and laundered it to Address F.

July 14, 2018

- At 12:59 am, the subjects peeled off 10 BTC from Address H and laundered it to an account at VCE5 (Defendant Property 68).
- At 12:59 am, the subjects peeled off 30 BTC from Address F and laundered it to an account at VCE6 (Defendant Property 57).

- At 12:59 am, the subjects laundered the remaining 290 BTC from Address H to Address I.
- At 1:40 am, the subjects peeled off 25 BTC from Address I and laundered it to an account at VCE5 (Defendant Property 65).
- At 1:40 am, the subjects laundered the remaining 265 BTC from Address I to Address J.
- At 2:21 am, the subjects peeled off 39 BTC from Address J and laundered it to an account at VCE5 (Defendant Property 68).
- At 2:21 am, the subjects laundered the remaining 226 BTC from Address J to Address K.

July 15, 2018

- At 2:12 am, the subjects peeled off 30 BTC from Address K and laundered it to an account at VCE5 (Defendant Property 68).
- At 2:12 am, the subjects laundered the remaining 196 BTC from Address K to Address L.
- At 2:12 am, the subjects peeled off 20 BTC from Address L and laundered it to an account at VCE5 (Defendant Property 68).

July 16, 2018

- At 3:29 am, the subjects peeled off 35 BTC from Address F and laundered it to an account at VCE6 (Defendant Property 58).

65. The transactions that occurred in the peel chain were automated. That is, the North Korean co-conspirators had a computer script that rapidly laundered the BTC to and from addresses and exchanges. In fact, many of the transactions occurred during the same minute. This

is a known tactic used by money launderers when trying to move large amount of BTC rapidly. Because of the complexity of addresses and number of transactions, human error could easily lead to the loss of funds. While a bank can claw back funds sent to an errant address, no such remedy exists for BTC. As such, money launderers use computer programs to ensure precision when transferring in high volumes at a high frequency.

66. The above peel chain analysis is a representative sample of the many peel chains involved in the money laundering scheme. The funds stolen from The Exchange 1 continued to be laundered via hundreds of peel chain transactions largely mirroring those described above, illustrated in substantive part in Exhibit 1. Within the many peel chains, multiple BTC address (Defendant Properties 35-43) maintained a balance of BTC traceable to the theft.

67. **Addendum A** (below) details additional peel chain analysis and recent money laundering subsequent to the publication of the original complaint.

iii. North Korean Attribution and Obfuscation in Phase One

68. Proceeds of the theft of BTC from The Exchange 1 were used to perpetuate additional schemes by paying for infrastructure, to include domain registration for websites like Celas LLC, site hosting from service providers that focus on client anonymity, and virtual private networks. The North Korean co-conspirators sent 0.003526 BTC (\$22.43) of the stolen BTC, which was previously laundered via the peel chain layering process, to pay for the registration of 12 months of business email services for celasllc.com on or about July 11, 2018.

69. The same North Korean co-conspirators registered the domain “celasllc.com.” According to its website, Celas LLC, a/k/a Celas Limited, purported to offer a cryptocurrency-trading platform, called Celas Trade Pro, which could be downloaded from celasllc.com. In

actuality, forensic analysis revealed that Celas Trade Pro was a malicious software code that provided the North Korean co-conspirators direct access to the downloader's system.

70. According to security researchers, Celas LLC shared a server IP address and an encryption key with the known malware named Fallchill. A joint technical alert published by the Department of Homeland Security and the Federal Bureau of Investigation associated Fallchill with the government of North Korea.

71. A specific command line in the Celas Trade Pro application and Fallchill are consistent with North Korean hacking campaigns against the financial industry dating back to 2016.

72. Celas Trade Pro used a language code associated with North Korea.

73. The North Korean co-conspirators caused the upload of a version of Celas Trade Pro to Website A in June 2108, shortly after the application had been compiled. Website A is a website that aggregates many antivirus products and online scan engines to check for viruses. Within minutes of the upload, the North Korean co-conspirators voted on the file as being safe. That is, the North Korean co-conspirators were attempting to see whether the malware would be detected, and then attempted to provide credibility to the program by voting it as safe.

G. Phishing Campaign

74. The North Korean co-conspirators who emailed The Exchange 1 malware were also engaged in a massive phishing campaign in an attempt to infect other users with malware. To provide credibility to the online personas, fake social media profiles were created. For example:

- e. A Twitter account was created with the name "Waliy Darwish" that made various posts related to cryptocurrency and included a link to celasllc.com;

- f. The same user created a LinkedIn page for “Waliy Darwish,” listing him as a business developer at Celas LLC with a bachelor’s degree from Rotterdam University; and
- g. The same user also created a Facebook and Instagram page.

75. The phishing campaign targeted thousands of email accounts at exchanges around the world and personal email accounts of prominent people within the cryptocurrency ecosystem, to include CEOs of major exchanges. The phishing emails were primarily three types: advertisements for Celas LLC; developers looking to work with/for the targeted exchange; or a prospective client. The emails often contained a link to celasllc.com or an attachment. Additionally, the Waliy Darwish LinkedIn account messaged multiple people as well.

76. To aid in the phishing campaign, the North Korean co-conspirators used various email plugins. Plugins are add-on tools that can help with email tracking, task management, and other tasks. Some of the plugins included:

- h. A tool to compose one email that is then automatically individually addressed to many recipients. It also allowed the sender to receive an email notifying them when a recipient has opened and read an email. This email contained the IP address, browser type, and user agent of the recipient.
- i. A tool to customize the email’s signature block with company contact information, pictures, and other information to make an email look professional.
- j. A tool that enables human editors to write and respond to email for a client, ensuring “perfect English.” The editors optimize grammar, punctuation, word choice, sentence rhythm, and tone.

H. Additional Connections to North Korea

77. One of the North Korean co-conspirators who was involved with the conspiracy to deliver the malware to The Exchange 1 researched the following:

- k. North Korea;
- l. North Korean Special Forces and the North Korean military;
- m. the United States military in regard to the North Korean military; and
- n. Kim Jong Un.

78. In spite of using VPN services to mask their addresses, law enforcement was able to trace back logins to an IP address within North Korea.

I. Laundering of Phase One and Phase Two Illicit Proceeds

i. Laundering of Proceeds from Hack of The Exchange 1 (Phase One)

79. Ultimately, after being laundered via hundreds of peel chain transactions, a bulk of the stolen BTC was deposited into four accounts at VCE5 (Defendant Properties 67 and 70) and VCE6 (Defendant Properties 56 and 62).

80. The accounts at VCE5 and VCE6 (Defendant Properties 56, 62, 67, and 70) belonged to "田寅寅" (a/k/a Tian Yinyin) and "李家东" (a/k/a Li Jiadong), also known by their registered usernames "snowsjohn" and "khaleesi" respectively.

81. Tian Yinyin and Li Jiadong are both Chinese nationals with government identification numbers and Chinese phone numbers.

82. Between in or about 2018 through in or about April 2019, Tian Yinyin and Li Jiadong engaged in \$100,812,842.54 in virtual currency transactions, which primarily consisted of their exchange of virtual currency traceable to the hack of The Exchange 1. Tian Yinyin and Li

Jiadong would convert such virtual currency into fiat currency and transfer it to customers, for a fee.

83. Tian Yinyin's and Li Jiadong's virtual currency accounts at VCE5 (Defendant Properties 67 and 70) had multiple connections. The accounts had significant transfers between each other and third party accounts.

84. Tian Yinyin linked a bank account at China Guangfa Bank ("CGB") to his VCE5 account less than a week after the intrusion and theft of The Exchange 1. This CGB account received approximately 491 deposits from VCE5 for 233,889,970 CYN (approximately \$34,504,173.43) and represents proceeds from his money laundering activities.

85. The same CGB bank account was linked to Tian Yinyin's VCE6 account (Defendant Property 62).

86. Tian Yinyin's accounts at VCE5 (Defendant Property 70) and VCE6 (Defendant Property 62) had no deposits for approximately two months prior to the hack of The Exchange 1.

87. Tian Yinyin also had an account at VCE7 (Defendant Property 83, which included the deposit address identified as Defendant Property 84), a U.S.-based exchange, where he sold BTC in exchange for prepaid Apple iTunes gift cards, a known method of money laundering.

88. Tian Yinyin's VCE7 advertisement stated that no ID was necessary for trades.

89. On multiple occasions, Tian Yinyin, using his account at VCE7 (Defendant Property 83), engaged in financial transactions to convert virtual currency to U.S. dollars with customers in the United States.

90. Li Jiadong laundered approximately 9.71443 BTC from his VCE5 (Defendant Property 70) and VCE6 (Defendant Property 62) accounts to Tian Yinyin's account at VCE7 (Defendant Property 83).

91. Tian Yinyin exchanged approximately \$1,448,694.74 worth of BTC for iTunes gift cards via 8,823 transactions from his account at VCE7 (Defendant Property 83).

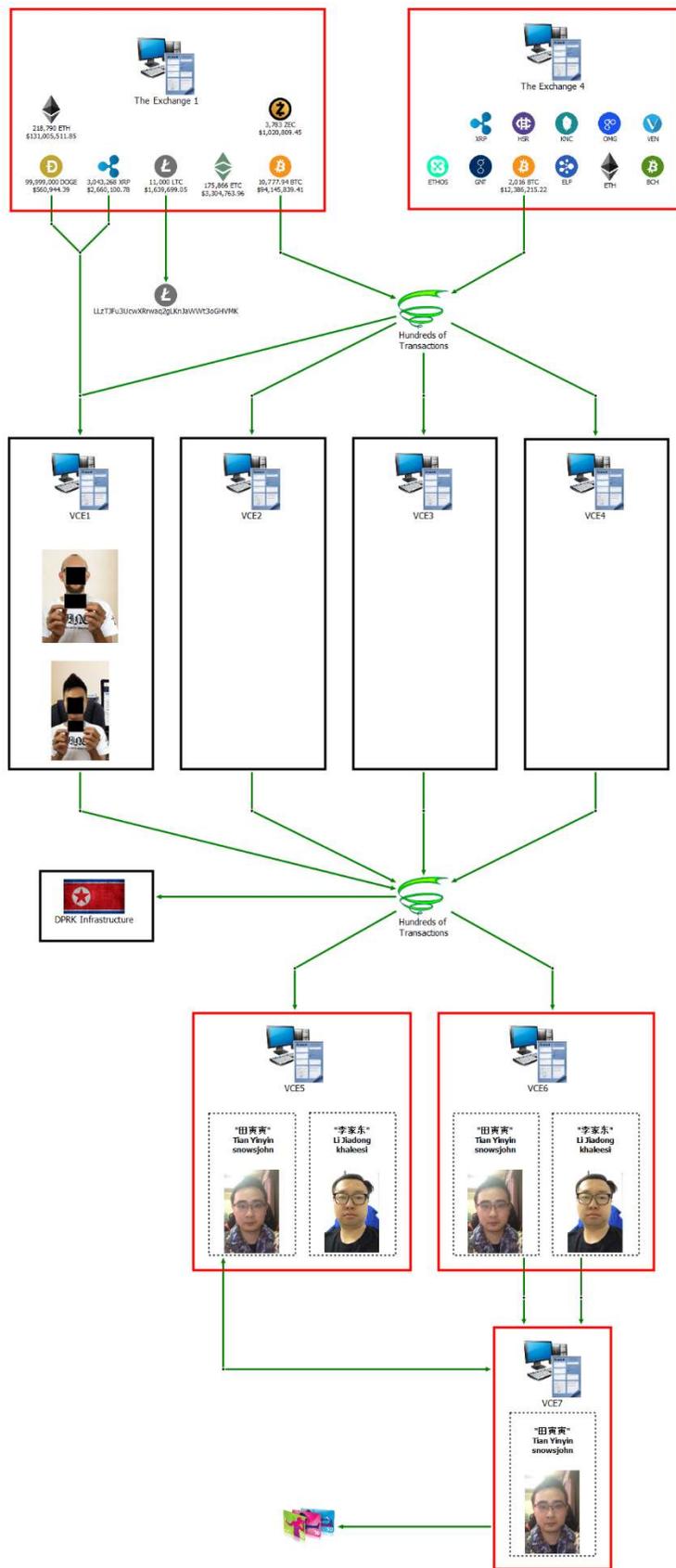
92. Li Jiadong's advertisement on another virtual currency exchange ("VCE8") noted that he was operating a professional business and gave his hours and payment information. Li Jiadong maintained multiple addresses on VCE8, consisting of Defendant Properties 71 through 80.

93. Li Jiadong linked bank accounts at nine Chinese banks—Agricultural Bank of China, China Everbright Bank, China CITIC Bank, CGB, China Minsheng Bank, Huaxia Bank, Industrial Bank, Pingan Bank, and Shanghai Pudong Development Bank—to his VCE5 account (Defendant Property 70). These bank accounts received approximately 2,000 deposits from VCE5 for 229,282,960.97 CYN (approximately \$32,848,567.00) and represent proceeds from his money laundering activities.

94. Tian Yinyin's VCE6 account (Defendant Property 62) sent approximately 25 BTC (approximately \$175,000) to Li Jiadong's VCE5 account (Defendant Property 67).

95. Tian Yinyin and Li Jiadong exchanged approximately 2,165.39 BTC (approximately \$15,529,934.00) and equivalent fiat currency between each other via VCE5.

96. The chart in Exhibit 2, below, depicts an overview of the laundering of funds from the hack of the Exchange 1.



ii. Laundering of Proceeds from the Hack of The Exchange 2 (Phase Two)

97. YINYIN's accounts at VCE5 and VCE6 were also used to launder the proceeds of the hack of The Exchange 2, a South Korea-based virtual currency exchange. Due to the role these funds played in the larger money laundering activity, the activity surrounding this hack is referred to herein as "Phase Two," though it occurred earlier in time than Phase One.

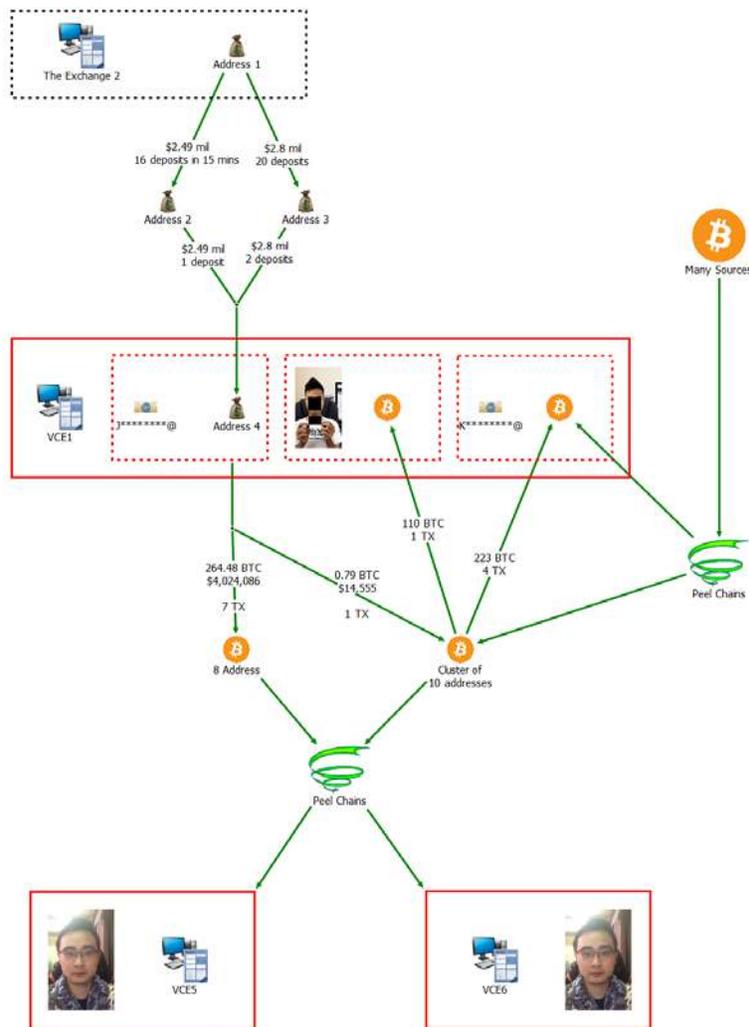
98. On or about December 19, 2017, The Exchange 2 announced through its website and various media outlets that it had been a victim of a hack and subsequent theft of approximately 17% of its total assets.

99. The Panel of Experts subsequently attributed this hack to North Korean actors.

100. At or about the same time of the hack of The Exchange 2, a single virtual currency address at The Exchange 2 routed funds to two addresses in a rapid series of transactions. One address received approximately 16 deposits of the same amount over a period of 15 minutes, totaling approximately \$2.49 million; the second address received approximately 20 deposits totaling approximately \$2.88 million. Later that same day, the originating virtual currency address at The Exchange 2 stopped making withdrawals, just as The Exchange 2 stated it was suspending trading.

101. Almost immediately following the initial withdrawal of the stolen funds from The Exchange 2, the funds were directed to an account at VCE1. At VCE1, the North Korean co-conspirators converted the stolen virtual currency to BTC, withdrew the funds, engaged in multiple peel chains, and ultimately deposited said proceeds into Tian Yinyin's accounts at VCE5 and VCE6, as demonstrated in Exhibit 3, below.

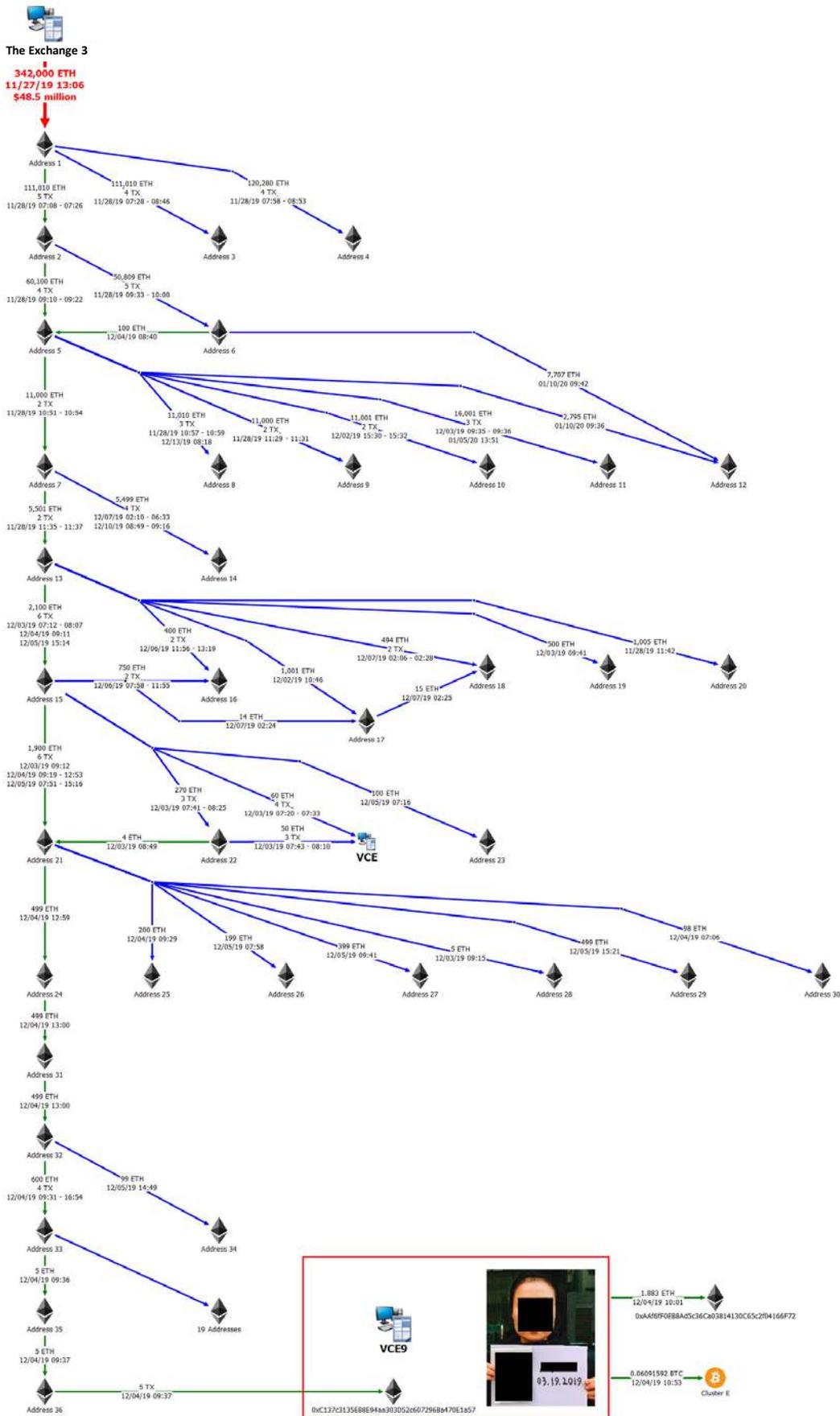
102. While the BTC was being laundered, a portion was sent to a cluster that had sent funds to two North Korean co-conspirator accounts, including Defendant Property 64.



J. Phase Three: The November 2019 Intrusion and Theft

103. On or about November 27, 2019, The Exchange 3, a South Korea-based virtual currency exchange, had approximately 342,000 ETH (\$48.5 million) stolen from it.

104. Over the subsequent few days, the ETH began to umbrella outward via multiple peel chains in attempt to obfuscate the trail before being deposited into various virtual currency exchanges. Exhibit 4, below, illustrates an example of the flow of a portion of stolen ETH from The Exchange 3 into an account at another exchange (Defendant Property 82) via approximately 14 transactions approximately seven days later.



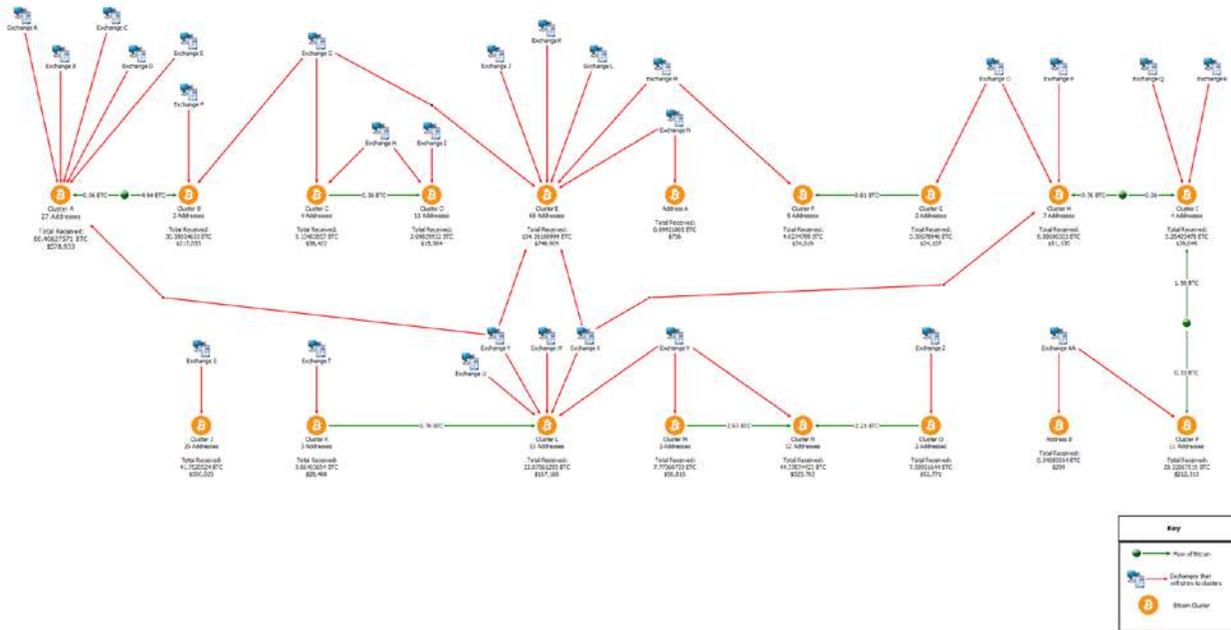
105. Notably, as the ETH splintered from the main trail, portions often circled back and regrouped with the main trail. This reflects that the stolen funds were still controlled by the same North Korean co-conspirators.

106. Ultimately, as shown in Exhibit 4, approximately 5 ETH was deposited into an account at another virtual currency exchange (“VCE9”) (Defendant Property 113) on December 4, 2019. The KYC information for this account reflected a purported South Korean individual.

107. A portion of the deposited ETH was converted into BTC using VCE9’s over-the-counter trading platform. Less than two hours after the ETH was deposited, BTC was withdrawn to a cluster. The deposits to this cluster originated at various exchanges that received stolen ETH that was converted to BTC.

108. By converting ETH to BTC, the North Korean co-conspirators switched the stolen proceeds from the ETH blockchain to the BTC blockchain. One of the primary purposes of doing this was to obfuscate the trail of the funds.

109. Included below as Exhibit 5 is a diagram that illustrates approximately 18 different clusters, comprised of approximately 200 different BTC addresses (including Defendant Properties 1 through 34 and Defendant Property 91), that received 383.79970162 BTC (\$2,781,754.23) from November 29, 2019 through January 4, 2020. Each of these clusters received BTC that was converted from ETH proceeds traced to the theft of The Exchange 3. To further connect these clusters and illustrate the common ownership, the diagram shows how accounts at various exchanges withdrew to multiple clusters listed and some of the clusters exchanged BTC amongst themselves.



110. From these 18 clusters, the subjects began to layer with peel chains and mix the BTC, in order to obfuscate the trail as they converted it to fiat currency. The peel chains from these clusters were connected to each other. Some of the accounts that received the stolen ETH still maintain a balance of stolen virtual currency and are held at various virtual currency exchanges, including VCE 4 (Defendant Properties 92-97), VCE10 (Defendant Properties 44-49), VCE11 (Defendant Properties 85-90), and VCE12 (Defendant Properties 53 and 54).

K. North Korean Attribution and Obfuscation in Phase Three

111. The North Korean co-conspirators' campaign, which included the theft of funds from The Exchange and related money laundering, continued with the theft from The Exchange 3 and related money laundering.

112. North Korean co-conspirators had targeted The Exchange 3 in May 2019, although this previously attempted theft failed. Specifically, emails originating from North Korea falsely gave the impression that The Exchange 3 was requesting information from its customers about a fictional sweepstakes payout.

113. As to the November 2019 theft, the North Korean co-conspirators continued to submit digitally altered KYC photos to virtual currency exchanges. This included by again using publically available photos for identification documents as well manipulating images to circumvent KYC checks.

114. The North Korean co-conspirators logged in from Pyongyang and used North Korean cell phone infrastructure to perpetrate this scheme.

115. The North Korean co-conspirators researched reporting related to the hack of The Exchange 3. In one instance, they researched a cyber security platform that was tracking the ETH stolen from The Exchange 3 to various exchanges and naming such exchanges. Additionally, the North Korean co-conspirators researched hacking tactics in Korean.

L. Failure to Register as a Money Transmitting Business

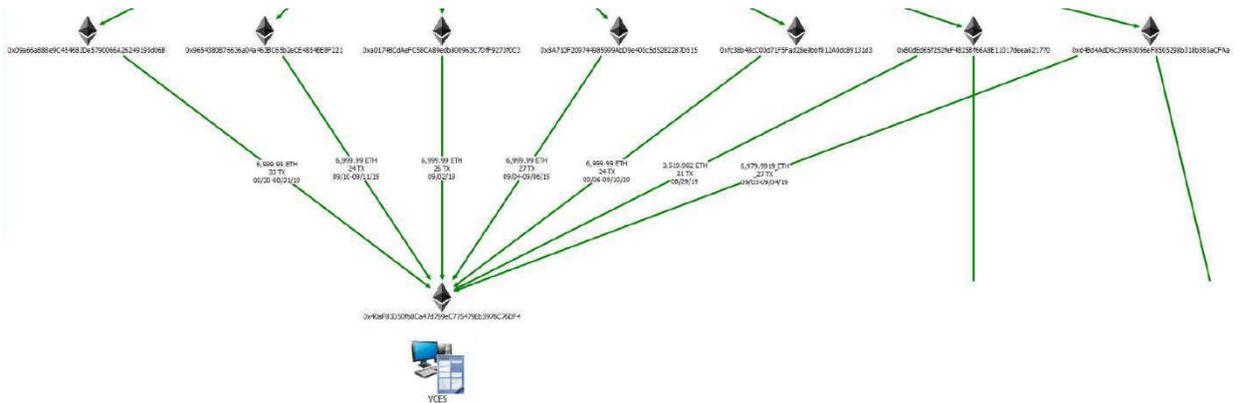
116. As explained in detail above, Tian Yinyin and Li Jiadong engaged in over \$100 million in virtual currency transactions. Tian Yinyin and Li Jiadong's primary source of virtual currency was proceeds of the hacks of virtual currency exchanges, including The Exchange 1 and The Exchange 2.

117. Tian Yinyin and Li Jiadong would convert such virtual currency into fiat currency and transfer it to customers, for a fee. Tian Yinyin and Li Jiadong's business included customers and financial accounts within the United States.

118. Tian Yinyin and Li Jiadong failed to register with FinCEN as money transmitting businesses.

119. Tian Yinyin and Li Jiadong maintained the BTC addresses identified in the property to be forfeited, which represent a portion of the defendant properties, further identified as

125. Following the pattern described in the complaint above, the funds in Defendant Properties 133-139 continued to be routed through a series of transactions in the peel chains, until the North Korean co-conspirators began to reconstitute the funds at a single account at VCE5 (Defendant Property 140). In total, the North Korean co-conspirators laundered 45,499.9239 ETH via 182 transaction to Defendant Property 140. Included below as Exhibit 7 is a diagram of this step in the money laundering process.



126. Between on or about August 28, 2019 and August 31, 2019, the North Korean co-conspirators laundered 8,581.716994 ETH via 150 transactions from Defendant Property 140 to a suspected escrow account at VCE5. These transactions were part of over-the-counter trading the North Korean co-conspirators conducted with suspected co-conspirator money launderers.

127. Defendant Property 140 ceased transactions on or about September 15, 2019, and did not resume laundering the stolen proceeds until March 5, 2020, just after the government filed the instant complaint.

128. Specifically, on March 5 and 6, 2020, the North Korean co-conspirators rapidly laundered approximately 8,758.9978 ETH (\$1,985,800.32) via over 44 transactions from Defendant Properties 115 and 123 (accounts which had been dormant since September 7, 2018) into Defendant Property 140 (their account at VCE5).

129. In turn, the North Korean co-conspirators then laundered these funds from Defendant Property 140 into the escrow account at VCE5.

130. On or about March 5, 2020, the government sought to restrain these funds at VCE5.

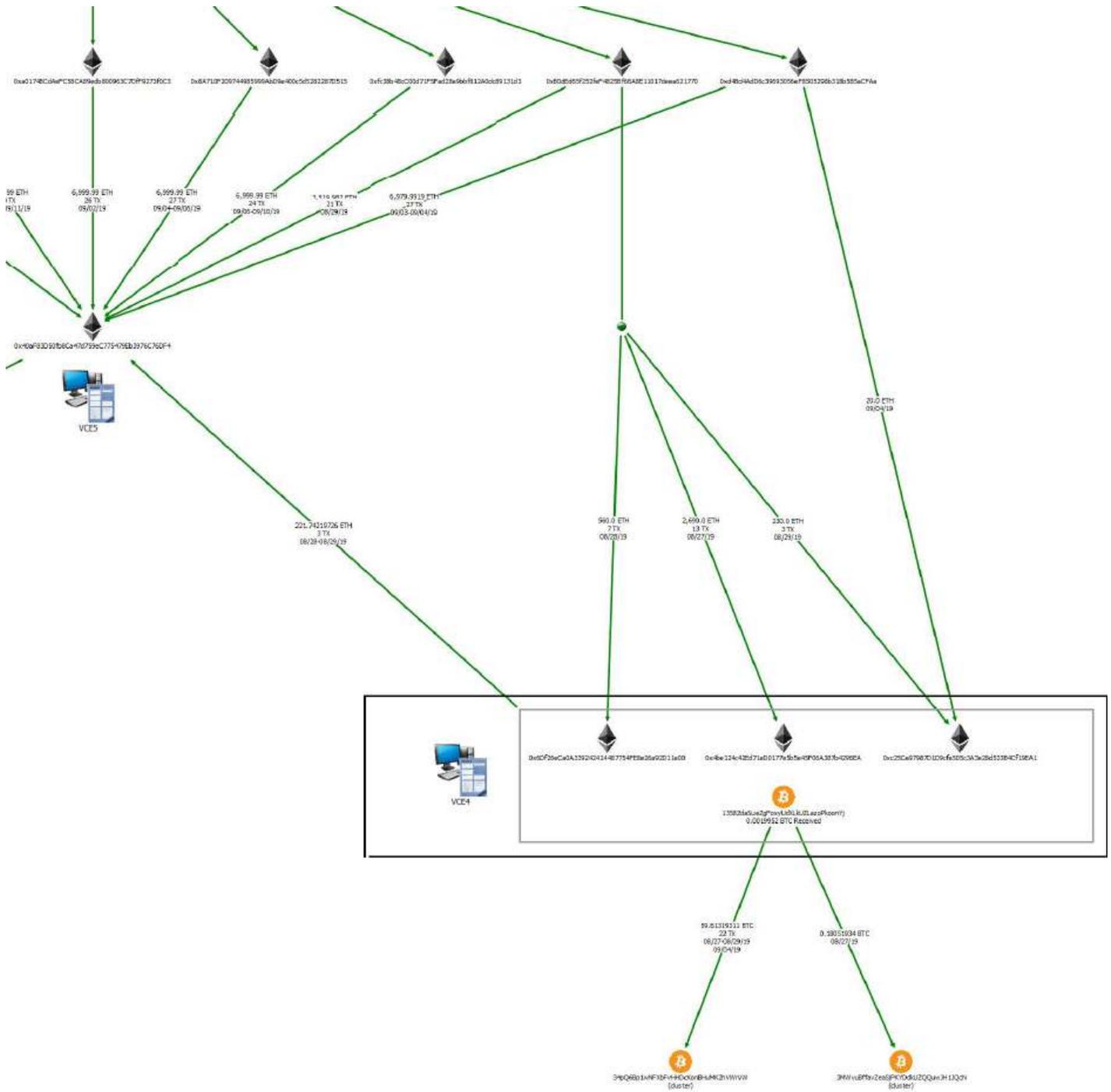
131. Separately from the above-described peel chain, the North Korean co-conspirators continued additional peel chains. Specifically, between August 28, 2019 and September 4, 2019, the North Korean co-conspirators laundered 3500 ETH via 24 transactions from Defendant Properties 138 and 139 to three addresses at VCE4 (Defendant Properties 141 through 143), all of which were also controlled by the North Korean co-conspirators.

132. The North Korean co-conspirators again converted stolen ETH into BTC at VCE4. The North Korean co-conspirators' account at VCE4 had a BTC deposit address (Defendant Property 144). Between August 27 and September 4, 2019, the North Korean co-conspirators laundered out 59.79363865 BTC from their account at VCE4 (which was funded by Defendant Properties 141 through 144) to two BTC clusters (Defendant Properties 145 and 146).

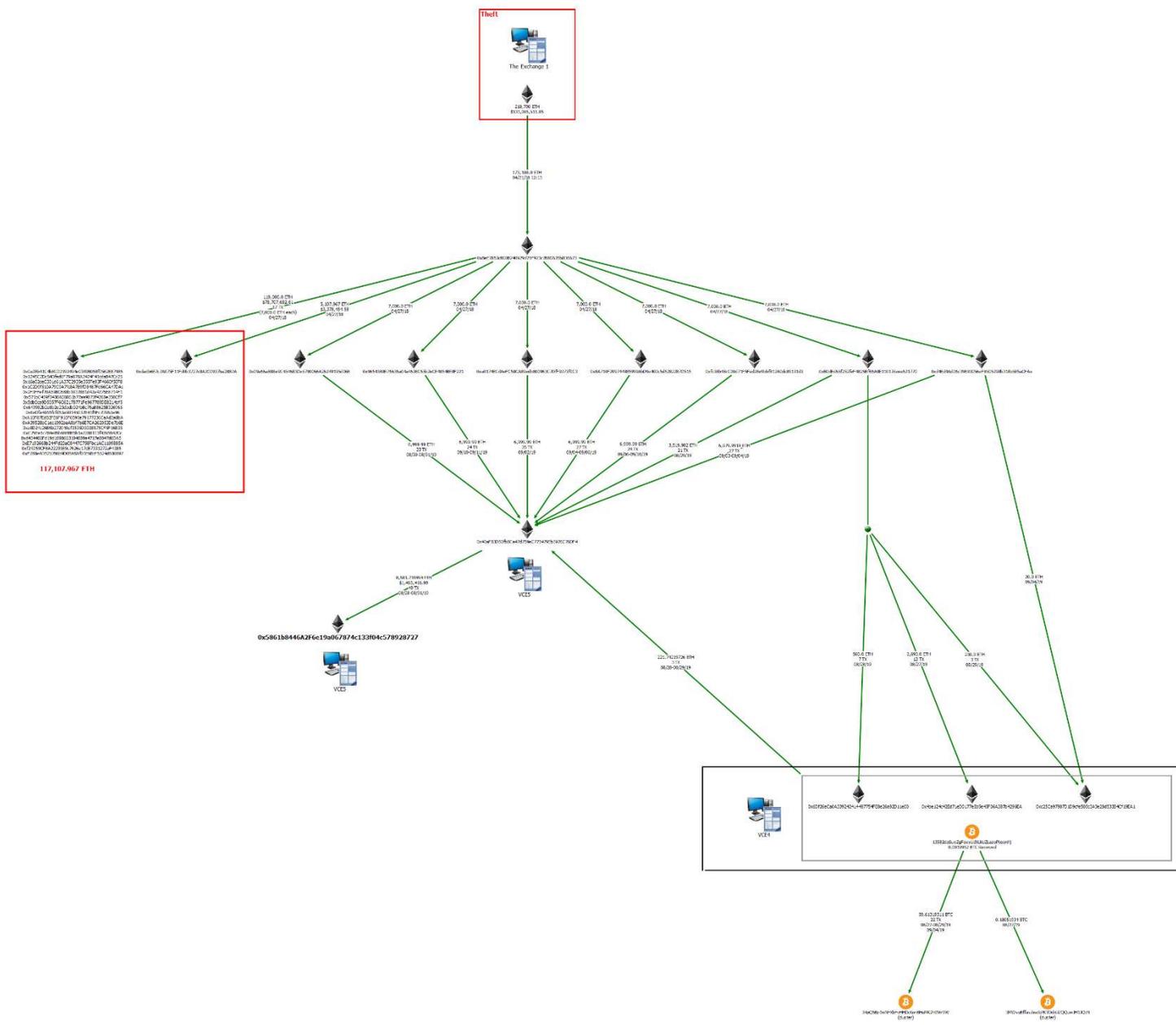
133. Consistent with the observed money laundering practices, the North Korean co-conspirators laundered funds from this separate peel chain back to their account at VCE5.

134. Specifically, between August 28 and 29, 2019, the North Korean co-conspirators laundered 221.74219726 ETH from their account at VCE4 (which was funded by Defendant Properties 141 through 144) back to Defendant Property 140 at VCE5 via 3 transactions.

135. Included below as Exhibit 8 is a diagram of this step in the money laundering process.



136. Included below as Exhibit 9 is a diagram summarizing the above-described scheme.



IV. CONCLUSION

137. Based on the facts described above, there is probable cause to believe that the Defendant Properties are subject to seizure and forfeiture.

Respectfully submitted,

/s/ Christopher Janczewski

Christopher Janczewski

Special Agent

Internal Revenue Service – Criminal

Investigation, CyberCrimes Unit

Dated: June 27, 2020

Attachment A

PROPERTY TO BE FORFEITED

Funds associated with the following virtual currency addresses and accounts:	
1	113vSKMWvuM8Weee2neMScXqdtXFLvy8z7
2	12DCmGuX87aCzxCDneyAxZdVWapuza9UyR
3	12JSAKyUMFmFp2ao5Rqt3s3X4xrQMXMzkr
4	12urwZAF7JvdhiQcYVbNG7VtKP3165pPnf
5	13Bcq6AcWusG3YKsYadBRNwnfezUrhRDER
6	13u7zCciSC7yGKfe8qqvQxK7BnGiwpdAbQ
7	14jP1TjTjrFBVFKUMcGaPjGRHaWAK6QVr7
8	14umE3q9knsWKZhjPgLYyv4rrCNjfXpAuF
9	16RWbMVHvERVUjrh28rRugmrgeDW1nweoo
10	17PSv7hd2cvSmgMTFw8CA3hjdYtGWuPh98
11	18LX9wjgJDbmRZXYhDLzZWCQ3pkUGB6gFf
12	19RfkmQPS3wBF5XhjcZwnbpMkd96GoituJ
13	19V5YCatY8sfdNuskawrGmbrZEohLkqV3d
14	1Ax8m2gy1Ta6vQTMSnWdCh71oMX7Z4nen
15	1Bht2x8Y8tJLpXxqK9LX4ehtLNk6kh3FLk
16	1C3K6yYxr1xomotxkEbMLAc3jVKDSyFBd
17	1C4hPundX3pBSiNbhkLpuLp246Ggc8gmwx
18	1C5S12fBSmeVedaEAqQzFf29H9hUucojPA
19	1JCWsAC86pokjDrvQsRwoU2jm9qA9Wc4qh
20	1K2FgtrdGk767RoLf8dN8tr5XsVc5st6RZ
21	1L5mPKvfKzGY2J99HtpoefxqbpLDxyMAZq
22	1LcsVyCd6yEyibDQS2WcxzTBT1iJGAqLhS
23	1MVkopW6PPWZtSAtp4295B6KfH93YKToZU
24	1Nmd7KBc3P6RgYcZ5n8ftdbw7z4jEzUSVj
25	1NMpPj2zUSPodncvZGp7owP2nttAgyFuY3
26	17UwTn7cVxu5ivkBnkPo83Gjtowi8dx75Q
27	1A3uGGvHFBauSmjZvdZFF6gjc8VSjgF7UY
28	1Bm659Wu5xVppUNRh7jKNFMboTbDepgmbm
29	18atn6kuyKzhnsWK554Uj6j1PAv3sPmx2p
30	18YNDeHouezsyxcvntohev9kANrMXiGBxr
31	1CD483mLYrMJwZF5drZnoPKSBbFTMSVvGf
32	1P8y7bj28tsq76anvKLGmhbbnTc1ZGcUVa
33	1Pa32FPFQJ5VdozwmMGE1ANNWVGB3XQJie
34	15pPmUErhTb8CaWF5x8iQggX3zK1y99ZN1

35	1EFWRRLUM3jy2poCpY7ALq2m7PPakyvns1
36	37JN1EDYCGYVabtofvYKKLtpA6uU3UBMLo
37	39PAYsdx2zi7GUhV71cx1zpp1N8495t58f
38	3ACmZQBNZsDDDs3UGoC6DeKMKHTE9RW1yu
39	3AUHHS4NQjJRAMbjdkeTdLDv9ZFeA9n1o3
40	3GAwA7PvLiHKjcmN2nsrHEpN7Qt9jwMQ4h
41	3HoJydELfq2kyZk9M6yug6CLQmYCS7FrJj
42	3M23QTysjRsfmJz4aDdc9RpaXjVZmbWKEt
43	3Nis34RW9uGV5mbovNidNNsxRTWwwqb1PS
44	User ID 36020326 at VCE10
45	User ID 35802038 at VCE10
46	User ID 35977393 at VCE10
47	User ID 35978286 at VCE10
48	0x8bdd991a7b8e2fe1bfc6b19ac3cf3e146cba415
49	User ID 38785599 at VCE10
50	1FKMe2Nyue2SDufB4RciiXsEEpAxtuBxD3
51	0xc4f9ee31626c8dee0ec02744732051e8b416e63e
52	User ID 9fdbd2ca-3994-411b-9ddb-f5318b63049d at VCE3
53	VCE12 internal transaction ID Fnc4bjm7ehwhdk6h4d
54	VCE12 internal transaction ID pd7e8fxxkuy2gfge7f
55	1EfMVkxQQuZfBdocpJu6RUsCJvenQWbQyE
56	Account 1000079600 at VCE6
57	134r8iHv69xdT6p5qVKTsHrcUEuBVZAYak
58	14kqryJUxM3a7aEi117KX9hoLUw592WsMR
59	15YK647qtoZQDzNrvY6HJL6QwXduLHfT28
60	1F2Gdug9ib9NQMHKMGJczMk5SuENoqrp
61	1PfwHNxUnkpfkK9MKjMqzR3Xq3KCtq9u17
62	Account 1000021204 at VCE6
63	0xA4b994F1bA984371ecCA18556Fe1531412D5C337
64	User k*****@***** at VCE1
65	17UVSMegvrzfobKC82dHXpZLtLcqzW9stF
66	19YVKCETP8yHX2m2VbEByVgWgJUAZd5tnS
67	User IDs 458281 & 4582819 at VCE5
68	1AXUTu9y3H8w4wYx4BjyFWgRhZKDhmcMrn
69	1Hn9ErTCPRP6j5UDBeuXPGuq5RtRjFJxJQ
70	User IDs 1473600 & 14736005 at VCE5
71	39eboeqYNFe2VoLC3mUGx4dh6GNhLB3D2q
72	39fhoB2DohisGBbHvvmkdPdShT75CNHdX
73	3E6rY4dSCDW6y2bzJNwrjvTtdmMQjB6yeh

74	3EeR8FbcPbkcGj77D6ttneJxmsr3Nu7KGV
75	3HQRveQzPifZorZLDXHernc5zjoZax8U9f
76	3JXKQ81JzBqVbB8VHdV9Jtd7auWokkdPgY
77	3KHfXU24Bt3YD5Ef4J7uNp2buCuhrxfGen
78	3LbDu1rUXHNyiz4i8eb3KwkSSBMf7C583D
79	3MN8nYo1tt5hLxMwMbxDkXWd7Xu522hb9P
80	3N6WeZ6i34taX8Ditser6LKWbCXmt2XXL4
81	LLzTJFu3UcwXRrwaq2gLKnJaWWt3oGHVMK
82	0x01facd1477e6df9e27fe9f0a459aaa0769c9af82
83	User 881051 at VCE7
84	3F2sZ4jbhvDKQdGbHYPC6ZxFXEau2m5Lqj
85	0X7175D1FA4461676AB8831483770FF84483F26501
86	Account 14167009 at VCE 11
87	0X93D8EDBC42E547C571CE5AF95F70C291D706925C
88	Account 14166934 at VCE 11
89	0XB35DF36FF3D686A63353FA01327F3FF4874CF21
90	Account 14166961 at VCE 11
91	BC1Q39HKR7TA25E65D7U0PM09L99JVFNY4LP3VAM4Q
92	0X81B34F7A426B31E77E875B8D00D830F8A5B044CB
93	User DavidniColinDC3 at VCE4
94	0XFC3D6AEE062C45B31E946BA49A7AA5ADDF1B53C6
95	User Ep4444 at VCE4
96	0XBD72F2CFB28ED38B7CEA94E26603983CE028C927
97	User Sma414 at VCE4
98	17KS1C6DxViF68YaSAhWUrnaCtxzbMq7CB
99	1MP62xKDtL79wQ8f8LbAg9dPpUHFTEVbJ
100	1GsAS3z7eG4Vw2QbyVqnR7cRQmpeRsCpt1
101	1K7cMd9RgwhThXi6VDu3Roti2W4241MLfG
102	1FhsTJ7hQKvpFXPRFFjsFPHQT4pQMqpgw1
103	1FzKR8XDmdrTRYfMcZRf3NPvSgyrUoG8kq
104	1AsHQhhCYwgd71cxnHA9a8dWeEh22ivdqn
105	1DZdJNQsEutzud3YX28DFXfzKVyEfoN8t2
106	1K83LzD1QR2iUVtHckFMUzzdF3xUhtNdYb
107	1DX3zJV4djK9CgCP48Ym3LEryq5RVdhWH8
108	1EFNjtGnJ7WohXd8L17NGA4N5osKRj98QN
109	1EU4tNd1RbhDCfkiQrtj6nfzxeRxRA9rBm
110	17Wx3A1tmiTnxJ9FAq7em1n6SxtXSG4r5F
111	1QBbEUUhG7CRJzJrSEnUvwrycYZzKB8YEq
112	1K1fa3ydmppWMuX8gWHk5W6gnVFX7nGQJsu

113	0xC137c3135EB8E94aa303D52c607296Ba470E1a57
Funds associated with the following additional 33 virtual currency addresses and accounts:	
114	0xBeE7853cB00B240929d75F923c7B8D62Bb8D6673
115	0x0a28b41C4b8CD2390494e0349B068f0562E87986
116	0x1245C2Dc54Dfed6F79a078A2424F45cdaB47Cc25
117	0x16a02ceC301d61A37C2935e355Fe93F4660f50F8
118	0x1C2D9f510A79C9A7fc8A7E9fD8487Fd66CA47DAc
119	0x2F3FFef70A59BC688b1037881d42a4276E8714F1
120	0x571bC459f3430A00861b77aa9873f4268e350Cf7
121	0x5db0ca9D5057F6C62178771Fe967789DE8214bf5
122	0x649982b2e8b2e23dbdb024bBc76aB8625B326965
123	0x6eDfa4055fcfd53a90145037B41fBFc7D963a96D
124	0xA10F87EdB2FE6F910F6595e79177236CaAd3a8bA
125	0xA39528bC1ec1992baA8bf7a6B7CA262053De7b6E
126	0xa8D24c26E6b272040ef3505D3038575CF5F16B35
127	0xC79Ee5c784e89b69BBB5b1a7288111f4395942Cc
128	0xd434486Fd19d1098663194889a4717e8047d6DA5
129	0xE7192668b244Fd20aC8447C758Fbc1AC1109885A
130	0xf24D59CF8A22293E9c7626e17dE7331272aF4385
131	0xF288eAD5257B6b9D0BABAfD1E6BcF5524d600897
132	0xdadb6B7c7A075F11Fd0b3727c8A2C0937ba288DA
133	0x09a66a888e9C454683De5790066A26249195d06B
134	0x9654380B76636a04a463BC65b2eCE4854BE8F221
135	0xa0174BCdAeFC58CA89edb800963C7DfF9273f0C3
136	0x8A710F209744985999AbD9e400c5d5282287D515
137	0xfc38b48cC00d71F5Fad28e9bbf812A0dc89131d3
138	0xB0dEd65f252feF4825Bf66A8E11017deea621770
139	0xd4Bd4AdD6c39693056eF8505298b318b585aCFAa
140	0x40aF83D50fb8Ca47d759eC775479Eb3976C76DF4
141	0x6Df26eCa0A339242414487754FE8e26a92D11e00
142	0x4be124c42Ed71eD0177e5b5e45F06A387b4296EA
143	0xc25Ca97987D1D9cfe505c3A3e28d533B4Cf19EA1
144	13582daSueZgFoxyUdXLkUZLazoPkoonYj
145	34pQ6Bp1wNFXbFvHHDcKonBHuMK2hVWrVW
146	3MWvuBffavZeaSjPKYDdkUZQQuwJH1JQcn