UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, **Plaintiff,** **v.** **280 VIRTUAL CURRENCY ACCOUNTS** **Defendants.**	**Civil Action No. 20-2396**

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

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 Rem* against the defendant properties, namely: 280 virtual currency accounts (the "Defendant Properties"), which are listed in Attachment A. The United States alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions:

THE DEFENDANT PROPERTIES

1. The Defendant Properties are comprised of miscellaneous financial instruments (listed in Attachment A).

NATURE OF ACTION AND THE DEFENDANTS IN REM

2. This *in rem* forfeiture action arises out of an investigation by the Internal Revenue Service – Criminal Investigation's Cyber Crimes Unit ("IRS-CI"), the Federal Bureau of Investigation ("FBI"), and Homeland Security Investigations ("HSI") into the laundering of monetary instruments, in violation of 18 U.S.C. § 1956.

3. The Defendant Properties are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), as property involved in, or traceable to, a financial transaction in violation of 18 U.S.C. § 1956.

JURISDICTION AND VENUE

4. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355. These statutes confer original jurisdiction to district courts of all civil actions, suits, or proceedings commenced by the United States and any action for the forfeiture of property incurred under any act of Congress.

5. Venue is proper pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred within the District of Columbia, specifically, relevant financial regulators are located in this district.

6. Venue is also proper within this judicial district pursuant to 28 U.S.C. § 1355(b)(2), because the property subject to forfeiture is located in a foreign country.

FACTS GIVING RISE TO FORFEITURE

I. Background

A. Bitcoin and Ether

7. Bitcoin ("BTC") and Ether ("ETH") are pseudonymous virtual currencies. Although BTC and ETH 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 unlawful drugs or other illegal items or services) look for ways to make their transactions even more anonymous.

8. BTC/ETH addresses are unique tokens; however, BTC/ETH are designed such that one person may easily operate many such accounts. 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.

9. 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 secure 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.

10. 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.

11. There are other virtual currencies similar to ETH that are stored and sent using ETH addresses and transactions. Some of these currencies are discussed in this affidavit below.

12. 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, 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 on 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

13. While the identity of a 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. North Korea's Documented Hacking of Virtual Currency Exchanges

14. 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.

15. 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.

16. 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.

17. "With regard to the foreign currency earned through cyberattacks, according to one U.N. Member State, 'These activities contribute to the [the Democratic People's Republic of Korea]'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.

18. 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 [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*.

II. Forfeiture of 146 Virtual Currency Accounts in March 2020 (Defendant Property 1)

19. In late 2018, IRS-CI's Cyber Crimes Unit learned that a South Korea-based virtual currency exchange ("Exchange 1") had been hacked. The North Korean cyber actors responsible for the hack stole nearly $250 million worth of virtual currencies. 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 ("KYC") information to various virtual currency exchanges. These communications include wire communications that transited through the United States.

20. On or about March 2, 2020, the United States filed a forfeiture complaint in this Court (Case No. 1:20-cv-00606-TJK) against 146 virtual currency accounts linked to the $250 million dollar theft and other related cryptocurrency thefts.

21. The complaint also detailed North Korean involvement in the hack of another South

Korea-based virtual currency exchange ("Exchange 2") on or about November 27, 2019. Approximately 342,000 ETH (valued at about $48.5 million) was stolen from Exchange 2.

22. The investigation of the laundering of the funds stolen from Exchange 2, and funds related to additional hacks, identified a U.S.-based email account ("Target Email 1") that a criminal actor ("Target Actor 1") had used to launder funds from the scheme.

23. In or about December 2019, Target Actor 1 attempted to convert ETH to BTC through a cryptocurrency trading platform ("Exchange 9") which was designed to enable the transfer of one form of cryptocurrency in exchange for another. Target Actor 1 submitted ETH for conversion into BTC, generating a transaction ID beginning with 6918d31f; however, Exchange 9 did not convert the ETH. On or about December 20, 2019, Target Actor 1 contacted a separate virtual currency wallet provider requesting assistance with the transaction. Exchange 9 notified the virtual currency wallet provider that transaction ID 6918d31f would not be processed because it contained funds related to the hack of Exchange 2.

24. The funds associated with transaction ID 6918d31f ("Defendant Property 1") are currently frozen at Exchange 9, pursuant to their own internal policies.

III. Hack of Exchange 3 and Laundering of Funds (Defendant Property 2 through Defendant Property 24)

A. Theft of Funds

25. On or about July 1, 2019, hackers stole approximately 401,981,748 Proton Tokens ("PTT") from a virtual currency exchange ("Exchange 3"). (As relevant here, Proton Tokens/PTT – like the other virtual currencies listed in the table below – function similarly to BTC and ETH.) While 280,269,180 PTT was contained before the hackers could liquidate it, the remaining approximately 121,712,568 PTT entered the market.

26. Subsequently, Exchange 3 informed the news media that hackers stole additional forms of virtual currency in addition to PTT on or about July 1, 2019.

27. Blockchain analysis corroborated Exchange 3's statements and provided more detail for the following thefts/transactions, all of which occurred at approximately the same time on July 1, 2019, and originated from Exchange 3's wallets:

Virtual Currency	Abbreviation	Icon	Approx. Amount Stolen	Approx. U.S. Dollar Value	Approx. Time of Transaction
Olive	OLE		9,064,558.36	$79,197.05	8:34
Proton Token	PTT		401,981,748.79	$80,396.35	8:36
PlayGame	PXG		17,829,785.00	$19,505.78	8:41
Yee	YEE		4,342,294.43	$11,055.48	8:42
Reputation	REP		1,963.28	$31,039.49	8:43
IHT Real Estate Protocol	IHT		137,793.98	$6,701.33	13:21
All Sports Coin	SOC		171,145.04	$962.86	13:23
StatusNetworks	SNT		71,237.03	$1,910.36	13:25
Cortex Coin	CTXC		23,300.29	$5,128.30	13:30
Bethereum	BETHER		24,798,773.00	$22,343.69	15:31
Taklimakan	TAN		2,784,773.00	$14,645.76	15:32
Total				$272,886.47	

B. Laundering of Funds Stolen from Exchange 3 (Defendant Property 2 through Defendant Property 7)

28. The entire balance of approximately 17,829,785 PlayGame ("PXG") tokens and 137,793.98 IHT Real Estate Protocol tokens ("IHT") were sent directly from Exchange 3's address starting with 0x60d6 to addresses starting with 0x52cb ("Defendant Property 2") and 0xeda8 ("Defendant Property 3") respectively.

29. Defendant Property 1 and Defendant Property 2 were hosted at a virtual currency exchange ("Exchange 4"). The Exchange 4 account owning the two addresses was opened on or

about July 1, 2019 at 02:24, mere hours before the theft from Exchange 3. The account was registered with Target Email 1.

30. Target Actor 1 provided falsified KYC data to open the account at Exchange 4. Specifically, Target Actor 1 provided the photo of the biographical page of a Russian Federation passport. Target Actor 1 provided the same name to the provider of Target Email 1, but claimed to be from Canada.

31. All deposit activity for Target Actor 1's account at Exchange 4 occurred on or about July 1, 2019, the same day as the theft from Exchange 3, and is as follows:

Deposit No.	Virtual Currency	Abbreviation	Approx. Amount	Approx. U.S. Dollar Amount	Deposit Time
1	PlayGame	PXG	17,829,785.00	$19,505.78	8:42
2	Tether	USDT	2,406.49	$2,406.49	10:29
3	IHT Real Estate Protocol	IHT	137,793.98	$6,701.33	13:22
4	Tether	USDT	1,495.00	$1,495.00	13:28
5	Stellar	XLM	952,215.00	$98,198.12	15:08
6	Stellar	XLM	5,000.00	$515.63	16:07
7	Tether	USDT	2,495.00	$2,495.00	18:10
	Total			$131,317.36	

32. As stated previously, the PXG and IHT deposits (Deposit Numbers 1 and 3 in the above chart) came directly from the theft at Exchange 3.

33. The stolen 9,064,558.36 Olive ("OLE") from Exchange 3, shown in the chart of deposits above, was moved to an intermediary address and then, at approximately 09:22, was deposited at another virtual currency exchange ("Exchange 5").

34. At approximately 10:29 and 18:10, Target Actor 1 received Deposit Numbers 2 and 7 (in the chart of deposits above) in another address ("Defendant Property 4") held within Target Actor 1's account at Exchange 4. These two deposits were in a different cryptocurrency, Tether ("USDT"). The timing of the deposits and Target Actor 1's *modus operandi* of converting

cryptocurrencies, as further described below, suggest that Target Actor 1 converted at least portions of the stolen OLE into USDT before depositing the funds into Exchange 4.

35. The 4,342,294.43 Yee ("YEE"), 171,145.04 All Sports Coin ("SOC"), 71,237.03 StatusNetworks ("SNT"), and 23,300.29 Cortex Coin ("CTXC") stolen from Exchange 3, shown in the chart in Paragraph 27 above, were all traced to an intermediary address starting with 0x1016 ("Defendant Property 5") before being deposited to an account ("Defendant Property 6") at a virtual currency exchange ("Exchange 6") on or about July 2, 2019 at 10:29, 22:32, 10:42, and 07:13 respectively.

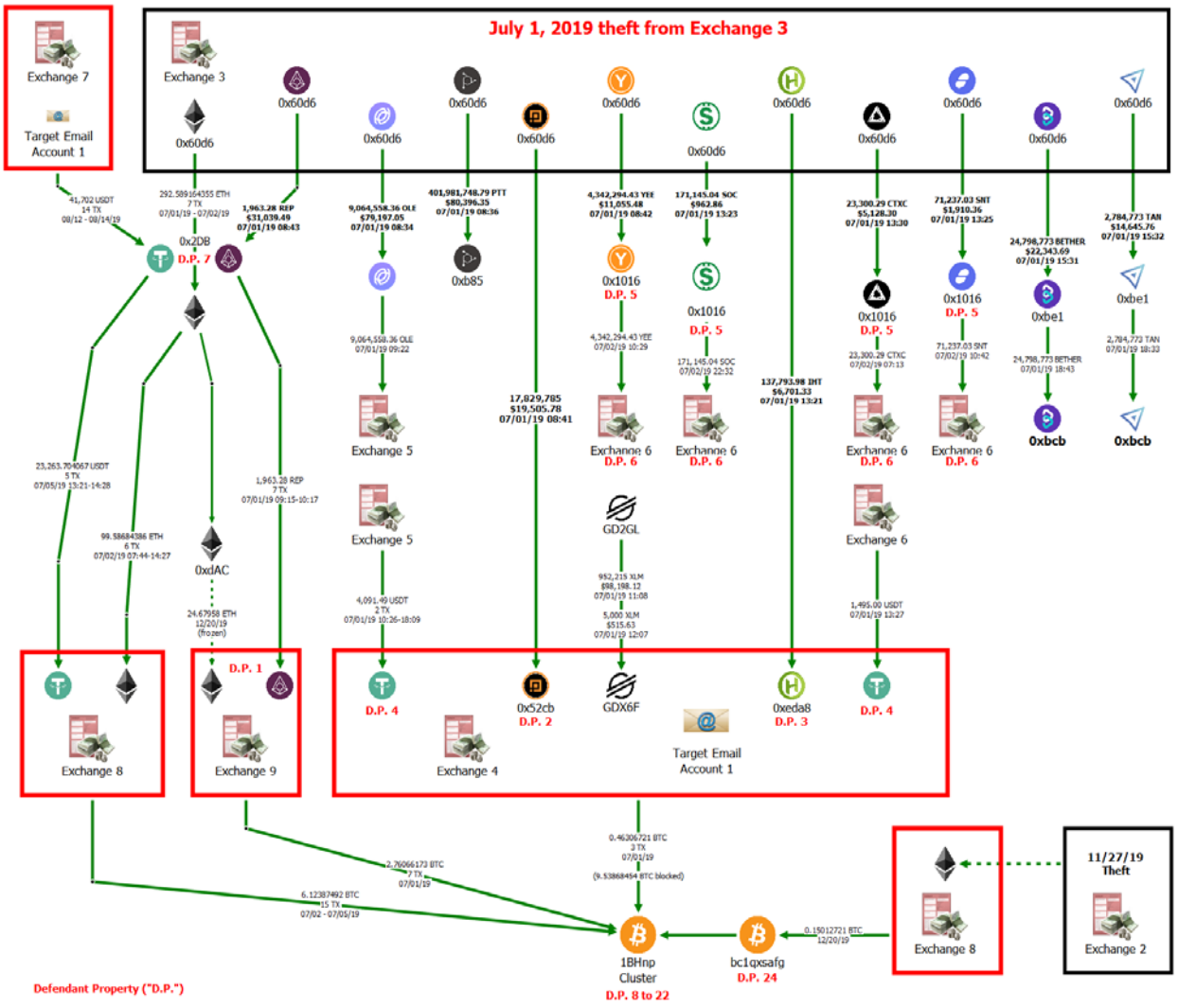
36. About that time, Target Actor 1's account at Exchange 4 received Deposit Number 4 (in the Paragraph 31 chart) from Exchange 6 in the form of USDT ("Defendant Property 4"). This transaction was again consistent with Target Actor 1 converting the cryptocurrency based on the timing and his *modus operandi*.

37. The 1,963.28 Reputation ("REP") stolen from Exchange 3, shown in the chart in Paragraph 27 above, was sent to an address starting with 0x2DB ("Defendant Property 7"). Defendant Property 7 also received approximately 41,702 USDT from an account at another virtual currency exchange ("Exchange 7") via 14 transactions between August 12, 2019 and August 14, 2019. The originating account at Exchange 7 was opened on or about July 2, 2019 and was registered with Target Email 1 and no other identifiable information.

38. The USDT at Defendant Property 7 was sent to another virtual currency exchange ("Exchange 8"), converted to BTC, and withdrawn to a cluster of BTC addresses starting with 1BHnp (described below).

39. The stolen REP at Defendant Property 7 was then sent to Exchange 9, converted to BTC, and also withdrawn to cluster 1BHnp.

40. The foregoing transactions are graphically summarized as follows:



C. Ties to North Korea and Additional Laundering (Defendant Property 8 through Defendant Property 24)

41. Target Actor 1 used an account at Exchange 4 to convert the various forms of stolen virtual currency received into BTC. This tactic of moving between different types of virtual currency, often referred to as "chain hopping," is frequently used by individuals who are laundering the proceeds of virtual currency thefts. Chain hopping seeks to accomplish several objectives. First, it helps obfuscate the trail of the stolen virtual currency because the path jumps from the blockchain of one virtual currency to another virtual currency. Second, the BTC

ecosystem is much larger, with more virtual currency exchanges and traders willing to accept BTC versus other virtual currencies. Therefore, it is generally easier to transact in BTC and hide among the crowd.

42. On or about July 1, 2019, Target Actor 1 withdrew approximately 0.46306721 BTC from Exchange 4 via three transactions. These funds represent a portion of the Defendant Properties, described further below. Target Actor 1 then attempted to withdraw an additional approximately 9.53868454 BTC from Exchange 4, but Exchange 4 blocked this transaction.

43. Target Actor 1 sent the BTC successfully withdrawn from his Exchange 4 account to a cluster including the bitcoin address beginning with 1BHnp ("Defendant Property 8") and approximately 14 additional BTC addresses ("Defendant Property 9" through "Defendant Property 22"). BTC cluster 1BHnp received approximately 80.86041444 BTC via 119 transactions between approximately July 1, 2019 through October 23, 2019. Defendant Property 8 also received approximately 15 BTC from accounts at Exchange 3, Exchange 5, and Exchange 6.

44. BTC from cluster 1BHnp, containing Defendant Property 8 through Defendant Property 22, was sent primarily to three intermediary BTC clusters and then to a BTC address starting with 1DXbM ("Defendant Property 23"). Other BTC addresses and clusters associated with cluster 1BHnp sent to address Defendant Property 23 as well, further illustrating common ownership as the funds regroup at the same destination after being layered. These transactions are shown on the chart appearing in Paragraph 61.

45. As also shown on the chart appearing in Paragraph 61, for the approximate period October 11, 2019 through December 9, 2019, Defendant Property 23 sent approximately 441.791834 BTC to approximately 14 different accounts at Exchange 6.

a. Many of these accounts were known to law enforcement as over-the-counter ("OTC") virtual currency traders acting as money services businesses that convert virtual currency into fiat currency for a profit.

b. In so doing, these OTC traders fail to collect the legally required KYC information about their clients and the source of the virtual currency being converted.

c. Many owners of illicit funds seek out these OTC traders because they are otherwise unable to obtain accounts at law-abiding virtual currency exchanges or risk having their funds frozen, as was the case with Target Actor 1's account at Exchange 4.

46. From the period of the opening of Target Actor 1's account at Exchange 4 to October 2019, the account was accessed by IP addresses resolving to Virtual Private Network ("VPN") providers, in an attempt by the user to conceal his location. The VPN IP addresses have been used by other North Korean cyber actors in related facets of the overall criminal schemes. Specifically, over 50% of the IP addresses used by Target Actor 1 at Exchange 4 matched IP addresses previously utilized by North Korean cyber actors who have been tied to hacks of at least two other cryptocurrency exchanges, including the previously mentioned theft from Exchange 2, and who subsequently laundered funds through the United States. Additionally, an IP address utilized to log into Target Actor 1's account at Exchange 4 matched the IP address utilized by the same North Korean cyber actors to log into a malicious website created by them. The website appears to target owners of cryptocurrency and solicit information from them.

47. On or about December 20, 2019, Exchange 8 received approximately 8.65658 ETH that was converted to 0.15012721 BTC and sent to a BTC address starting with bc1qxsafg

("Defendant Property 24"). Defendant Property 24 has transacted with cluster 1BHnp, containing Defendant Property 8 through Defendant Property 22. The source of the 8.65658 ETH was the November 27, 2019 theft from Exchange 2, after being layered through multiple ETH addresses. The request to convert ETH to BTC at Exchange 8 came from an IP address at a Hong Kong-based Internet service provider (ISP) that has previously received payment via stolen BTC from North Korean cyber actors.

48. Multiple addresses connected to cluster 1BHnp sent payments to a U.S.-based BTC payment processor to purchase services from the Hong Kong-based ISP. The account at this U.S.-based BTC payment processor was registered using "Target Email 2."

49. In late April 2019 and early May 2019, several months before the hack of Exchange 3, Target Actor 1, using Target Email 1, communicated via email with another individual ("Target Actor 2"), who was using Target Email 2. According to a website tracking malware submitted by community users, Target Email 2 was contained within a piece of malware designed to allow an attacker to execute code on a victim computer after the victim opened a word processing document, giving the hacker the ability to gain access to the victim's computer and/or network. The file type was a Korean word processor file related to exploits used by North Korea against cryptocurrency exchanges since at least 2017.

IV. Hack of Exchange 10 and Laundering of Funds (Defendant Property 25 through Defendant Property 280)

A. Theft of Funds

50. "Exchange 10" is a U.S.-based company focused on the Algorand blockchain, which administers ALGO tokens, a form of virtual currency. On or about September 25, 2019, Exchange 10 was the victim of a theft of multiple virtual currencies in which hackers used stolen

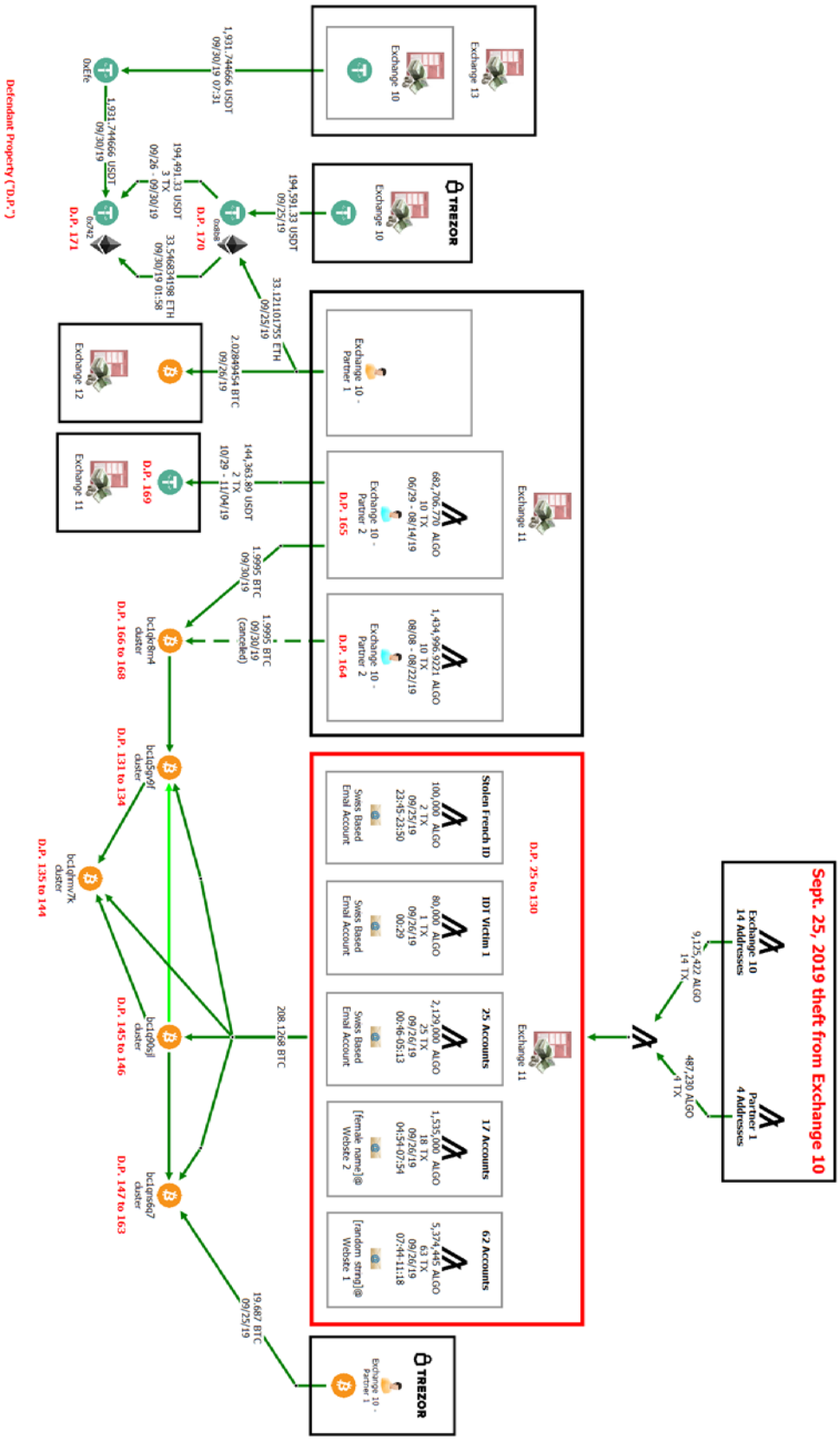
recovery seeds[1] to recreate wallets owned by Exchange 10 and its partners, including "Exchange 10 - Partner 1" and "Exchange 10 - Partner 2." (In essence, by re-creating the wallets, the hackers were able to direct the transfer of funds out of the wallets into other addresses and wallets controlled by the hackers, thereby stealing the virtual currency from Exchange 10 and its partners.) Additionally, hackers gained access to Exchange 10-owned accounts at multiple other virtual currency exchanges. In all, the security incident resulted in the theft of the following:

	Location	Owner	Virtual Currency	Approx. Amount	Approx. USD
1	Exchange 10	Exchange 10	ALGO	9,612,652.0000	$1,922,530.40
2	Trezor	Exchange 10	USDT	194,591.3300	$194,591.33
3	Trezor	Partner 1	BTC	19.6870	$165,804.11
4	Exchange 11	Partner 2	USDT	144,363.8900	$144,363.89
5	Exchange 11	Partner 1	BTC	2.0285	$17,128.26
6	Exchange 11	Partner 2	BTC	1.9995	$15,996.00
7	Exchange 11	Partner 1	ETH	33.1211	$5,622.97
8	Exchange 13	Exchange 10	USDT	1,931.7447	$1,931.74
9	Exchange 11	Partner 2	BTC	(Attempted 1.9995)	
		Total			**$2,467,968.71**

B. Laundering of Stolen Funds
(Defendant Property 25 through Defendant Property 171)

51. The North Korean actors illegally recreated 14 ALGO addresses within wallets owned by Exchange 10 and four ALGO addresses in wallets owned by Exchange 10 - Partner 1, and sent approximately 9,612,652 ALGO (line number 1 on the above chart) to one ALGO address. The malicious actors then split up the ALGO tokens via approximately 109 transactions and sent the tokens to approximately 106 different accounts ("Defendant Property 25" through "Defendant Property 130") held at another exchange ("Exchange 11"), as shown in the chart below.

[1] A recovery seed, also known as a recovery phrase, is a list of upwards of 12 words that when entered in a specific order into virtual currency wallet software, allows whomever is in possession of the words to recreate access to virtual assets within the wallet.


Sept. 25, 2019 theft from Exchange 10
Exchange 10
14 Addresses
Partner 1
4 Addresses
9,125,422 ALGO
14 TX
487,230 ALGO
4 TX
Exchange 11
D.P. 25 to 130
Stolen French ID
100,000 ALGO
2 TX
09/25/19
23:45:23:50
Swiss Based
Email Account
IDT Victim 1
80,000 ALGO
1 TX
09/26/19
00:29
25 Accounts
2,129,000 ALGO
25 TX
09/26/19
00:46:05:13
17 Accounts
1,535,000 ALGO
18 TX
09/26/19
04:54:07:54
[female name]@
Website 2
62 Accounts
5,374,445 ALGO
63 TX
09/26/19
07:44:11:18
[random string]@
Website 1
208.1268 BTC
19.687 BTC
09/25/19
TREZOR
Exchange 10 -
Partner 1
D.P. 135 to 144
bc1qfmv7k
cluster
D.P. 131 to 134
bc1q5p9f
cluster
D.P. 145 to 146
bc1q0s8j
cluster
D.P. 147 to 163
bc1qrs6q7
cluster
D.P. 166 to 168
bc1qk8rn4
cluster
1.9995 BTC
09/30/19
(cancelled)
1.9995 BTC
09/30/19
682,706.770 ALGO
10 TX
06/29 - 08/14/19
Exchange 10 -
Partner 2
D.P. 165
1,434,996.9221 ALGO
10 TX
08/08 - 08/22/19
Exchange 10 -
Partner 2
D.P. 164
Exchange 10 -
Partner 1
33.12110755 ETH
09/25/19
2.02849454 BTC
09/26/19
Exchange 12
144.363.89 USDT
2 TX
10/29 - 11/04/19
D.P. 169
Exchange 11
194,591.33 USDT
09/25/19
Exchange 10
Exchange 13
1,931,744666 USDT
09/30/19 07:31
0xEfe
1,931,744666 USDT
09/30/19
194,491.33 USDT
3 TX
09/26 - 09/30/19
33.546834198 ETH
09/30/19 01:58
D.P. 170
0xbe8
D.P. 171
0x742
Defendant Property ("D.P.")

52. One of the first accounts (Defendant Property 110) at Exchange 11 to receive the stolen ALGO was registered in the name of a U.S. Citizen ("IDT Victim 1") on or about September 26, 2019. A selfie-style photo and a photo of IDT Victim 1's biographical U.S. passport page were submitted to Exchange 11. The account had only one deposit, approximately 80,000 stolen ALGO.

53. In an interview with law enforcement, IDT Victim 1 verified that he or she did not open the account in question at Exchange 11. The photos submitted to Exchange 11 were likely stolen during the 2018 hack of a U.S.-based crypto currency exchange where IDT Victim 1 was a customer.

54. The ALGO tokens sent to Defendant Property 25 through Defendant Property 130 were promptly converted into BTC. Of that BTC, approximately 208.1268 BTC were withdrawn to four BTC clusters, which contained addresses enumerated as "Defendant Property 131" through "Defendant Property 163." One of the four clusters, a cluster starting with bc1qns6q7 (containing the addresses enumerated as Defendant Property 147 through Defendant Property 163), also received the stolen approximately 19.69 BTC from Exchange 10 - Partner 1's Trezor wallet[2] (line number 3 in the above chart).

55. Exchange 10 - Partner 2 owned two accounts ("Defendant Property 164" and "Defendant Property 165") at Exchange 11. Exchange 10 - Partner 2 funded both accounts exclusively by ALGO tokens received prior to the hack.

56. After the hack on September 30, 2019, these two accounts sent approximately 1.9995 BTC to a BTC cluster starting with bc1qkr8m4 (containing addresses enumerated as "Defendant Property 166" through "Defendant Property 168") (line number 6 in the chart above).

[2] A Trezor wallet is a wallet generated through the use of a Trezor, a physical device designed for securely storing a user's bitcoin.

57. On the same day, approximately 15 minutes later, one of the two accounts attempted to send approximately 1.9995 BTC to cluster bc1qkr8m4 (line number 9 in the above chart), but Exchange 11 canceled the transaction. Cluster bc1qkr8m4 sent BTC to one of the four previously mentioned BTC clusters that received the BTC from Exchange 11 and contained Defendant Property 131 through Defendant Property 134.

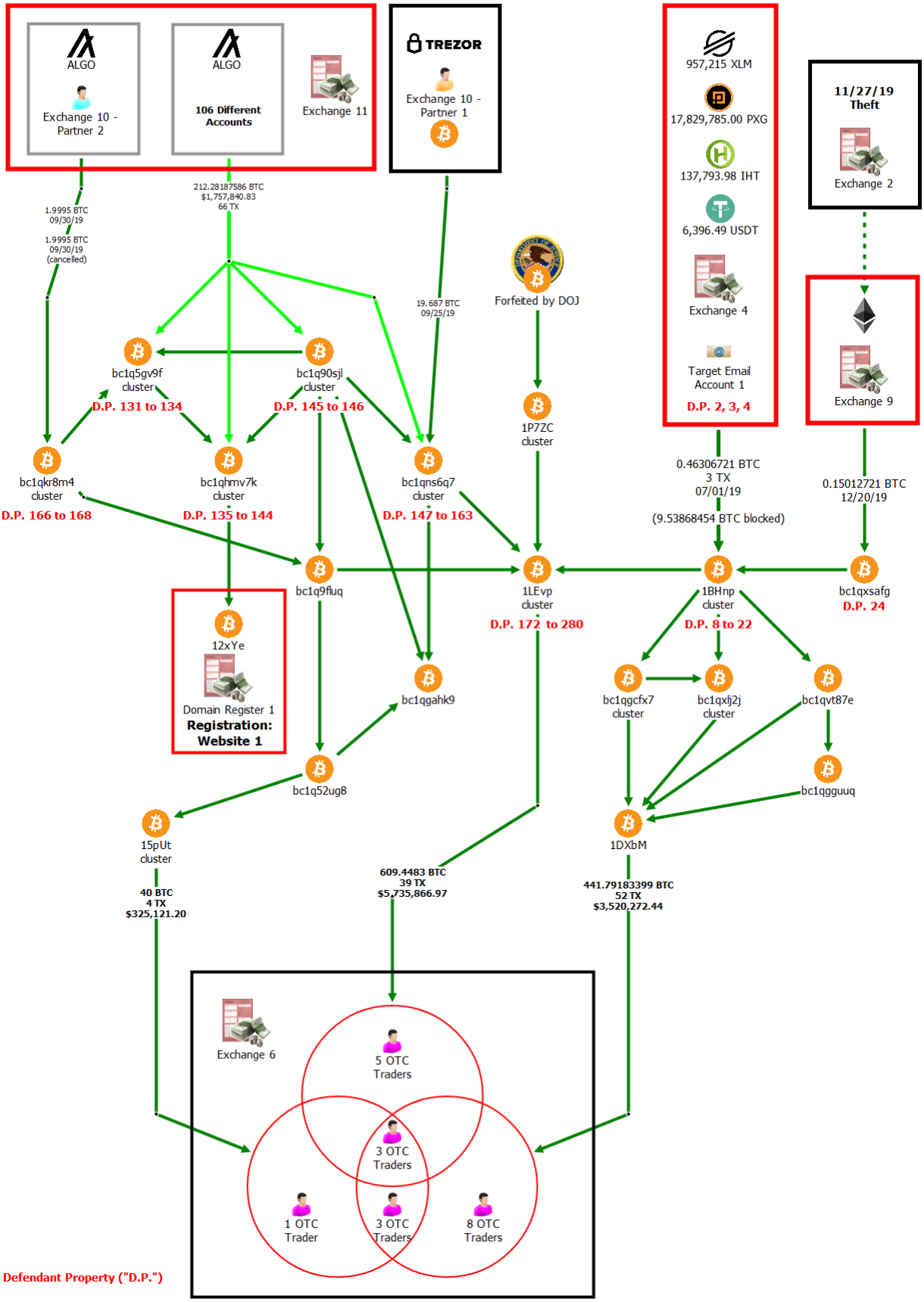
58. Exchange 10 - Partner 1's account at Exchange 11 sent the stolen 144,363.89 USDT to another account ("Defendant Property 169") at Exchange 11 (line number 4 in the above chart).

59. The stolen 194,591.33 USDT from Exchange 10's Trezor wallet (line number 2 in the above chart) and the stolen 33.12 ETH from Exchange 10 – Partner 1's account at Exchange 11 (line number 7 in the above chart) were both sent to the same address starting with 0x8bB ("Defendant Property 170"). Then the stolen USDT and ETH was sent to an address starting with 0x742 ("Defendant Property 171"). The stolen 1,931.74 USDT from Exchange 10's account (line number 8 in the above chart) was sent to an intermediary address before being sent to Defendant Property 171 as well. From Defendant Property 171, the ETH and USDT were sent to another virtual asset service provider.

60. The Exchange 10 – Partner 1's account at Exchange 11 also sent approximately 2.0285 BTC to an account at another exchange ("Exchange 12") (line number 5 in the chart above).

C. Connections of Hack of Exchange 11 to Hack of Exchange 3 and North Korea (Defendant Property 172 through Defendant Property 280)

61. As previously stated, the stolen ALGO tokens were deposited into 106 different accounts at Exchange 11, converted to BTC, and withdrawn to four BTC clusters (shown below, in light green lines).


ALGO
Exchange 10 - Partner 2
ALGO
106 Different Accounts
Exchange 11
TREZOR
Exchange 10 - Partner 1
957,215 XLM
17,829,785.00 PXG
137,793.98 IHT
6,396.49 USDT
Exchange 4
Target Email Account 1
D.P. 2, 3, 4
11/27/19 Theft
Exchange 2
Exchange 9
1.9995 BTC 09/30/19
1.9995 BTC 09/30/19 (cancelled)
212.28187586 BTC $1,757,840.83 66 TX
19.687 BTC 09/25/19
Forfeited by DOJ
bc1q5gv9f cluster
D.P. 131 to 134
bc1q90sjl cluster
D.P. 145 to 146
1P7ZC cluster
bc1qkr8m4 cluster
D.P. 166 to 168
bc1qhmv7k cluster
D.P. 135 to 144
bc1qns6q7 cluster
D.P. 147 to 163
0.46306721 BTC 3 TX 07/01/19
(9.53868454 BTC blocked)
0.15012721 BTC 12/20/19
bc1q9fluq
1LEvp cluster
D.P. 172 to 280
1BHnp cluster
D.P. 8 to 22
bc1qxsafg
D.P. 24
12xYe
Domain Register 1
Registration: Website 1
bc1qgahk9
bc1qgcfx7 cluster
bc1qxlj2j cluster
bc1qvt87e
bc1q52ug8
bc1qgguuq
15pUt cluster
1DXbM
40 BTC 4 TX $325,121.20
609.4483 BTC 39 TX $5,735,866.97
441.79183399 BTC 52 TX $3,520,272.44
Exchange 6
5 OTC Traders
3 OTC Traders
1 OTC Trader
3 OTC Traders
8 OTC Traders
Defendant Property ("D.P.")

These four clusters are connected via cluster 1LEvp (containing "Defendant Property 172" through "Defendant Property 280") to cluster 1BHnp (containing Defendant Property 8 through Defendant Property 22), which was involved in the laundering of the stolen funds from the Exchange 3 theft as described above.

62. Cluster 1LEvp (containing Defendant Property 172 through Defendant Property 280) is also connected to BTC addresses previously named in the above-referenced forfeiture complaint, *see* 1:20-cv-00606-TJK, and attributed to thefts by North Korea. In spite of the actors' use of VPN services to mask their location during this theft, law enforcement was able to trace logins to an IP address within North Korea.

63. Ultimately the funds from the thefts of Exchange 3, Exchange 10, and the recent thefts attributed to North Korea, *see* 1:20-cv-00606-TJK, were laundered, at least in part, by the same Chinese OTC traders operating at Exchange 6 as illustrated above in the Venn diagram. Notably, there are three OTC trader accounts that received funds from each of the three events.

64. The addresses contained in cluster bc1qhmv7k (Defendant Property 147 through Defendant Property 156) received BTC from Exchange 11. Cluster bc1qhmv7k funded an account at a U.S.-based domain registrar ("Domain Registrar 1") that registered "Website 1" on or about September 26, 2019. The same day, approximately 62 new accounts at Exchange 11 registered with Website 1 email accounts began receiving ALGO stolen from Exchange 10. The username portion of the Website 1 email addresses appear to be a random string of characters, as if automatically generated.

65. IP addresses logging into this Domain Registrar 1 account resolve to a VPN service. Target Actor 1 was paying for services at this same VPN service with stolen BTC.

66. Open source research shows that Website 1 appears to be a restaurant in South East Asia. However, it is a common tactic for hackers to squat on a legitimate business's web page or make one unbeknownst to the business, in order to provide cover for the hackers' nefarious exploits.

FIRST CLAIM FOR RELIEF
(18 U.S.C. § 981(a)(1)(A))

67. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 66 above as if fully set forth herein.

68. The Defendant Properties were involved in, and traceable to, a conspiracy to violate and substantive violations of:

a. Title 18, United States Code, Section 1956(a)(1)(A)(i), that is, by conducting financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, violations of: section 1343 (relating to wire fraud), knowing that the property involved in such financial transactions represented the proceeds of some form of unlawful activity, with the intent to promote the carrying on of said specified unlawful activity;

b. Title 18, United States Code, Section 1956(a)(1)(B)(i), that is, by transporting, transmitting, and transferring, or attempting to transport, transmit, and transfer monetary instruments and funds from places outside of the United States to and through a place inside the United States, and from a place in the United States to or through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, violations of: section 1343 (relating to wire fraud).

69. As such, the Defendant Properties are subject to forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(A), as property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property traceable to such property.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Properties as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that a warrant of arrest *in rem* issue according to law; that judgment be entered declaring that the Defendant Properties be forfeited for disposition according to law; and 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.

Dated: August 27, 2020

Respectfully submitted,

MICHAEL R. SHERWIN
Acting United States Attorney

By: /s/ *Zia Faruqui*
Zia M. Faruqui, D.C. Bar No. 494990
Jessi Camille Brooks
Christopher B. Brown
Assistant United States Attorneys
555 Fourth Street, N.W.
Washington, D.C. 20530
(202) 252-7117 (Faruqui)

/s/ *Alden Pelker*
C. Alden Pelker
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Ave NW
Washington, D.C. 20005
(202) 514-1026

Attorneys for the United States of America

VERIFICATION

I, Christopher Janczewski, a Special Agent with the Internal Revenue Service, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing 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 27th day of August, 2020.

/s/
Special Agent Christopher Janczewski
Internal Revenue Service-Criminal Investigations

I, Christopher Wong, a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing 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 27th day of August, 2020.

/s/
Special Agent Christopher Wong
Federal Bureau of Investigation

I, Thomas Tamsi, a Special Agent with the Homeland Security Investigations, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing 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 27th day of August, 2020.

/s/
Special Agent Thomas Tamsi
Homeland Security Investigations

Attachment A

PROPERTY TO BE FORFEITED

Funds associated with the following virtual currency addresses and accounts:	
1	Order ID 6918d31f-097c-4afe-8d06-054dd38a34ac
2	0x52cbb6be7ad204904486f89e264029c94525966d
3	0xeda8b016efa8b1161208cf041cd86972eee0f31e
4	3QAmBJmK4PbEg1QeKoVYWcP5LGUsjRodcb
5	0x1016b7835d409692e02ed2035e053fbfb4602982
6	0x46705dfff24256421a05d056c29e81bdc09723b8
7	0x2DBC0f6B71e341C7Eca01c5287Eb57AF3038A9c5
8	1BHnp77MqZGGFaCGQ9J4GhLstPUeBshVcc
9	bc1q9zlw8sp3qs3qtp9mswg68g073x65lm7v02ta5r
10	bc1qpnrkqlyznqdw4qpuzzpnqzknqsjxychct9dq7f
11	bc1qz00xgh24knenhar7adx3tu0lfe6fk99n7w05q7
12	bc1qx3umk9rwzl80z0qyt49ajec4ev36h8jrdy7ghn
13	bc1q2cf3hammnfw3dlh7rsmpmmqyvhlpfq4n2hys4p
14	bc1q8cn703h86phx6rnphx7wjq09lsahx8jcrs5ued
15	14LcoKEFrtnGzCSabNZneJqRg2zcFvTRRw
16	bc1qk2h3tgx5mspv9vjh08lhjfqq457jdkcu5vw64m
17	bc1qllhp9pkpkae7mdw3n0z2u2znjv4f9k5dvyyyah
18	1As1nMhxhnN3HM9xK5DPmBS4A8E9RgXZXT
19	bc1qh5jnylxv5030qhrls6j6uu4cufg0kjnk9psfgu
20	bc1q87cxpu5cgq07ywkyv68tcl6tfykpf2kdzaawh9
21	15kNzXrVhZ7ZJ86GLyGCUWjDM1EYDNjiSz
22	bc1qnzhecl9mwc6nv9plrgm9hph7ldm0egjhsa80gs
23	1DXbMUZwLea1jiYay1CaCNvYwR3chmVfvf
24	bc1qxsafg5y5tnt7w343tec8l4mehzwhkkqwzvv5yf
25	DCRKBSHNTY7OCZ4MTR5MWXETALEQ2DEK6SCRX3ROMLUCHRFXBZ2D4YGJUM
26	D6OVTBZHNIJTKO5YHKKA3EK4ZXSGW4TVMXIAGY27JVMWZ37M7GZRC2MU3U
27	D4G3AF7I5OVF3KIGF6QBHHMAICG5CWQSW33NBCKUGKZAXH4BISPMJDY42U
28	CCZMHKP2AFW54II4XS77YBXLA5SLMRXHQYRRFRZA7IE43YWDWFZYF3ZTNQ
29	DAQH7K6FCKAWCSSI3LADZQXCKDHPOHF53CH4FT4EPZDHPCMM3SQEFAAX34
30	CLTKYQRL3Y7JEEKGMFMJCX2JGHDZICNZRMTJ53IBYFLPWBHFY6H6IODURI
31	DANFVITT5NE5RTP2F5SNOBVNY27ZUFRMAZCH7DNL3RUDITC4H5F63RCQRM
32	D6KLGE5R77WMGKMHBQNR5SBKRVSVJPKVFDZZCCS7J3LQBS4TN7HKHHTTKE
33	CUSSUT6CAIUUCUFG52ARUJAYFWNYR4WN6OGAIWDL3GIE4GA7MTGNW6BQKQ
34	D6DYVN6KI3XNWAPOTQHPE77VB2AOVIIUXMM7TAYKPBQFGFTP3WP2KGE6AU
35	DBYE2VOKDSI5PJUNBPWZNTWSKRHU5NB7OLABDG7EQXHP3WUH32DUYAWFFE
36	CUEENNYBXTMZXD74HDNONFYNNSI6ILB422T2KRGELY7PPQXMBUN4OKFRP4
37	CNYSZPI5M3APBKGR2XY3ZIYCF4VWS55VGK5UD4YM2H3OP52AEDO26NAGWI

38	D4KNLVFGLJXX7ZLN43PUEBVQQSXZCRSKUKU7J54ZZFDF23SPUA46DZHN2I
39	CZJPZAOJVSUFKLTJQYVBY6N7ZIMGIVIGTMWHVWYFRA43MQY4753ZF4JJKQ
40	CRF5NGXVQTETHSF73XWLMIC4MJAIQWJMWPM4PKPI4RVYT2I25OLCFJG5PA
41	D3VWEM7UISBPKO4W2IEQ5PH66GBSKB73ANWZ6D7DMWUPC7PZYGN7KS7N4M
42	DBNG6IDQWWBXVFTSNBCNHB3JVQZ7TWRO5FVUAGQPYD4AGZGGQMCUO3XI3I
43	D47R53JAUW7ZSKYP5BFT4V7SFTSBD65BFJH7C6LAC6ZQFWQWVBNTG7LQ3E
44	CWNF7XCDPYS3WSX4ZRWJPURTYPW2IB5OEV4GAQMDKKAQZ2C27FHATGYGLQ
45	BZ4O57CAYVH6EYUKHZNVEGPTICFFGVIAOQCYKXZLZJIGFGZGKU74VVHRXA
46	DADW2L2XBZBBJNWJ7LEBNDGBIEQXYCQLINU6HAJNH3GUXEQN4ZNUPI4BS4
47	DBNNBKS3ULMJS6FSKWOHF2U6ZHIAT5VJLEWM2ZPUGLOCL5SDIVUKJRPNJI
48	CXQNFOTJZRMJEGHQ264Q3DVKDITP6XCXEGVVGWSYQFADPKIZI5332FRU5A
49	D3PLK6HOOXTM2LMRMTXAL2SSD2KGWBQAP4HEH5KNJ5YD5YJ4WUW3YXYGM4
50	D2C7ECOPJYOF4RQRL42THGXMNZO63FJBWMPCTHN2FJYMDXNDWLUV5564NI
51	D5HJ2JXFYBMER5AF7KECCB4BFQLALBCEHUNGKCWE7C4QIX4M4PBFSSD3DQ
52	CVVIHBHVJGLDQD6ERJIYY5MZ7VQOJF2KXFI6URUGPFMJNBU5VAKCZS3VIQ
53	CTM6PDELXLAYJLVZY4NH4CUUIW7QPGRYY4EDCAZELVWNNKNMDFVYB56VOM
54	CJK2LWFPIAAFRS65UDMYNBVXHYIU5WSTLV6LZQNQM6UGKIKPC4KX2NAD2U
55	CSAUJTTXE2RDEDP363ZCD7NKGBN3LTUWNDER7TOPKLL7TRK6CFF2XNVKL4
56	DA26WFJD6ZPQW3MGPDSFNIKYXPXCURRG43DYPMVJLZCRA23IWZVT4LT42Y
57	D7LTCFSH7XJZQW7STL5USFGAFKREGYD3A2L33WIUPD5RTGWEE35YORTFII
58	D2LEEU2YOGB3S43VTRHZLPJN5MUNIYH4YPQ6BHE7KQBXJLKUHF47Z6WG2E
59	D4XWPOKN6DZLUV6E4GYB2UL4N4FCGI3TXQWDCOWMTPM373GBW55XDOJIKE
60	CI2J4IJEK3SYOTPZMDKMRXBM2EYQGB6IIRDNJCXCNSSINPZYQKA5PSFIDQ
61	CQMTUOGANIIWVB363R4Q3Z4D3WHEUQ6FAQPFKDB6MNWDE3EJ45NNNLHIT4
62	CYEFCWI2LX45XP33KYMCEVXYRD7GZYZJZGA3VIZQEBMDL4COKUEFRADPFY
63	CYZM3UXFMA3BUKOTG3OMVZ2NUO3UG53TG3AVAPMV47WSISU74LG4GW3RBY
64	D3IQLA3YSSFCKHWE225666SR6XDJOSAJYBP34QFDQQNLCP6ZWL6U5DSI6M
65	CIO33QCAX5EDDEDX4R3BW4KHRJBXLRU67XJ66VTMXJWPG7LAJEYT6IJEWI
66	D2CO3KW2KDTJMYJ7CHXU7N7BSETVJORCZSUAHZEGQJBJJ6OGAN5OOZYAHY
67	CXZ6HJZKKSTKHJHVVAFQGMBUESHFYB2ZI3IVME6AYJBWUSLGUTP3QRQOZ4
68	CKGZTGNSSAJ4SGYOZOQ57AHR5CQPCCAYHQIYO64C2VAYJZVCUASPO422GE
69	D2S4RV2U5CP3UFY4ROIHKOCJZEZ6EXW43KVIJQXZ53UVUX45FR3KC7J6WA
70	CIYUUUWUFUO3KOU2XN46EV6DE5KIAF6UKNR5F4H3NVOYPWCX572Z5XABSA
71	D52ZWKZYL5OV4DACHQXFQ2MF7Z4RVVYBZ7XPOEK2AVRRNSR6LVVPSNEMQU
72	CHCWVJET5CNBHVE6777JVDLGCPUTES6PQ65JHGFT2AMJQHSBKQUFF5BEQM
73	CTLOI5VNBZTRGCSHZ4VSVSCWOUYCK42Z6XD3N4GLEQPEBJTG2S4GXT7GSM
74	D3M2TNEBRVCOVGTIRD5SNVVOBZPI7RCS6OL5JAE3XDBHPEJCQLBWFJYNFE
75	CXZ45FS3KXXGKNGDQYESCS7F6P6NE34FFFZZUBD4V4GD2S7QUUW3IGPHSM
76	CZOI6Y52ZWD2FNFOUGZJM24PCSMKYZPDJ4KCUH72NIPV5435UHSQ5T2NGI
77	D4A5RKQ7YZNBQ74U2DZ75JDG3E66IRCUKQSFWV22JH3A662CVK7BUI76LY
78	CX5EQ2IBGB35U235BC7SA7FNAKBQEREIZ5DBHXCVZZUNF4XTOUVR5FS3JU

79	D3K76QIQJWN5ZNLSW4ZZCSWR5CZMLYRCIFSU3ZVVG3XDLKKNQZSRRZPDR4
80	D325OBHIQ2CJ6JKF2I3GJWDL5NKVC4ZT27FSWX3H4U64QVGPMRQVEODC4Q
81	CWIQHIZ6MBDZ76QYTAAWX3Y2Q34NMMBIVVB5E4RSEYQP75LMNYBFUYLAJE
82	CYNFLBP6VIT4JSK6QRYAU3O7THPOXDWLGEH4VLRMABLS5NRNMPRSAAWS2U
83	C7NA45LM4JUYLQWPIBMC5MB6CQMX2IYCGQSJAOPCXUUMWCQBDNTTXUSIDE
84	CPANMWE6Z4Y52DHDFRDGGNYMAXV2FROFEDDEZC7P74ZS7CZVK53T4QTWS4
85	CWBJKZKNW326HB6KJ2UAL3M7UNOFMVAV2ZJPCC325EKYKWCFCGKRX2TMGQ
86	CXZ22XE2N6ALFPLYLOTQKXEBP2TG7R6JNTOSV6J5MXRPGVYYNX36REXJKU
87	CVNDGR3MVJRILZ4UCBCTRFCCQ4PV3FL3C3K6MJ7JVIQHWREKJX64LSCDUM
88	CNMYEZKLIFG3WA673H2JPC3W5LUYS2ROIBKS7P2NN4SABXUF5G4MMGHVN4
89	D2GBI7YXHWHPI6XG2DJIWHNQHGTYYGSVECVI3ROWOFNVOGKPBXNXQLGSFY
90	CYD5HSI4LC74R7DRZNRBQNS6Q7ACNCOSO4I5DTMH5AK3XQJPNOSBNDYDPI
91	CQ6FVHAG2M5JDS4OILOKDXCDU35B763Z6C5B7ONHRZ6DLIGTX54XCGLWP4
92	CZOAJAYS6MT742KH73RPB7QB2NKWUSZ7Y3BU42JRPMO65WQ6KEYM4332SQ
93	CZZHZSSX3UL2GYV4SPB4WIDRRV67QN3VN24D5YA3QZJDPPGKXDGNFHL25U
94	CW2DX3G2HDDYRP7KZS7CPMCUFQTODTYJPKUJA2ZGA65OOF5K7I7PJLJGRU
95	CVVVHGHMFPO4PXC5JQMYHK7ADRY5D2TOPSSRHRO5QLORRNEDER6VN32Q24
96	CZ6KBPPIGHDBYWFPJIRRAXRIN5KQXXBTWKDOUBZ2PWU6Y7ZIJH4E4UDWNY
97	CMBY2EENNVKEFU5USWCM7UGMHLKPXLOWG5HI36MPRAKOS3D2MOUTE5M2DU
98	CYAM42TJ7SS3XHPVBVKFT7RVZ5SJXFFBXMI73TB7WYDIIPVPBB4ZBDMMWY
99	CYMNKNYWZVVU4ASE56CIOYILPKNJIIKN5MKXJMPALTJGVPO6TBQED4GHWI
100	CHOWLPLVNA3BZ2GNXJZV2BCR7XAPX4DP7RCX7I532LCGON44SB4ROLC3KU
101	CNO2ESTI7WKYHRLV5K2TB4QF5P65TCH3ECL6EY4ECZDIJWAEPNTD6BYJJQ
102	CYHRSCQUMNC7WVLMKQK55MHDMJKYG5BPE4UNR3WZRYM5B7CZWMVHNNUJRE
103	CJZUPZTH7RJ6MUQKFKYJV6IDAFM2L5ZJSYHDUT3GIKYBM3B7ZMVCHKF5FE
104	CU6Y6THUUQZR72J2BQ3P5PVXRFLNHRZRPZZ4YUZQAPGVZ3G7PJZBLVWLLE
105	C2QDN2STNZIZKFXNXY6CBS3HWU6B6CDAXIOE3PADOVCNH7YNEFRGZPZ6E4
106	CSWL65ZFTFLSS3UMOODU3GI3FKOE2EKOZY6ON64U3XKILWR322K2D2OEFI
107	CTUSJ4XY3WMD4NZHVIRPCRPLZATLJZQFAHJC72KSEMAHHLDHMPR7KKAQB4
108	C3WYI3ZP57HDGQMKCY2SXUP7LZGKGWKAPOF3NEESHKRXAESXHWMAUY7UGU
109	CO2QR2XZAMIKECXPFL4OFFP527MAV3LXPQFVRWO4J7ZAICICIRCABCG2TQ
110	CSTQDBDWCF5SWQ22WBQXK2VGGEX2DCR3OQIW3KTOFNIR5N5M6W6RW6D67Q
111	CY4EB7MBUCMQWIV3Y3VAZDYWKNUZKIRJCKB3LSUXMJF6WQZ35AEH3L6NWQ
112	CRLVEC74LECHRNAVRW5KJZRSL6UXCBVSCGB3BF77MSXOKMCCG3DQDMJNRY
113	CRRJ5CREC7RQJ4S5USSHTIPICVTMWXDQHZ4LRJJPALW7LAH5KNP5PQX4CM
114	CBWBXDJAIALZV6YUZZY3LY4V4PRNAS5QPOD24HD4N5JSQAU3I2XZC7WVGE
115	CGDMC7ZN4WWCKAGJWXPCFGSVMEXQ4LVFMVP5I75HGVIMRRO5V4ZKFSGMW4
116	CPFQSWGCU4EAUFW4VIPIK7XOYAXGBL6YWBPRKRLP6E7SHSPO5ZYX3QLQQE
117	CVWRZ4LPPU5PNPU26BLXYUVSYJLPLPF7TMRQWAOQIVLWXSBMIXUOZL7TIM
118	CLV7CWXEFJUR6373EL4AI3IOUK5ABF57IBXGJEQT7QK4OPH36YGPURW3EI
119	CZERVM2EK2CSLV6OHQL4JWSAIOCRBT362WSFP73KJ3UVB2LLBVW4HJM7AI

120	CRBXNJRTE4DCWVOS5XAK5SQ7PUG4TF5FIJ52VLTV47SYUKAZC2GLG5OEVA
121	D5OSU5G4ZQBK7CH2TKVAUCSSQGJ2NUGTDKCQUUA7U7SKMHS2FZQGKFJ3XE
122	CJQU3R7PDR7RI4DFBO6NTTMGIZHV3C3M6Y3SNVFL7PKFTWCC533DPNFCUQ
123	CL6TF4ECREQ5QEV3MPRIXPS6NOZ3BWIAVASAM2LZJMNODBALNPJPGOLPGE
124	CXS2PRGINQWZIL4YZCOJOUBJRHGG4DHT55X6W3QW7RPFVYXDQC33KAAFKA
125	D3YUGJAWBFCAG3XHVYL4X5VKSLNHLXD2LNKLXFCMCNK6QUKVGIOCQAPIBM
126	CTSLGWCHGT7WK4KHV33T3YQBQZIUIYN5O2UHZYWJEXKNFK3TVX6SOWJUHM
127	COQE3AXY7IBHWJS2T7EWJX5D4D3XF4J5LFQJ44XMFB63B6L4RIKB2FY7OM
128	CSNYBUJPFPO6LPSNW5FV4LRWQDY63C2JV7ON6YOTZUQP7X24HBAJUFOB4I
129	CWF6VMV4EGAGD2UBYNKLM3373BSVLRTS4CYSJ5FSMGBKLENGHXBMDHFI44
130	D2SQTR4G6TPCMA3V2ICHTRWOZAPLZCFZUGUJX7YIWJK4D2YQWH2YQIEW7A
131	bc1q5gv9fjpxgqurzzekhnpqa6pnq98uhu0wumcnzh
132	bc1qtdgp95m5x7w4hryp4ctazf55c0hwu8vkw6s4c9
133	bc1qwm0dy7wkwnkkwvfgejxd3geaecdsj8l343at6j
134	bc1qw0e7ls4ttus9r6j32kn8078q7sgqzletuvzxa2
135	bc1qhmv7k95xhca2x7h20yr7qmc0kvdfwqwlfs2cmv
136	bc1q9xsunf8dqewcujyjt2pyz24nznjkwm29569wqn
137	bc1qfvgfvckc8dykn2dee4r40g478jcke6k3gsxwy5
138	bc1qhvwnql30la8zekeyd6sq6w9gultvacfmf0x952
139	bc1qvhp33tdgpdmqcwfztsz8rjgr8ygjcssdpld68x
140	bc1qf57cnnl55ar8ae2zm9wrgrpz7z8t3e3vxmyq0y
141	bc1q788lywseynl95asx53t652jlzwmrmj66qdakaf
142	bc1qlrv7qfwxd05pq3jvlqfrqf33vru7efrwt8le7n
143	bc1qnnre8nu263wn8yrnc0dqqv48530mzn06vsg5vk
144	bc1qlm409u5cegge54uxgyz7f7zn7v8cc49fmtzwwq
145	bc1q90sjl7ykuwcyrkl5t3zexpfv0dqtm3923eqhxk
146	bc1q3z8w5jmgzdx9nfnjv0xxtvqe354t00xppceaum
147	bc1qns6q7kjewls42qaf32pq4vkn6p5746ut602t5v
148	bc1qzywf80ap334jvjfscqjvfuyyhypxteal2w2s3j
149	bc1q3lfcz7c3uw34825chdzu0eqmvcp230glfcqc7m
150	bc1qhtj78mlqv6a3ey0232v2kypq8m6udhy670cl7c
151	bc1qwldjepv2p6md583xd4jy4hkrhyar320a9n4sdz
152	bc1q5ds8sjtk8vdzzlkrpyf5zuw9txlujan44ny525
153	bc1qnkhzvtwcgt967uttmdg9xr0rspk8ehqcp9yzxc
154	bc1q9ecf5qkmza7nym4c593ktr4lnruyk5q7alhxmn
155	bc1q6pdu9pcdeqzsr00m3s5jy8988qp9uaypvgh4f4
156	bc1qte606xucpptfkdctp0pmmxe5kdk9g03m32cvvl
157	bc1qxs6gz66e4rz37cw78zv6qugexs3t5mk0enmf39
158	bc1q7tnuph04knh40dkphp6cktakq56usnqzjkfdxn
159	bc1qefc3hgtwszqrl8jlkauewshc5t60w72tz00ktk
160	bc1q4h47x948cgwuyjtdytjyr974udr2y4jvlldg05

161	bc1qgwqjy3ens22ecl2em5en7cqfdyl2mfrylhnqhf
162	bc1qy24rqhjsca05gmn4s4pmg2gqwv0ydehprp3c7s
163	bc1qe5n20acas6akpn2g0jxuk3vytjkvt4jh2thf4k
164	User ID 37312566
165	User ID 37039524
166	bc1qkr8m4wvndesu4v92ulnyxeug4yta3nyamye24s
167	bc1qyauwwxkjwq3rq0vyj79s3k3xlllvt2fy7wa9zk
168	bc1q7ckw4s5jra70f3t0cfm99vlx4j0ewym0snanhr
169	0xeb0e94dcb4a8be477e11ca35b043be4b301f735e
170	0x8bB65FB263585D04a139D4213CC6A96637FD1Fc5
171	0x742B115424Ccda93d9228cA9aa56ec2442b94CA9
172	1LEvp3YQYERyuDSpV7bHAgqHaXhxDme59R
173	1ANKiPsYo12uek8nKPermBTFEHK8tVcT22
174	1MfqK7q7YYYGnzCQpkkgwsr1vvGBpF4Gp4
175	12YcetmDe2mWeRQhF6GKixFqDxxRdoSHUw
176	154Z1J4Lf7Fedsqx6bNxs7CVhLQX7LqJVt
177	13PCPwJX8aLWKq9hJqcaeFTFubE7WdnbBN
178	1JwueJtsYonmkyfmaK5KMZBgVZz9nPBuac
179	1Ya3Vv1si13TayfqhTH5ueVpmZdt2iPzx
180	1LzKztXkfDZYkH1qyHyBTb6yn4vQzysHh8
181	1Ee3aNyosfXVtgGPjsR2nM2qUfqFKX6LzE
182	1CtSWX7f8i2Lz91gfGFL67i1nxG5Prn4rR
183	1NzecyhqEx9YFL8brpnFw6ermEfsEayDt2
184	1EPeNq1P2WiWamEGwTZ2U4jCoFp1SWhCAp
185	1K8WCS2Hkh61NQZfRfH9mn69GMYV5qRwym
186	1M3NpgnpbazbcYFTVz5f1ThtPMSHMvQpUF
187	19m1HvBscdHjux66CUoPEyiyp7PM9GxcKQ
188	15voECtiu2K4nccwbMYwpWuUij8Jp3Wt3r
189	17T2TijGn2f4basCSMdRHZn8eMaDKQPzuJ
190	15kVYmnKkU4XkDmgKEic6YKXWotLwkn6Zj
191	1MT3gfWChDNWJYJ7PMDDxGd9ttBHBm5Aci
192	1GsLNuub5FT2QkBw68VZ8N9nJ53WTVj6wi
193	1EMgDFko7FYGpfqY8CkE1GPGVRCvZTuiAW
194	1Kd8GwUWAhJcskDhcXhP8b2yTk22tWxeQX
195	12khRBotv54N235dwyeouYfYRnR8f5ePM8
196	161MfHMaPMP1NeY48XHuiq57gavJQmASEe
197	1Z5KPQEj7vReoVHFc674QuS7LWnQ4sRaa
198	1EXnSic4ZsD1d7pjt6u5Xv7zK3BCm4rwvZ
199	121J5XRTBSrt5783jW55HzXvEMHmPAoTRZ
200	188jjzHMzW5tTabZe8foCpD4rrBq884Mwe
201	1E1akxCiziVymLK7gUod2XkeGWwrWbzp6s

202	1QGAGP93w4GjQGGCCqrjfCow9D9TcwYhs1
203	13W9T9kj6XDpHpvygKbzxJvVQkW2AwnTb9
204	13coFqMThfJ3HAUh9mu8smskHEK93Bu8iB
205	1RCi3TWt4ikPny356HbJDv5t6cFc9j2JX
206	13ZgSjJ2G7JewHUnorLn5v23eoiDBsbMAa
207	18bgaesGQtGDvXThhThR65skk3g86ye135
208	1418puf9SVtQNzVF2P4Uw3mB4c9rULqabq
209	1Dvvir6yhwWbXCDvQXYRsWNcp8CTpUHPMx
210	1AJEwAZosXzuKrYM4MsHYcULofqDaMdDtU
211	1GhEJdP4GyiEABBiBse6tbe128QPfDG9rA
212	1Gkc68BLTuUitkuP41Z1PgxJBwb8HHZtuA
213	19duo2vntPtnjvq1MRS19LKgmJ4Jrj4bQD
214	12Eg4vXMcYgZLrWduymy8EmsUEK2etG9Jj
215	1BQFtGbQoz3gmV1WvEbZamPj9bPEuJLLsN
216	1KEmCvVw4DGhSxgZ5HHCw9b57kZ61Mn6Rc
217	1NZgueXDQUm2hcBCnAApNUwsqPAPmVx6PY
218	1PdRxEgyS4exU17Skg1L9Kh7FmRZxKFHCR
219	1DpuH87nZfwnWYwrxuqe5dhW5DxJsL3LrZ
220	1Nzu3Jby4mtDMREm3aaWGNbqRc3h4CqD3X
221	1AHr84HcNj7U75DntNTZVJvx2ShAAE5SC8
222	1GCdjgqnZ7jJ4tKZLftrwZQGWHnprTDj1t
223	1Fmn17TPqAmCpXeUJFASxQ1s9AJyP5iPV
224	1JJNhoRBnB1dsZZJMJ1m6LtEdgtoWZfa3J
225	1J6H5YAJ5VfrCJnpwVpnPpcoWcENRZFtYs
226	1Eg1w9Nnf3JS7FC5WLFrpqdaoxfpUqCrWZ
227	1AeuzJE4Gr1qSU7EYXWEKaREPsGFLBHye5
228	1DJ3dNyUcRbFRC58VGF8GR8RUR6gc3jVWg
229	195VRNyucLi4uLfMQj6QSXWLVCFtT7wg3f
230	16ePr6UqtE8M3s3WQvxR8P3QtdjXRhxKfg
231	1MbAYj5FEv59tgTxFDfRDvuPrgPJBixMqM
232	18Nh9RZpZDp3PVP64x4iaJKgejY6XagNX5
233	1G1bxjmWfjpA3NDixT4U8QEyvtNyQxYLhG
234	1GZ3B6dYLtt8k7GUZxWhcGA4P2x5AvinYy
235	14PxGCQDgrZtVG3MvpecXbqWZZknRqvf4b
236	19tbULYdzocrWhY1rBJXxn36oQrx9otqZA
237	1LMumzf4KgPdsRHC2aSvgz5136Tt3HVqrB
238	1QFaLxx9TGmH6nS9ZTcJJwTtJd6Dr7gHi8
239	1FEUR7gYNo62GZLfZuF1AoCo7k6nNV3oNK
240	1A5dVQg4xBnBhdbGECdJ6tJL5AVNBywS8V
241	19ZYnDYCQSCSLZqCv9PV7iQa5dwcnFfLmC
242	1mqZLJbqQLVHye9AdHx2q9DeeEGnx1Ucq

243	1E38kt7ryhbRXUzbam6iQ6sd93VHUUdjEE
244	1HkmNiYEAj2hEktLK55qhfjTdurAVcd5Dv
245	1HHr5CaguMUQPPuRcn3E7CzQEUr1ANbQjv
246	15nEAKCqhsc9jemcamXrV34bEkY94ATwwk
247	18jNW8GKqv19mtUY5p27EpcaUUS2YcMs1R
248	1HorBze2ySoCE1Uf6tuKhyL9wdHGGBRrUW
249	17YrGQ1RbWBeboPkLZ2XWZHtVP3ifQFNCz
250	1GeDEW8rUCLnp73Xz9sKCvVE4MwtnPgXs1
251	12fbGWEF11sYjLK2LXK5nrZAHurEizdEWG
252	1EPzw8Zv3SXepEfgj5SxYzCmmBqeaiJq1W
253	13kFwLpg1KkBEmJyh1VZuzgRTBdeHW5ic8
254	16RiuUih7GTMwd4TGYxQ3HqFaMzNKJhUd4
255	1E8UAStQHBxUwbHgaKCycL6w4bPvYhVdZN
256	177Cy2BwkuBJhwqdHQGVqGr2X3tQyKfz8Z
257	18juhhXUko84Q7yfHM7t7MZ3xPHSy3CaGm
258	19k8sMW98S7ouVidJzLvHFibb1MvMv7LsB
259	1ABxRsdAYxcP7EDBqG88g7YMUyxHE3XW4h
260	17k1tXLo6n2sSi7CgEgBSEbTJdngyhfyyZ
261	1PcXunfRsrkiTfmiqZoY4EbVYqTeSy77Ex
262	1GDdzW4cqfuRQWjSumfUg46yyqMjXthrvV
263	1AddLyqEcTj3D4YMTrU1dwanU4jYw92Qxx
264	172CY2EKYP3ZSrJC8mc15BQSxgjrjv87NA
265	1ELL8mm8bCRXB7tSMhGVmjamo2mRrALjL7
266	16bUoLU4wyPXpAp2f44fjSgRLW2mBtiNnE
267	1GZ1Gwe99SdB3iGLQfQPYTXoM1f8xhNYBe
268	1A4oTddEWJHirmijSboUqsRSXWQpVxy5Qk
269	1GEZAVEW8WezL2Pnro35TC1DbjTa7waKmR
270	17cHkKEyKCdCf6GdSFTdzWf3twp24boB3w
271	1AYidQgj3LJP7zjXNHSeRq5siSnXhawGRg
272	1Jeup4LVUMC3hVvFXUf7rqUmE43vnD53g8
273	1AkCjm2EeuczickGL6SHdsmnoLpC9SDAf9
274	19xYNAKa9XWyvHsfUZNcc44RSwT6nXcDoD
275	16TwdEPrLpMe2zEyDNRZLccG7agEbnBsBp
276	1BDh6aKK4t2JyQJfMS2ZAfp8AGZZbq1hqT
277	1itbSqDkSrHCtZ78GnA1N1ccDaXEcmSVd
278	1BCq5EfSUYUHPkwp4xVCBXiaDx73RvhPDZ
279	1QocxVj3j8nFMnsmKxt68XvZnXzgqgxqN
280	1A3ponnkRfe8x4yoFk7W68H4gcZtG4uoiP