UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	**CRIMINAL NO. 22-cr-22 (RMM)**
v.	:	
	:	
ILYA LICHTENSTEIN	:	
	:	
and	:	
	:	
HEATHER MORGAN,	:	
	:	
Defendants.	:	

GOVERNMENT'S REPLY IN SUPPORT
OF REVIEW OF DETENTION ORDER

The United States, by and through its attorney, the United States Attorney for the District of Columbia, respectfully files its reply in support of its February 8 Motion for Emergency Stay and Review of Detention Order, ECF No. 9. On February 9, the defense filed a Letter Brief urging the court to uphold the decision of Southern District of New York Magistrate Judge Debra Freeman to release the defendants on bond, subject to additional conditions and monitoring, ECF No. 15. The defense bluster in the Letter Brief notwithstanding, the evidence of the offense is strong: the government seized stolen cryptocurrency valued at the time at $3.6 billion from defendant Lichtenstein's own account, an account which directly received the proceeds of the hack – a point that the defendants' Letter Brief conveniently glosses over while complaining that the government lacks "direct evidence" connecting the defendants to the specified unlawful activity at issue. Similarly, the Letter Brief attempts to portray defendant Morgan as an unwitting bystander to any alleged wrongdoing, when she in fact played an integral role in the money laundering and fraud scheme. Furthermore, the evidence regarding flight risk (access to hundreds of millions of dollars' worth of cryptocurrency, overseas ties, and fraudulent identities) is highly

troubling. Having now been charged and seeing the strength of the case, the defendants' incentive to flee is dramatically increased. In short, no condition or combination of conditions can reliably ensure the appearance of such sophisticated defendants with the means to flee and ample incentive to do so.

In support of its arguments regarding detention, the government proffers additional evidence to supplement the record made in the proceedings in the Southern District of New York, and states as follows:

FACTUAL BACKGROUND

As summarized by the sworn agent affidavit in support of the criminal complaint in this case, ECF No. 1-1, which is incorporated by reference herein, the defendants Ilya Lichtenstein (Lichtenstein) and Heather Morgan (Morgan) are highly sophisticated criminals who conspired to launder over 119,754 BTC[1] – presently valued at approximately 5 billion dollars – stolen directly from a virtual currency exchange (Victim VCE) in 2016. *See* ECF No. 1-1. On January 31, 2021, the government decrypted a file stored on defendant Lichtenstein's cloud storage account which contained the private key information for 94,636 BTC of the BTC stolen in the hack of Victim VCE. This BTC was worth $3.629 billion at the time of the seizure. The government also traced proceeds from the hack to multiple accounts held by both of the defendants and their businesses. The defendants are believed to have significant additional assets, including the

[1] The virtual currency bitcoin (abbreviated "BTC") is a form of value that is able to be transacted over the Internet using Bitcoin software. This software provides all necessary services including allowing users to create "bitcoin addresses," roughly analogous to anonymous accounts; the injection of new bitcoin into circulation; and securely transferring bitcoin from one bitcoin address to another. It is common for a single bitcoin user to control numerous bitcoin addresses, which are stored and controlled in a "wallet." Each address is controlled through the use of a unique "private key," akin to a password.

remaining hundreds of millions of dollars' worth of virtual currency stolen in the hack that has not yet been recovered. The defendants also have access to numerous fraudulent identities and documents purchased on the darknet, and the ability to easily acquire more. Lichtenstein is a dual Russian citizen. The defendants have established financial accounts in Russia and Ukraine, and appear to have been setting up a contingency plan for a life in Ukraine and/or Russia prior to the COVID-19 pandemic.

1. Introduction

In or around August 2016, a hacker breached Victim VCE's security systems and infiltrated its infrastructure. While inside Victim VCE's network, the hacker was able to initiate over 2,000 unauthorized BTC transactions, in which approximately 119,754 BTC was transferred from Victim VCE's wallets[2] to an outside wallet (Wallet 1CGA4s[3]). At the time of the breach, 119,754 BTC was valued at approximately $71 million. Due to the increase in the value[4] of BTC since the breach, the stolen funds are valued at over $5 billion as of February 2022. Victim VCE reported the incident to law enforcement and cooperated in the investigation.

U.S. authorities traced the stolen funds on the BTC blockchain.[5] As detailed in the complaint, beginning in or around January 2017, a portion of the stolen BTC moved out of Wallet 1CGA4s in a series of small, complex transactions across multiple accounts and platforms.

2 The storage of virtual currency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets are used to store and transact in virtual currency. A wallet may include many virtual currency addresses, roughly equivalent to anonymous account numbers.

3 BTC wallets and clusters in the government's filings will be referred to by the first six characters of the BTC address associated with the wallet or cluster.

4 The trading value of BTC fluctuates over time, depending on market demand.

5 The BTC blockchain is a public transaction ledger that includes a record of every BTC transaction that has ever occurred.

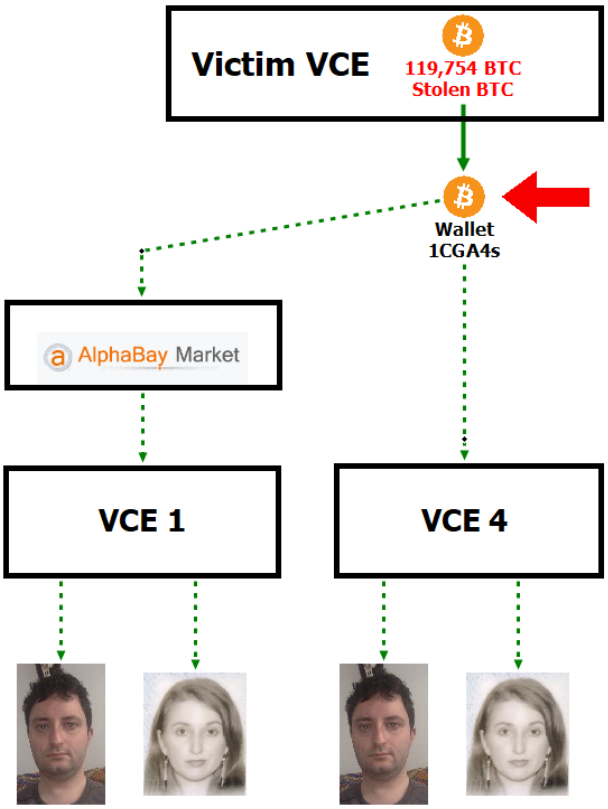
Despite these efforts, U.S. authorities traced the stolen BTC to multiple accounts controlled by both of the defendants.

The 2017 transfers notwithstanding, the majority of the stolen funds remained in Wallet 1CGA4s from August 2016 until January 31, 2022. On January 31, 2022, law enforcement gained access to Wallet 1CGA4s by decrypting a file saved to Lichtenstein's cloud storage account,[6] which had been obtained pursuant to a search warrant. The file contained a list of 2,000 virtual currency addresses, along with corresponding private keys.[7] Blockchain analysis confirmed that almost all[8] of those addresses were directly linked to the hack. Between January 31, 2022, and February 1, 2022, law enforcement used the private keys from LICHTENSTEIN's file to seize Wallet 1CGA4's remaining balance of approximately 94,636 BTC, worth $3.629 billion at the time of the seizure.

6 A cloud storage account allows users to store computer files in a remote location, rather than saved to their own devices.

7 Each virtual currency address has a corresponding private key, which is roughly equivalent to a complex password or PIN code and which is needed to spend any virtual currency contained in the address.

8 More specifically, all of the 2,000 addresses either contained BTC directly linked to the hack of Victim VCE (*i.e.*, was exclusively funded from the hack) or did not contain any virtual currency at all (*i.e.*, they contained a balance of zero and had never been used to transact in virtual currency).

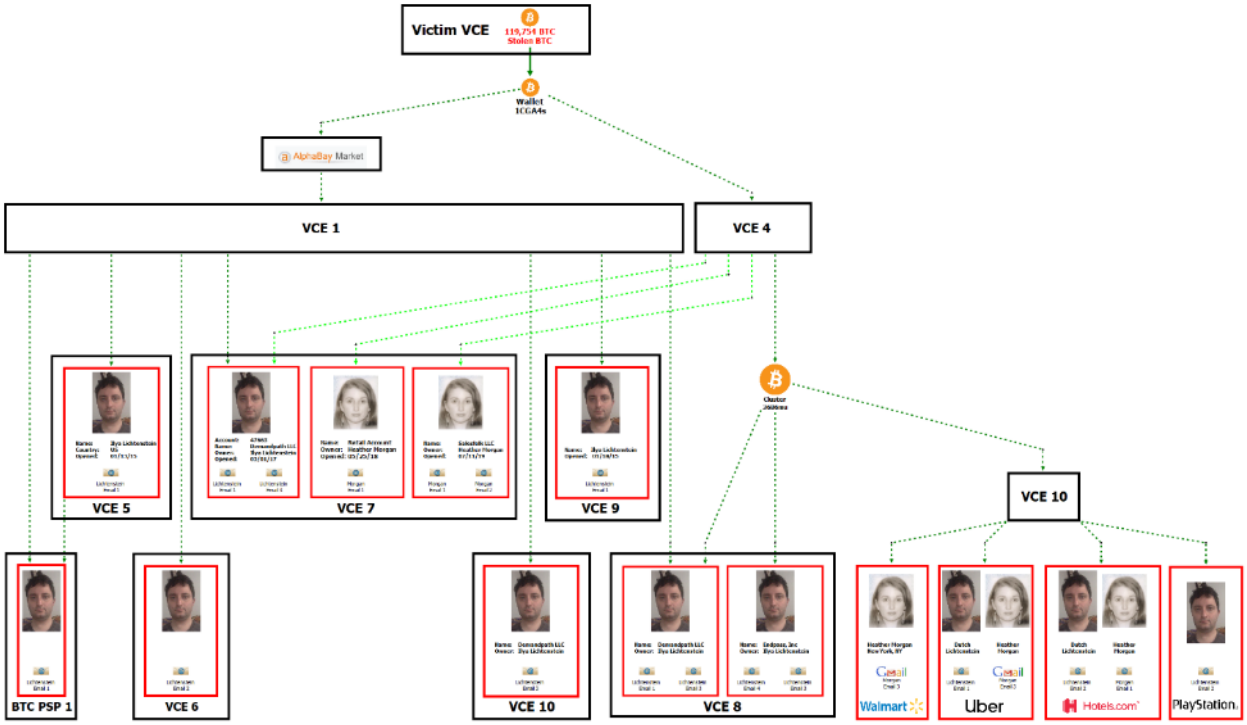


2. Tracing the Stolen Funds to Lichtenstein and Morgan

As detailed in the complaint, the defendants went to great lengths to launder their funds. Law enforcement traced the stolen funds through thousands of transactions to over a dozen accounts in the true name of Lichtenstein, Morgan, and/or their businesses – Endpass, Demandpath, and SalesFolk. Law enforcement was also able to determine that numerous accounts set up with fictitious personas and involved in the laundering were, in fact, controlled by Lichtenstein and Morgan.

The chart below is a simplified[9] illustration of how the stolen BTC moved in a series of transactions from Victim VCE to accounts connected to Lichtenstein and Morgan:

9 Because the stolen BTC was transferred and split up so many times, condensing all the transaction information into one chart would be impractical. The charts within the government's filings do not depict all known transactions, or



Lichtenstein and Morgan employed numerous money laundering techniques, including: (1) using accounts set up with fictitious identities; (2) moving the stolen funds in a series of small amounts, totaling thousands of transactions, as opposed to moving the funds all at once or in larger chunks; (3) utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; (4) layering the stolen funds by depositing them into accounts at a variety of VCEs and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; (5) converting the BTC to other forms of virtual currency, including anonymity-enhanced virtual

even all transactions related to the activity depicted. Rather, they are meant to be illustrations of the general flow of the stolen BTC from one point to another.

currency,[10] in a practice known as "chain hopping"; and (6) using U.S.-based business accounts to legitimize activity.

Nonetheless, law enforcement was able to trace the stolen funds to numerous accounts controlled by Lichtenstein. Detailed examples of that tracing are included in the complaint and are not restated here at length. In brief, law enforcement traced the stolen funds:

a. **First**, to Wallet 1CGa4s, an unhosted wallet[11] containing over 2,000 BTC addresses (which were saved, along with their associated private keys, in LICHTENSTEIN's cloud storage account), where the stolen funds remained dormant until January 2017;
b. **Second**, to accounts at the darknet market AlphaBay;[12]
c. **Third**, to seven interconnected accounts at a U.S.-based VCE ("VCE 1"), as well as accounts at additional VCEs ("VCE 2," "VCE 3," and "VCE 4");
d. **Fourth**, to various unhosted BTC wallets; and
e. **Fifth**, to accounts owned by Lichtenstein and Morgan at six other VCEs ("VCE 5," "VCE 6," "VCE 7," "VCE 8," "VCE 9," and "VCE 10").

Many of the accounts used in the laundering were set up using fictitious personas that did not initially appear to be connected to Lichtenstein or Morgan. However, law enforcement located a spreadsheet within an account controlled by Lichtenstein that included detailed information for many of the accounts, including the access information and an indication where the accounts had been "FROZEN." (On several instances, virtual currency exchanges had flagged the activity as suspicious and, after failing to receive sufficient assurances from the

10 Anonymity-enhanced virtual currency, also called anonymity-enhanced cryptocurrency (AECs) or privacy coins, are virtual currency alternatives to BTC which endeavor to provide greater anonymity when making transactions.

11 BTC wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are called "unhosted" wallets.

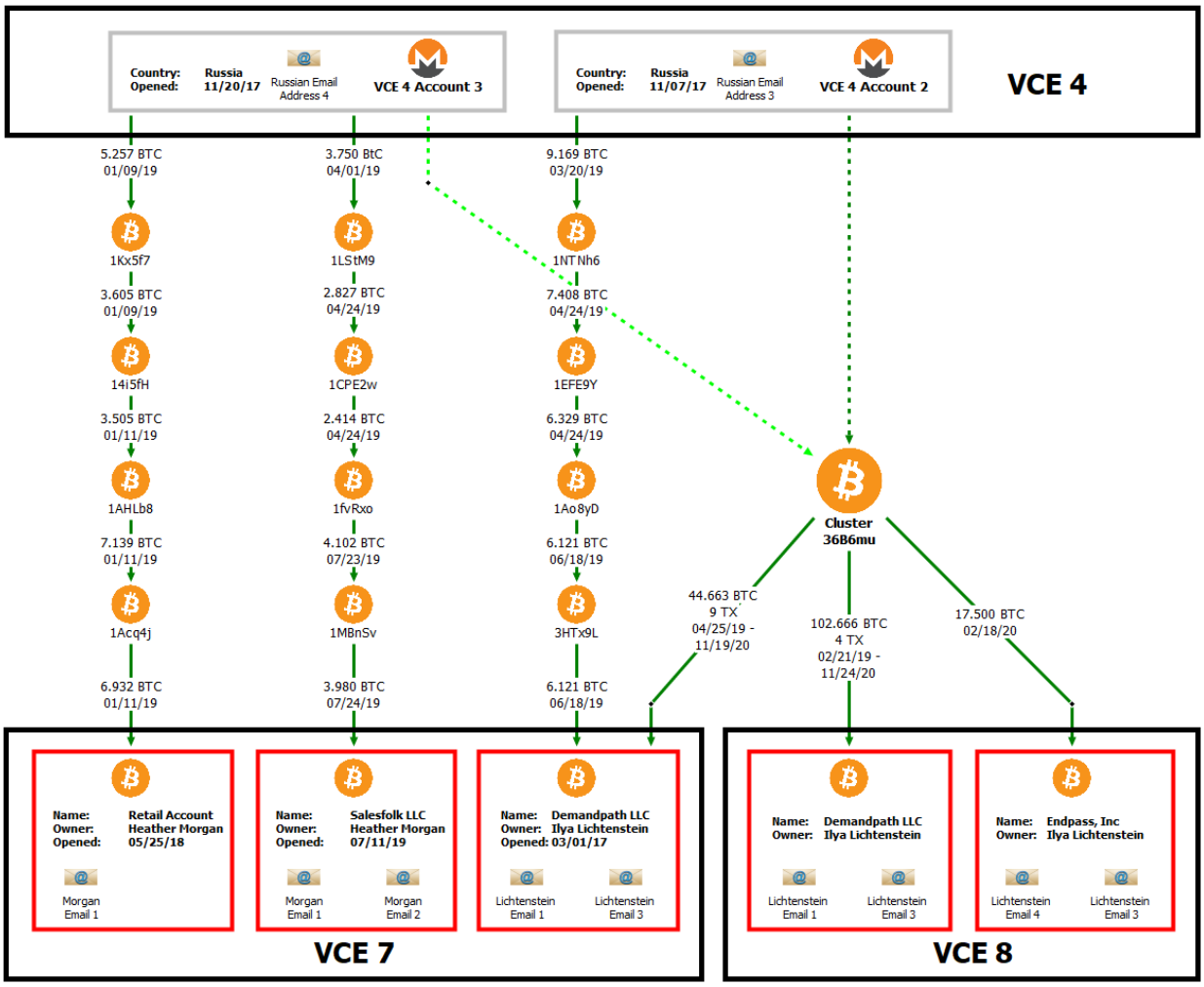
12 A darknet market is an ecommerce platform through which vendors can sell illegal goods and services, such as illegal narcotics, stolen financial information, and hacking tools. Darknet markets typically allow users to create accounts and deposit, store, and withdraw virtual currency from those accounts, in order to buy and sell items on the site. AlphaBay was one of the largest darknet markets and operated from December 2014 through July 2017.

fictitious account-holder, froze the accounts. In total, Lichtenstein and Morgan abandoned hundreds of thousands of dollars flagged at exchanges in this manner.)

3. Lichtenstein and Morgan's Deceptive Statements

Lichtenstein and Morgan repeatedly fabricated stories regarding their source of funds and the nature of their cryptocurrency activities. For example, the government traced funds from accounts holding monero[13] at VCE 4, and then to accounts held by Morgan, Lichtenstein, and their businesses. From there, Morgan and Lichtenstein converted the funds to U.S. dollars and transferred the funds to traditional banks. Shortly thereafter, the accounts at VCE 4 were flagged as suspicious and frozen by VCE 4.

13 Monero is a virtual currency designed to increase transaction anonymity by obscuring activity on the blockchain.



When asked by VCE 7 about the nature of their account activity, Morgan and Lichtenstein provided false explanations. In or around June 2019, Morgan applied for an institutional, or business, account with VCE 7 on behalf of her business, SalesFolk; Morgan had previously sought a limit increase for her personal account with VCE 7 to allow her to transact in higher volume. Morgan indicated to VCE 7 that the account would be funded with SalesFolk customers that pay in crypto and her own cryptocurrency. In a follow-up conversation with VCE 7, Morgan indicated that the funds were gifted to her by her boyfriend (now husband) in 2014/2015 and that

she had been keeping them in cold storage. In fact, as is evident from the blockchain and shown in the chart above, the funds were transferred from a shell account at VCE 4.

Morgan used other SalesFolk business accounts, in addition to her personal accounts, to launder the hack proceeds. Another SalesFolk account received approximately $130,000 worth of virtual currency from a single company ("Shell Company 1"), which claimed to operate out of Hong Kong. From May 2017 to June 2018, Shell Company 1 made 17 payments to the SalesFolk account. The payment was purportedly for advertising services. However, Shell Company 1 had no website, and investigators were unable to identify any legitimate business activity by Shell Company 1, much less any advertising. Shell Company 1's domain – used for email purposes – was registered with the same registrar as Morgan's and Lichtenstein's businesses. Payment for the domain originated from a peel chain that, four hops later, sent BTC to an account held by Lichtenstein in his true name at VCE 5.

Morgan extended this deception into her communications with the accountant who prepared federal personal and business income tax returns for Morgan and Lichtenstein. A repeated topic of conversation was the sale of BTC by Lichtenstein and Morgan and the cost basis from when the BTC was acquired. Generally speaking, when BTC is sold for more than for what it was acquired (cost basis), the capital gain must be reported on an income tax return, much like a publicly traded stock or other property. The full sales proceeds of the BTC is not taxed, only the gain. If the BTC was sold for less than for what it was acquired, a non-taxable capital loss would be reported, which could offset other capital gains. Therefore, it is more tax advantageous to have a higher cost basis in order to avoid paying more tax.

Over the course of several emails in fall 2020, the accountant pressed Morgan and Lichtenstein for details of their basis. Morgan suggested that, "Worst-case, I guess we could always make the basis zero." The accountant responded that he would "rather provide a conservative estimate than use zero basis." Ultimately, Lichtenstein and Morgan indicated, without providing receipts or transaction records, that they acquired 120 BTC on May 7, 2011 at a cost of $3.64 per BTC for a total cost of $436.92. Lichtenstein advised the accountant, "We will likely end up owing some tax due to the low basis, but it shouldn't be too much."

4. Incriminating Files in Lichtenstein's Cloud Storage Account

As detailed in the complaint, Lichtenstein held an account at a U.S.-based provider that offered email as well as cloud storage services, among other products. In 2021, agents obtained a copy of the contents of the cloud storage account pursuant to a search warrant. Upon reviewing the contents of the account, agents confirmed that the account was used by Lichtenstein. However, a subset of files were secured with a strong encryption algorithm and a lengthy password; a password of that length would typically prevent even a well-resourced attacker from accessing the file within his lifetime.

On or about January 31, 2022, law enforcement was able to decrypt several key files contained within the account. Most notably, the account contained a file listing all of the addresses within Wallet 1CGA4s and their corresponding private keys. Using this information, law enforcement seized the remaining contents of the wallet, totaling approximately 94,636 BTC, presently worth $3.629 billion, as described above.

Lichtenstein's cloud storage account also contained an account spreadsheet, depicted below, detailing the log-in information and status of accounts at numerous VCEs, including a

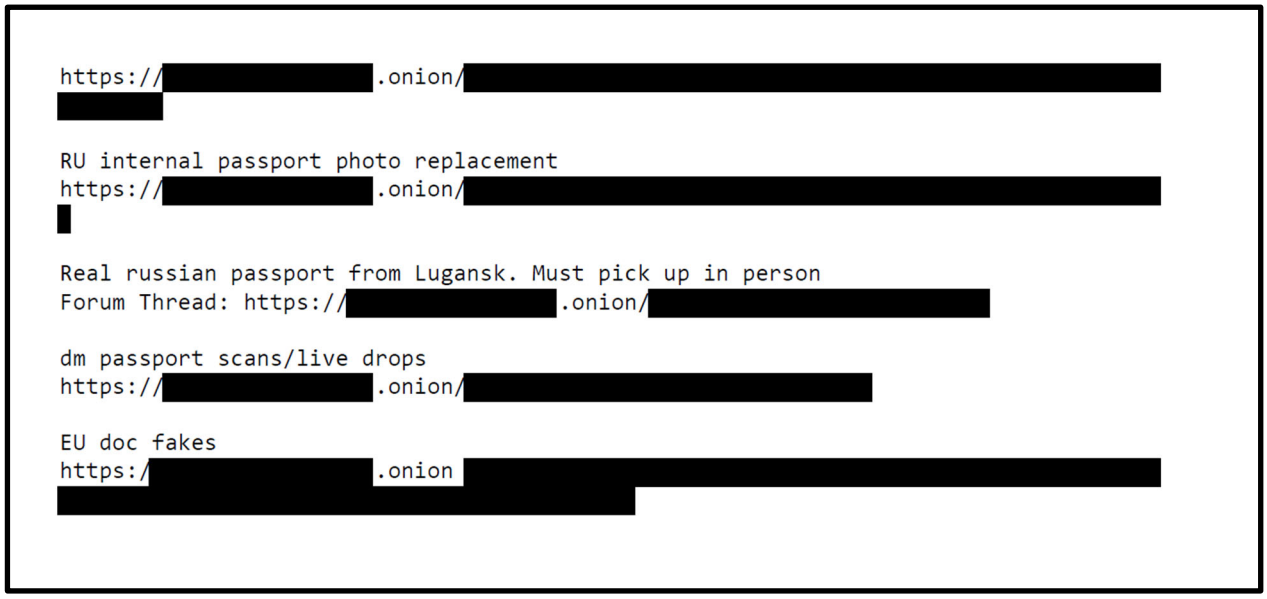
notation of which accounts had been frozen or emptied. As explained in the complaint and above, many of these accounts were opened with fictitious identities and received stolen funds from Victim VCE.

	A	B	C	D	E
1	/	created_at	exchange	status	login
2	1		[redacted]	DEAD	[redacted]
3	2				
4	4			FROZEN- 6/3/17 link alternate accounts	
5	5			FROZEN- 6/3/17 link alternate accounts	
6	6			FROZEN- 6/3/17 link alternate accounts	
7	7			FROZEN- 6/3/17 link alternate accounts	
8	8			FROZEN- 6/3/17 link alternate accounts	
9	9				
10	10				
11	11				
12	12				
13	13			Has tokens	
14	14			Has tokens and BTC	
15	15	04/20/2017		EMPTY	
16	16	04/21/2017		Has tokens	
17	17	04/23/2017		EMPTY	
18	18	04/23/2017		EMPTY	
19	19	05/24/2017		EMPTY	
20	20	05/24/2017		Basic Verified, EMPTY	
21	21	06/12/2017		EMPTY	
22	22	06/29/2017		Basic Verified, EMPTY	
23	23	06/29/2017			
24	23	07/01/2017			
25	24	07/24/2017		LOCKED, 13BTC	
26	25	01/01/2018		PIN: [redacted]	
27	26	12/07/2017		LOCKED, 18BTC	
28	27	04/04/2018		API TEST. PIN: [redacted]	
29	28	04/21/2018		must whitelist ip for api withdrawals	
30	29	04/25/2018			
31	30	08/08/2018			
32	31	08/08/2018			
33	32	08/08/2018		XMR withdrawals disabled!!	

The encrypted area within the cloud storage account also held apparent wallet files for additional cryptocurrency that the government has not yet been able to seize. Several of these files include variations of the word "dirty" in their names, such as "dirty_wallet.dat."

The account also contained a folder holding data files for numerous financial institutions, many in Russia, with notes that appear to be reconnaissance of potential laundering avenues. The

account additionally included a text file named "passport_ideas" that included links to different darknet vendor accounts that appeared to be offering passports or identification cards for sale, depicted in the redacted screenshot below.



A folder titled "4-yandex-money" – referring to the Russian platform Yandex – contained approximately 7 sub-folders, each with a text file listing what appear to be Yandex transactions; a foreign cell phone number; an email address ending in .ru, indicating a Russian account; and what appears to be a password. Each sub-folder also contained Russian persona information in the form of a passport and/or a "selfie"-style photo – a common know-your-customer identification method for financial institutions and especially virtual currency exchanges.

The files in Lichtenstein's cloud storage account also included multiple references to Ukraine in relation to apparent money laundering activity. For example, a document regarding "Offshore Company Registration" includes a list of Ukrainian companies that will assist with offshore company registrations. A document titled "btc_rub_exchange" sets out a comparison of

options for exchanging BTC to "RUB," or Russian rubles, with a note that one, "Might need a lot of KYC[14]…"

5. Suspicious Ukraine Activity

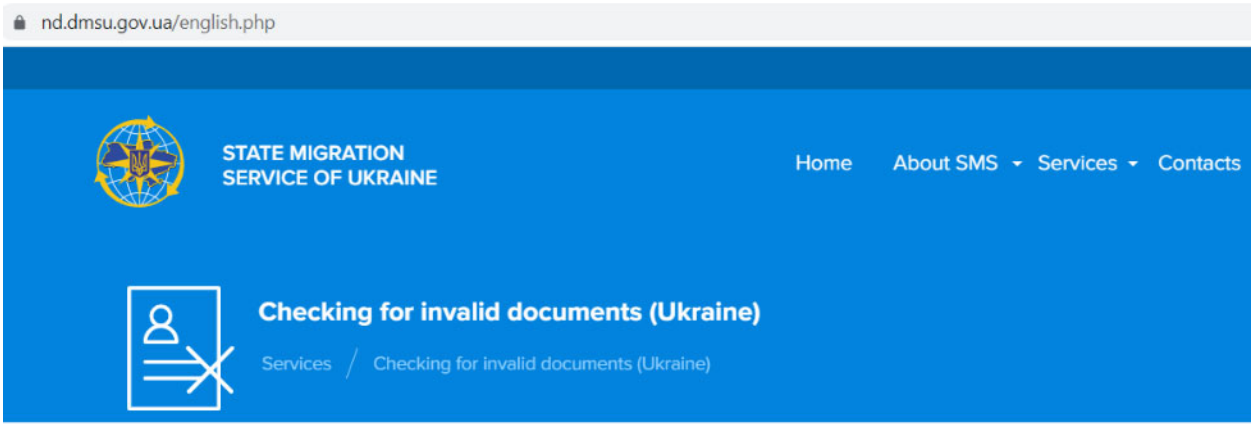
In August 2019, Morgan and Lichtenstein traveled together to Ukraine for a one-month trip, returning in September 2019. During that time, Lichtenstein created and/or modified numerous files in his cloud storage account that contained notes about money laundering and/or false identification documentation with Ukrainian connections.

As noted in the complaint, Lichtenstein's cloud storage account contained a folder named "personas." The "personas" folder was organized into subfolders named "RU," indicating Russia, and "UA," indicating Ukraine. Each folder contained biographical information and identification documents for numerous individuals, both male and female.

A document titled "vendors" (Exhibit 1) lists descriptions of multiple darknet vendors and includes notes regarding delivery options to Ukraine. One vendor is marked as "can exchange for cash in UA Kiev." Following another vendor, the document comments, "Ask about delivery to Ukraine, how it works." Yet another vendor (Vendor 1) is listed as selling "Ukraine internal passport fakes/photo paste," with a note, "internal delivery in Ukraine via Novaya Pochta," referencing a Ukrainian postal service. The reference to "passport fakes/photo paste" indicates that the vendor is selling fake passports that can be customized with photographs provided by the purchaser. Vendor 1's listing also noted that the passport status could be verified via https://nd.dmsu.gov.ua/. According to an English translation of the website, the site is a website

14 "KYC" refers to "know-your-customer," information, which is information about customers and their activities that financial institutions collect as part of their anti-money laundering procedures.

for the State Migration Service of Ukraine. The site, depicted below, allows a user to check the validity of passports.



A file titled "courier" (Exhibit 2) contained a list of what appeared to be various tracking numbers for packages from darknet vendors, including vendors from the previously described "vendors" document. One vendor (Vendor 2) – who appeared in the "vendor" document with the note, "Bank debit cards on drops, can guarantee 12 months. Also can make cards for our scans" – appears in the "courier" document with a notation "good opsec[15]!" Below Vendor 2's username is the acronym "EMS," a reference to Ukraine's mail service, a tracking number, and a notation "from: Vladivostok." The tracking number was confirmed to be a valid EMS tracking number, showing a shipment from Vladivostok, Russia to Kiev, Ukraine, arriving on September 9, 2019, during the time that Morgan and Lichtenstein were in Kiev. The "personas" folder in Lichtenstein's cloud storage account also contained two text files (including Exhibit 3) with detailed identification information for Russian personas that include the reference "Vendor:

15 "Opsec" is a term commonly used to mean "operational security." Among darknet actors, opsec is often used to describe a vendor's efforts to avoid detection by law enforcement.

[Vendor 2]." The files were each created on September 10, 2019, the day after the package from Vendor 2 was delivered in Kiev.

Additional EMS tracking numbers contained within the "courier" document were confirmed to be valid tracking numbers, showing shipments arriving in Ukraine during the time that Lichtenstein and Morgan were visiting.

The "notes" folder also includes a file titled "info" that lists "delivery info" as "11 Mirrors Design Hotel," a hotel in Kiev. Morgan posted photos to social media during her trip, indicating that she was staying at a Hilton hotel near the 11 Mirrors Design Hotel. According to an Uber receipt, Morgan took an Uber from the 11 Mirrors Design Hotel at 07:09 a.m. on September 11, 2019.

Another document titled "ukraine_package," written in Russian, explains "how to anonymously receive a parcel in Ukraine" (according to a machine translation) and includes details of common camera positioning in Ukrainian post offices and how to avoid being captured on a security camera when receiving packages in Ukraine.

A file titled "sim_cards" contained credentials for multiple email accounts; what appears to be a Novaya Potcha account, and a phone number – all of the requirements for receiving anonymous packages laid out in the "ukraine_package" file referenced above.

On August 23, 2019, funds from BTC Cluster 36B6mu[16] were used to purchase a gift card for Kyivstar, a Ukrainian telecommunications company. The gift card purchase was conducted from a Ukrainian IP address. The contents of Morgan's iCloud account, obtained by search

16 Cluster 36B6mu, described in the complaint, was frequently used as an intermediary between VCEs withdrawing BTC and VCE accounts held by LICHTENSTEIN and MORGAN in their true names.

warrant, include a photo of what appears to be Morgan's hand holding a Kyivstar SIM card. A Ukrainian phone number is listed on the SIM card.

Another file titled "phone_imei" contained information related to changing a device's IMEI. IMEIs are numbers that uniquely identify a mobile device, such as a cell phone or a GPS tracker. IMEIs are intended to be static, unlike a SIM card which may be swapped, and are often used to track an individual's location or activities.

6. Search of Defendants' Apartment

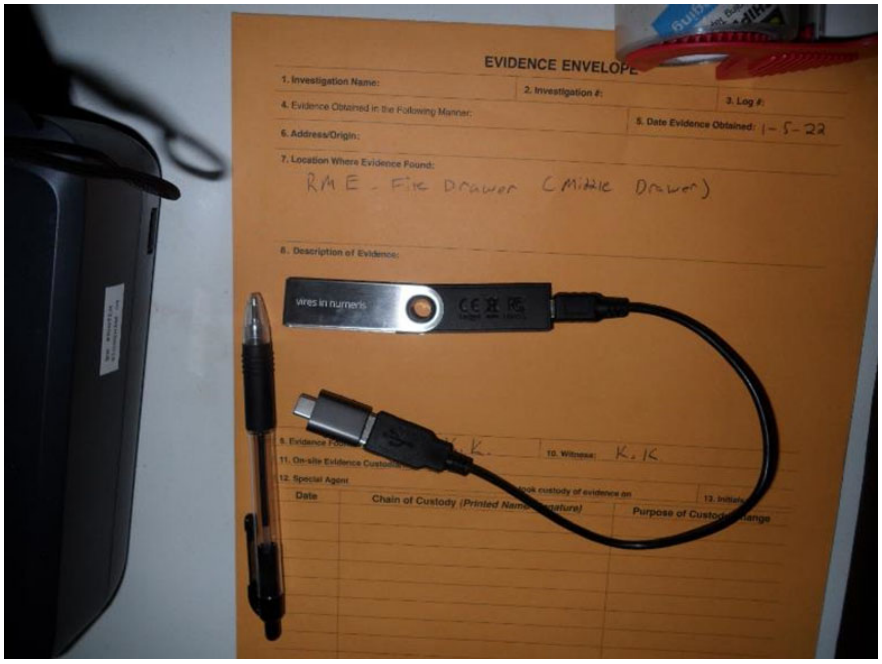
On January 5, 2022 – prior to law enforcement's decryption of Lichtenstein's cloud storage account – agents executed a search of Morgan and Lichtenstein's apartment in New York.

After agents secured the scene, Morgan and Lichtenstein advised that they did not want to remain on the premises during the search and decided to take their cat with them. Agents permitted Morgan to retrieve the defendants' cat, which was hiding under the bed. While Morgan was crouched next to the bed calling to the cat, she positioned herself next to the nightstand, which was still holding one of her phones. She then reached up and grabbed her cell phone from the nightstand and repeatedly hit the lock button. It appeared that Morgan was attempting to lock the phone in a way that would make it more difficult for law enforcement to search the phone's contents. Law enforcement had to wrest the phone from her hands.

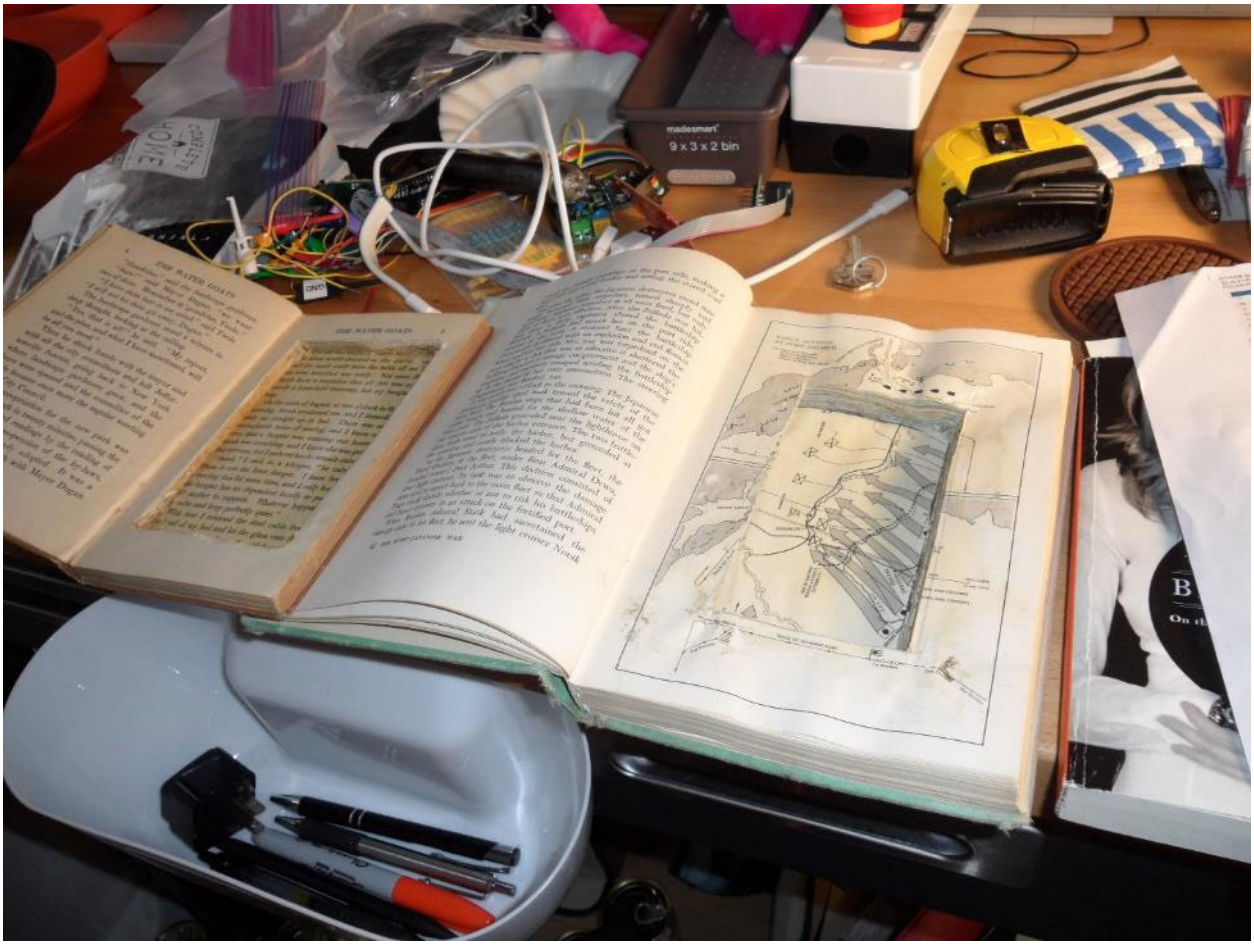
Under the same bed, agents located a bin containing various bags holding multiple cell phones, SIM cards, and assorted electronics. One of the bags was labeled "Burner Phone."

Law enforcement seized over 50 electronic devices during the search of Lichtenstein and Morgan's apartment. Many of those devices were partially or fully encrypted or otherwise password-protected.

Law enforcement also seized multiple hardware wallets, which are secure, portable virtual currency storage devices, depicted below along with a financial account access token.



Lichtenstein's office contained two hollowed-out books, whose pages appeared to be roughly cut out by hand, shown below. The compartments were empty.



Law enforcement also seized more than $40,000 in cash and what appears to be a substantial amount of foreign currency.

As noted in the complaint, Lichtenstein had previously used virtual currency traced to the hack to purchase gold from a precious metals dealer. ECF No. 1-1 at 7. Over the course of several transactions at different vendors, Lichtenstein and Morgan amassed over 70 one-ounce gold coins. Law enforcement did not locate a single gold coin during the search of Lichtenstein and Morgan's residence or their storage unit.

7. Subsequent Procedural History

The defendants were presented on February 8, 2022, for their Initial Appearance in the Southern District of New York, before Magistrate Judge Debra Freeman. Detention arguments were heard. Among other things, the defense represented that Morgan had undergone a serious medical procedure on January 31, 2022, and that she was scheduled to have "oral surgery" the next day, February 9, 2022. At the conclusion of the hearing, Magistrate Judge Freeman ordered both defendants released on bond—specifically, a $5 million bond for Lichtenstein, and a $3 million bond for Morgan—and subject to other conditions of release, including home incarceration, GPS monitoring, and restrictions on the use of Internet-connected devices.

Counsel for the government requested a courtesy 24-hour stay of Magistrate Judge Freeman's release decision to facilitate an appeal pursuant to 18 U.S.C. § 3145. Magistrate Judge Freeman declined to grant a stay, stating that it would take some time for the defendants to post bond, so a stay would be unnecessary. The government immediately filed a Motion for an Emergency Stay and a Review of Detention Order in the District Court for the District of Columbia, ECF No. 9, based on the defendants' significant risk of flight. This court promptly issued an order staying the defendants' release, ECF No. 10. On February 10, 2022, the defendants filed a letter brief in support of their clients' release, ECF No. 15. A detention hearing

is set for February 11, 2022.

APPLICABLE LAW

Under the Bail Reform Act, the Court "shall order" that the defendant be detained pending trial if it determines after a hearing that no condition or combination of conditions "will reasonably assure the appearance of the person as required and the safety of any other person and the community." 18 U.S.C. § 3142(e). A finding of either risk of flight or danger is sufficient for detention. *See, e.g.*, *United States v. Ferranti*, 66 F.3d 540, 543-44 (2d Cir. 1995). The government must prove the defendant presents a risk of flight only by a preponderance of the evidence, not by clear or convincing evidence or other, more demanding standards. *United States v. Vortis*, 785 F.2d 327, 328-29 (D.C. Cir. 1986); *United States v. Xulam*, 84 F.3d 441, 442 (D.C. Cir. 1996). At a detention hearing, the government may present evidence by way of proffer, *United States v. Smith*, 79 F.3d 1208, 1209-10 (D.C. Cir. 1996), and "[t]he rules concerning admissibility of evidence in criminal trials do not apply" at a detention hearing, 18 U.S.C. § 3142(f).

In reviewing the Magistrate Judge's detention order, this Court conducts a *de novo* review of the record to determine whether the defendant should be detained pending trial. *United States v. Smith*, 160 F. Supp. 3d 280, 282 (D.D.C. 2016). "The Court is free to use in its analysis any evidence or reasons relied on by the magistrate judge, but it may also hear additional evidence and rely on its own reasons." *Id.* (quoting *United States v. Hubbard*, 962 F. Supp. 2d 212, 215 (D.D.C. 2013)).

In assessing the risk of flight presented by the defendant, the Court must assess the statutory factors specified in 18 U.S.C. § 3142(g), including (1) the nature and circumstances of the offense

charged; (2) the weight of the evidence against the defendant; and (3) the history and characteristics of the defendant. 18 U.S.C. § 3142(g)(1)-(3).[17]

ARGUMENT

1. The Nature and Circumstances of the Offense

a. The Vast Scale and Sophistication of the Defendants' Money Laundering

The defendants are charged with conspiring to launder bitcoin that is now worth billions of dollars. In furtherance of that conspiracy, the defendants sent thousands of transactions, transferring cryptocurrency through over a dozen virtual currency exchanges across the globe as well as darknet markets and other platforms. The defendants' own Letter Brief describes this extensive laundering activity as "a complex web of convoluted blockchain and cryptocurrency tracing." Lichtenstein has a background in coding and claimed to be working on a

[17] The defendants suggest that the Court should also consider whether pretrial release would be helpful in the preparation of their defense, but that is not one of the statutory factors listed under § 3142(g). The question before the Court is solely whether the defendants pose a serious risk of flight such that no condition or combination of conditions will reasonably assure their appearance at trial. To the extent the defendants wish to argue that pretrial release is necessary for the preparation of their defense, they must move pursuant to 18 U.S.C. § 3142(i), and the *defendant*, not the government, bears the burden of showing that pretrial release is "necessary" for such purposes. *See United States v. Otunyo*, No. 18-cr-251, 2020 WL 2065041 (BAH), at *3 (D.D.C. Apr. 28, 2020) ("Section 3142(i) provides a distinct mechanism for temporarily releasing a detained defendant, in a manner that has nothing to do with a revisiting of the initial detention determination, but a defendant has the burden of showing that temporary release is 'necessary.'") (internal citations and alterations omitted); *see generally United States v. Bikundi*, 47 F. Supp. 3d 131, 136 (D.D.C. 2014) ("[D]efense counsel pointed out at a May 29, 2014 status hearing that the defendant's ability to assist in review of the [discovery] material is adversely affected by her incarceration pending trial. . . . The remedy for that concern, however, is not pretrial release when the statutory conditions are not met, but unrelenting efforts by the government to process discovery and get ready for trial as promptly as possible."). The government would not oppose the defendants remaining incarcerated in New York to the extent that it would afford counsel easier access to the defendants.

Similarly, the defendants raise concerns regarding Morgan's access to medical care while incarcerated. That, too, is better suited for a different vehicle. *See, e.g.*, *United States v. Folse*, Nos. CR 15-2485 JB, CR 15-3883 JB, 2016 WL 3996386, at *15 (D.N.M. June 15, 2016) ("The general rule is that a defendant must file a separate civil action to address his conditions of confinement."); *United States v. Luong*, No. Cr. 99-433 WBS GGH, 2009 WL 2852111, at *1 (E.D. Cal. Sept. 2, 2009) ("As several courts have recognized, the proper procedure to redress a defendant's grievances regarding treatment within a jail or prison is to file a civil suit against the relevant parties . . . rather than a motion in his criminal case.").

cryptocurrency wallet that he described as "the first decentralized cloud wallet [for certain virtual assets]." His online bio touted, "He's been reverse engineering hardware and writing code since age 9." Morgan was also well-educated and had significant crypto-savvy, holding numerous cryptocurrency accounts and going so far as to mint her own non-fungible tokens (NFTs)[18] tied to her rap album covers.

b. Deceptive and Deceitful Nature of Activity

The defendants are charged with conspiring to defraud the United States, a violation involving deceit and deception. The complaint details the extensive deceptive acts and statements by both Lichtenstein and Morgan, and additional examples are included within this reply. Lichtenstein and Morgan both repeatedly misled financial institutions about the nature of their activity. The couple's activities in Ukraine at times appear pulled from the pages of a spy novel. In materials promoting herself and her companies, Morgan repeatedly boasts of her ability to "social engineer" her way into and out of different scenarios. Morgan also appeared to be attempting to interfere with law enforcement's search of the defendants' residence by grabbing for and attempting to lock her phone under the pretense of retrieving her cat.

Notably, one of the principal targets of the defendants' deception was an agency of the U.S. Government – specifically, the Financial Crimes Enforcement Network (FinCEN), tasked with, *inter alia*, safeguarding the U.S. financial from abuse by money launderers. As set forth in the complaint, the defendants were clearly very familiar with anti-money laundering (AML) and

[18] Non-fungible tokens (NFTs) are blockchain-based digital units used to transfer or validate ownership of unique items, such as artwork. The government does not intend to suggest that all, or even most, NFT owners are well-versed in cryptocurrency, but Morgan's NFT activity is framed within a broader involvement in cryptocurrency, including her conspiracy to launder BTC currently valued at over $5 billion.

know-your-customer (KYC) requirements, and went to great lengths to thwart their enforcement. Such disregard for the core mission of a U.S. government agency does not suggest that the defendants would abide by an order of this court or instructions from Pretrial Services regarding conditions of release.

c. Substantial Criminal and Financial Penalties Provide Incentive To Flee

If convicted, the defendants face significant criminal and financial penalties. In Count One, the defendants are charged with laundering bitcoin that was the proceeds of the hack of a virtual currency exchange, a felony punishable by up to 20 years of imprisonment and a $250,000 fine. *See* 18 U.S.C. §§ 1956(h), 3571(b)(3). The defendants are also charged with conspiring to defraud the United States, *see* 18 U.S.C. § 371. Although this offense carries a maximum term of 5 years of imprisonment, the scale of the defendants' illegal activity would likely push their recommended sentence under the U.S. Sentencing Commission Guidelines Manual (the "Guidelines" or U.S.S.G.) well past the 5-year statutory maximum. In fact, the defendants' Guidelines calculation for these offenses may be so high that, under the total punishment provision of U.S.S.G. § 5G1.2(d), the defendants' sentences for Counts One and Two may be stacked to run consecutively under the Guidelines for as long as 25 years.[19]

[19] Under U.S.S.G. § 5G1.2(d), if the combined Guidelines range exceeds the statutory maximum of the Count carrying the highest authorized term of imprisonment, "then the sentence imposed on one or more other counts shall run consecutively, but only to the extent necessary to produce a combined sentence equal to the total punishment." Here, that would mean consecutive sentences for Count One (20 years) and Count Two (5 years). While this Court may well depart from the advisory Guidelines range provided by § 5G1.2(d), or find that one or more specific offense characteristics do not apply, the possibility of an advisory recommendation at the highest end of the Sentencing Table, up to and including "life" in prison—even if limited by statute to 25 years—provides a strong incentive to flee rather than face prosecution.
.

In addition, a conviction under § 1956(h) carries other significant financial penalties, including a fine of up to "twice the value of the property involved in the transaction[s]," 18 U.S.C. § 1956(a)(1) & (h), and forfeiture of not just the proceeds of the offense but "any property . . . *involved in* such offense," 18 U.S.C. § 982(a)(1) (emphasis added)—resulting in fines and a forfeiture money judgment of potentially *billions* of dollars and forfeiture of any cryptocurrency or other assets that the defendants accumulated through their laundering scheme, or purchased with their illegal proceeds. These significant personal and financial penalties provide the defendants with an overwhelming incentive to flee prosecution.

In sum, the nature and sophistication of the defendants' scheme and the significant criminal and financial penalties they face all weigh heavily in favor of detention.

2. The Weight of the Evidence Against the Defendants

The government's case against the defendants is strong. To be sure, the defendants went to elaborate lengths to conceal their identities, but once these strands are untangled, the defendants' activities are clear. Most notably, the government seized stolen cryptocurrency valued at the time at $3.6 billion ***from Lichtenstein's own account*** – a point that the defendants' Letter Brief conveniently glosses over while complaining that the government lacks "direct evidence" connecting the defendants to the specified unlawful activity at issue. Furthermore, blockchain analysis, combined with financial records for the defendants, shows that numerous accounts held in the defendants' true names have received deposits derived from the Victim VCE Hack, many laundered through different paths but all tracing back to the stolen funds.

The defendants' Letter Brief also grossly mischaracterizes the government's evidence and its strength regarding Morgan. The defense Letter Brief attempts to paint Morgan as a passive,

unknowing recipient of any "supposedly tainted" hack proceeds. However, Morgan's active involvement in the laundering scheme belies such a defense. Morgan was extremely hands-on and involved in managing the cryptocurrency held in her own accounts and in the accounts of her businesses. Her business accounts were used to clean and legitimize funds stolen from the Victim VCE. Morgan engaged in numerous and repeated conversations with multiple virtual currency exchanges that were seeking to verify her account activity as part of their anti-money laundering controls. Morgan's explanations of the source of funds are directly controverted by the evidence on the blockchain. Morgan traveled with Lichtenstein to Ukraine, and Uber records place her at the hotel where the darknet vendors were shipping the fictitious documents and/or cards, at the time of the shipments. Morgan engaged directly with the accountant responsible for filing taxes, and she personally suggested reporting her and Lichtenstein's bitcoin sales in a way that would have *increased* their tax obligation, against the advice of their accountant. She delivered talks on topics such as "How to Social Engineer Your Way into Anything" and wrote online articles on cybersecurity such as "Experts Share Tips to Protect Your Business From Cybercriminals," which included "interviewing" – and gaining access to – several virtual currency exchange employees who discussed their companies' anti-money-laundering and anti-fraud protocols. Morgan was an amateur rap artist, and even her rap lyrics show her technical proclivities, including at one point rapping, "Spear phish your password/all your funds transferred," referring to the hacking technique of spear phishing to gain access to a user's account password, and then transferring all of the user's funds out of the account.

The strength of the government's evidence, the absence of any serious counterargument by the defendants – apart from bare assertions that Morgan was unaware of the illicit nature of the funds – and the paucity of viable legal defenses all weigh in favor of pretrial detention.

3. The Defendants' History and Characteristics

The defendants' access to hundreds of millions of dollars in cryptocurrency weigh heavily in favor of detention. Notwithstanding the government's recent seizure of 94,636 bitcoin from Lichtenstein's cloud storage account, the defendants have access to considerable assets. Most notably, the government believes the defendants have control over 24 BTC addresses that received money directly from the 1CGA4s cluster. These addresses hold a total of approximately 7,500 bitcoin, valued at over $300 million. Law enforcement has not yet located the private keys to these addresses, and they are believed to be located on an unhosted wallet. Cryptocurrency assets such as these can be accessed with an Internet connection from anywhere in the world, and they can be reconstituted without physical access to the electronic storage media on which the private keys are stored if the user has configured a seed recovery key.[20] With hundreds of millions of dollars in cryptocurrency assets at their disposal, accessible from anywhere in the world with an Internet connection, the defendants could easily finance a flight from prosecution. The government has seized substantial assets, but substantial assets remain outstanding. Based on its review of Lichtenstein and Morgan's accounts and devices to date, the government has located wallets containing multiple forms of virtual currency valued at several million dollars; the government has not yet been able to seize those funds. Furthermore, the review of Lichtenstein

[20] A seed key or seed phrase is a list of words used to encode a bitcoin wallet. Wallet software will typically generate a seed phrase and instruct the user to write it down on paper. The same software can be used to decode the seed phrase and reconstitute the wallet.

and Morgan's devices is ongoing, and it is likely that additional wallets are contained within encrypted partitions and other secured folders. Additionally, the government is aware of dozens of accounts that the defendants set up at financial institutions around the world using fictitious identities, and there are undoubtedly many more of which the government is still unaware.

As noted in the complaint, Lichtenstein used virtual currency traced to the hack to purchase gold from a precious metals dealer. ECF No. 1-1 at 7. Over the course of several transactions at different vendors, Lichtenstein and Morgan amassed over 70 one-ounce gold coins. Law enforcement did not locate a single gold coin during the search of Lichtenstein and Morgan's residence or their storage unit.

Lichtenstein was born in Russia and is a dual Russian-U.S. citizen. Counsel represented at the hearing in SDNY that Lichtenstein's family fled Russia due to persecution, which the government does not question. However, during the search of Lichtenstein and Morgan's apartment, agents located a Russian passport which Lichtenstein acquired in 2019 and which is valid through 2029. Russia does not extradite its own citizens. If Lichtenstein succeeded in fleeing to Russia, he could escape prosecution in the United States indefinitely. Morgan's marriage to Lichtenstein would allow her to qualify for Russian citizenship as well after meeting certain additional administrative requirements. The files from Lichtenstein's cloud storage account indicate that Lichtenstein has access to numerous accounts at Russian financial institutions and false Russian identity documents for both male and female personas. Morgan, who traveled extensively prior to the COVID-19 pandemic and previously lived in Hong Kong and Egypt, has

been studying Russian. When the couple was arrested, they had a brief conversation with each other in Russian.

The defendants have an established history of creating and using fictitious identities and concealing their activities online. At a minimum, this would make it virtually impossible for Pretrial Services to adequately track and monitor the defendants' online activities, should they be released pending trial. The defendants could easily obtain additional false identification documents and flee to evade prosecution. As this Court noted in *United States v. Eccleston*, 140 F. Supp. 3d 102 (D.D.C. 2015), pretrial supervision is ill-equipped to prevent a determined defendant from accessing an Internet-connected device in violation of his conditions of release. *See id.* at 107 ("[I]t is a case in which supervision can do little to alleviate the risk that the defendant might access a computer or other electronic device and continue to engage in the alleged criminal behavior."); *see also United States v. Sterlingov*, --- F. Supp. 3d ----, 2021 WL 5275702, at *8 (D.D.C. Nov. 10, 2021) ("[The defendant's] familiarity with darknet marketplaces, along with his history 'of creating numerous limited-use identities to obfuscate, conceal, and compartmentalize his activities online,' ... suggest that pre-trial services would be unable effectively to enforce any internet restrictions the Court might place on [the defendant] were he released pending trial."). The defendants' technical sophistication raises significant concerns regarding the efficacy of GPS monitoring, particularly in light of the document found on Lichtenstein's cloud storage account providing information about changing a device's IMEI, a hardware identifier number often used when tracking a device's location.

In sum, the defendants have not just a strong incentive to flee, but the means to do so, and they appear to have taken meaningful steps toward establishing new identities and financial

accounts in Ukraine and Russia to enable this flight. The defendants' access to hundreds of millions of dollars in cryptocurrency, ability to procure false identity documents on the darknet, and history of extensive deceitful behavior weigh heavily in favor of detention.

4. The Defendants' Proposed Conditions of Release Would Not Reasonably Assure Their Appearance

The defendants propose that they be released into home detention with location monitoring and bonds of $5 million for Lichtenstein and $3 million for Morgan. Even putting aside that cash bail is generally disfavored in the District of Columbia, these conditions are not likely to ensure the defendants' return to court to face the serious charges in this matter. The value of any bond – though significant by any normal measure – is dwarfed by the value of the funds available to the defendants if they chose to flee.

The offer by the defendants' parents to secure the defendants' bond with their own homes is generous, but the (unspecified) value of such property is presumably trivial in comparison to the hundreds of millions of dollars in cryptocurrency assets to which the defendants have access. As detailed in the complaint, the defendants have abandoned hundreds of thousands of dollars' worth of virtual currency at exchanges, after the exchanges flagged the funds as suspicious. If the defendants were willing to relinquish those funds when faced with mere follow-up questions from exchanges, they would certainly be willing to give up several million dollars in exchange for their freedom. The defendants have access to hundreds of millions of dollars' worth of cryptocurrency. They could easily buy their parents new homes after fleeing to Ukraine or Russia, or setting up a new life for themselves anywhere with their newly purchased identities.

That the defendants did not flee upon learning of the investigation is not an indication that they would not now flee, facing the government's strong evidence and lengthy sentencing

guidelines. According to the defendants, they received word from an Internet Service Provider (ISP) that the government had sought records pertaining to the defendants through a grand jury subpoena one year prior. ECF No. 15 at 2. Such a notification could have easily led the defendants to assume that the government's investigation had hit a dead end or gone in a different direction. Similarly, following the execution of the search of the defendants' residence, the government revealed only that it was investigating the hack of Victim VCE and that it had traced funds to several of the defendants' accounts. At that point, the defendants likely believed that the government lacked sufficient information to charge them, or that the government viewed their roles as minor and attenuated. As far as the defendants were concerned, the incriminating files were encrypted with a lengthy password and safely out of the government's reach.[21]

The government's seizure of $3.6 billion worth of cryptocurrency using Lichtenstein's private keys garnered significant attention at the time, with most members of the public assuming that the "hackers" were moving the funds. On February 1, the defendants would likely have realized that the government had gained access to highly incriminating files. At that point, however, Morgan was recovering from a recent medical procedure, and by February 4 a major snowstorm had caused widespread flight cancellations and made travel impracticable. Furthermore, on January 23, 2022, the State Department issued a travel advisory warning individuals not to travel to Ukraine due to the increased threats of Russian military action, as well as the ongoing threat of COVID-19. In short, the defendants had only a small window of time to

[21] Indeed, such an assumption as to the incriminating files would have been well-founded, as the government did not discover the $3.6 billion in stolen funds stored in Lichtenstein's cloud storage account until January 31, 2022, when it finally decrypted the relevant files. The discovery of this immense amount of stolen virtual currency, linked one step away from the original hack of the Victim VCE, and stored in the cloud in a format that would have been accessible to Lichtenstein and Morgan from anywhere in the world, substantially altered the risk-of-flight analysis.

flee – significantly complicated by geopolitical developments and the global pandemic – and their failure to act on it effectively is not indicative of their future risk of flight.

CONCLUSION

For the foregoing reasons, there is no condition or combination of conditions that can reasonably assure the defendants' appearance for proceedings in this case. The defendants' motion should be denied, and the defendants should continue to be detained without bail pending trial in this case.

Respectfully submitted,

MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar No. 481052

BY: */s/ Christopher B. Brown*
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
555 4th Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

/s/ C. Alden Pelker
C. Alden Pelker, Maryland Bar
Jessica Peck, N.Y. Bar Number 5188248
Trial Attorneys, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007 (Pelker)
(202) 353-9455 (Peck)
Catherine.Pelker@usdoj.gov
Jessica.Peck@usdoj.gov