UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
Ilya Lichtenstein
Defendant

Case No. 22-mj-22

ORDER OF DETENTION PENDING TRIAL

Part I - Eligibility for Detention

Upon the

- ❒ Motion of the Government attorney pursuant to 18 U.S.C. § 3142(f)(1), or
- ☑ Motion of the Government or Court's own motion pursuant to 18 U.S.C. § 3142(f)(2),

the Court held a detention hearing and found that detention is warranted. This order sets forth the Court's findings of fact and conclusions of law, as required by 18 U.S.C. § 3142(i), in addition to any other findings made at the hearing.

Part II - Findings of Fact and Law as to Presumptions under § 3142(e)

❒ **A. Rebuttable Presumption Arises Under 18 U.S.C. § 3142(e)(2)** *(previous violator)*: There is a rebuttable presumption that no condition or combination of conditions will reasonably assure the safety of any other person and the community because the following conditions have been met:

- ❒ **(1)** the defendant is charged with one of the following crimes described in 18 U.S.C. § 3142(f)(1):
  - ❒ **(a)** a crime of violence, a violation of 18 U.S.C. § 1591, or an offense listed in 18 U.S.C. § 2332b(g)(5)(B) for which a maximum term of imprisonment of 10 years or more is prescribed; **or**
  - ❒ **(b)** an offense for which the maximum sentence is life imprisonment or death; **or**
  - ❒ **(c)** an offense for which a maximum term of imprisonment of 10 years or more is prescribed in the Controlled Substances Act (21 U.S.C. §§ 801-904), the Controlled Substances Import and Export Act (21 U.S.C. §§ 951-971), or Chapter 705 of Title 46, U.S.C. (46 U.S.C. §§ 70501-70508); **or**
  - ❒ **(d)** any felony if such person has been convicted of two or more offenses described in subparagraphs (a) through (c) of this paragraph, or two or more State or local offenses that would have been offenses described in subparagraphs (a) through (c) of this paragraph if a circumstance giving rise to Federal jurisdiction had existed, or a combination of such offenses; **or**
  - ❒ **(e)** any felony that is not otherwise a crime of violence but involves:
    (i) a minor victim; **(ii)** the possession of a firearm or destructive device (as defined in 18 U.S.C. § 921); **(iii)** any other dangerous weapon; or **(iv)** a failure to register under 18 U.S.C. § 2250; ***and***
- ❒ **(2)** the defendant has previously been convicted of a Federal offense that is described in 18 U.S.C. § 3142(f)(1), or of a State or local offense that would have been such an offense if a circumstance giving rise to Federal jurisdiction had existed; ***and***
- ❒ **(3)** the offense described in paragraph (2) above for which the defendant has been convicted was committed while the defendant was on release pending trial for a Federal, State, or local offense; ***and***
- ❒ **(4)** a period of not more than five years has elapsed since the date of conviction, or the release of the defendant from imprisonment, for the offense described in paragraph (2) above, whichever is later.

❒ **B. Rebuttable Presumption Arises Under 18 U.S.C. § 3142(e)(3)** *(narcotics, firearm, other offenses)*: There is a rebuttable presumption that no condition or combination of conditions will reasonably assure the appearance of the defendant as required and the safety of the community because there is probable cause to believe that the defendant committed one or more of the following offenses:

- ❒ **(1)** an offense for which a maximum term of imprisonment of 10 years or more is prescribed in the Controlled Substances Act (21 U.S.C. §§ 801-904), the Controlled Substances Import and Export Act (21 U.S.C. §§ 951-971), or Chapter 705 of Title 46, U.S.C. (46 U.S.C. §§ 70501-70508);
- ❒ **(2)** an offense under 18 U.S.C. §§ 924(c), 956(a), or 2332b;
- ❒ **(3)** an offense listed in 18 U.S.C. § 2332b(g)(5)(B) for which a maximum term of imprisonment of 10 years or more is prescribed;
- ❒ **(4)** an offense under Chapter 77 of Title 18, U.S.C. (18 U.S.C. §§ 1581-1597) for which a maximum term of imprisonment of 20 years or more is prescribed; **or**
- ❒ **(5)** an offense involving a minor victim under 18 U.S.C. §§ 1201, 1591, 2241, 2242, 2244(a)(1), 2245, 2251, 2251A, 2252(a)(1), 2252(a)(2), 2252(a)(3), 2252A(a)(1), 2252A(a)(2), 2252A(a)(3), 2252A(a)(4), 2260, 2421, 2422, 2423, or 2425.

❒ **C. Conclusions Regarding Applicability of Any Presumption Established Above**

❒ The defendant has not introduced sufficient evidence to rebut the presumption above, and detention is ordered on that basis, with the evidence or argument presented by the defendant summarized in Part III.C.

❒ The defendant has presented evidence sufficient to rebut the presumption, but after considering the presumption and the other factors discussed below, detention is warranted for the reasons summarized in Part III.

OR

❒ The defendant has not presented sufficient evidence to rebut the presumption. Moreover, after considering the presumption and the other factors discussed below, detention is warranted for the reasons summarized in Part III.

Part III - Analysis and Statement of the Reasons for Detention

A. After considering the factors set forth in 18 U.S.C. § 3142(g) and the information presented at the detention hearing, the Court concludes that the defendant must be detained pending trial because the Government has proven:

❒ By clear and convincing evidence that no condition or combination of conditions of release will reasonably assure the safety of any other person and the community.

☑ By a preponderance of evidence that no condition or combination of conditions of release will reasonably assure the defendant's appearance as required.

B. In addition to any findings made on the record at the hearing, the reasons for detention include the following:

☑ Weight of evidence against the defendant is strong
☑ Subject to lengthy period of incarceration if convicted
❒ Prior criminal history
❒ Participation in criminal activity while on probation, parole, or supervision

- ❒ History of violence or use of weapons
- ❒ History of alcohol or substance abuse
- ❒ Lack of stable employment
- ❒ Lack of stable residence
- ❒ Lack of financially responsible sureties
- ❒ Lack of significant community or family ties to this district
- ☑ Significant family or other ties outside the United States
- ❒ Lack of legal status in the United States
- ❒ Subject to removal or deportation after serving any period of incarceration
- ❒ Prior failure to appear in court as ordered
- ❒ Prior attempt(s) to evade law enforcement
- ☑ Use of alias(es) or false documents
- ❒ Background information unknown or unverified
- ❒ Prior violations of probation, parole, or supervised release

C. OTHER REASONS OR FURTHER EXPLANATION:

The defendant's evidence/arguments for release:

See Attachment.

Nature and circumstances of offense:

See Attachment.

The strength of the government's evidence:

See Attachment.

The defendant's history and characteristics, including criminal history:

See Attachment.

The defendant's dangerousness/risk of flight:

See Attachment.

Part IV - Directions Regarding Detention

The defendant is remanded to the custody of the Attorney General or to the Attorney General's designated representative for confinement in a corrections facility separate, to the extent practicable, from persons awaiting or serving sentences or being held in custody pending appeal. The defendant must be afforded a reasonable opportunity for private consultation with defense counsel. On order of a court of the United States or on request of an attorney for the Government, the person in charge of the corrections facility must deliver the defendant to a United States Marshal for the purpose of an appearance in connection with a court proceeding.

Date: 02/15/2022

BERYL A. HOWELL
Chief Judge, United States District Court
for the District of Columbia

ATTACHMENT TO ORDER OF DETENTION PENDING TRIAL, PART III. C: Consideration of Defendant's evidence/arguments for release and 18 U.S.C. § 3142(g) Factors

(1) **The Nature and Circumstances of the Offense**:

The nature and circumstances of the offense weigh heavily in favor of detention. Defendant is charged in a two-count criminal complaint with conspiring to commit money laundering and conspiring to defraud the United States, Compl., ECF No. 1, based on his alleged participation in a conspiracy with his wife and co-defendant, Heather Morgan, to conceal and disguise the nature, location, source, ownership, and control of approximately 119,754 Bitcoin (with a current estimated value of over $5 billion) stolen from a 2016 hack of one of the world's largest virtual currency exchange's ("VCE"). Gov't's Mot. for Review of Release Order ("Gov't's Mot.") at 3, ECF No. 8. Although the government has not named the person or persons responsible for the hack, nor accused either defendant of being the actual hacker, the government proffers that the unidentified hacker initiated over 2,000 unauthorized bitcoin transactions, transferring 119,754 Bitcoin from wallets held by the victim VCE to an unhosted wallet, Wallet 1CGA4s ("Wallet 4s"), which was in defendants' control and served as the originating point for defendants' money laundering activities. *Id.* at 3–4.

Specifically, the government proffers that beginning around January 2017, defendants began moving a portion of the stolen bitcoin out of Wallet 4s "in a series of small, complex transactions across multiple accounts and platforms." Gov't's Reply in Supp. of Review Detention Order ("Gov't's Reply") at 3, ECF No. 18. According to the government, while engaging in these transactions, defendants used a multitude of complex money laundering techniques to conceal their activities 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 . . . ; (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 [bitcoin] to other forms of virtual currency, including anonymity-enhanced virtual currency, in a practice known as 'chain hopping'; and (6) using U.S.-based business accounts to legitimize activity." *Id.* at 6–7. Despite these serious attempts at concealment, the government was ultimately able to trace the stolen bitcoin to multiple accounts controlled by defendants, including accounts held by their businesses.

In tandem with these transactions, the government proffers defendants "repeatedly provided false information to and deceived" VCEs and other financial institutions doing business in the United States for the purpose of frustrating these institutions' due diligence efforts required by the Bank Secrecy Act. Statement of Offense ("SOF") at ¶¶ 56–59, ECF No. 1-1. The government proffered several examples of this conduct, which included both defendants lying to VCEs in response to "Know Your Client" and other due diligence inquiries and lying to financial institutions in order to conceal that the source of virtual currency held in their accounts was directly linked to the funds stolen in the 2016 hack. *Id.* at ¶¶ 22–23, 33–35, 37–38.

Aside from defendants' alleged activity involving the bitcoin transferred from Wallet 4s, the public bitcoin ledger showed that the majority of the stolen funds from the hack remained in the wallet. The government proffers that Wallet 4s was also in defendants' control. On January 31, 2022, law enforcement gained access to the wallet by decrypting a file saved to defendant's cloud storage account, which the government obtained pursuant to a search warrant. Gov't's Reply at 4. This file contained a list of 2,000 virtual currency addresses, along with their corresponding private keys. *Id.* According to the government, blockchain analysis confirmed

that almost all of the 2,000 addresses were directly linked to the 2016 hack. *Id*. Using the private keys discovered in defendant's file, the government was able to seize approximately 94,636 Bitcoin (currently valued at $3.6 billion).

As a result of this offense conduct, as noted, defendant is charged with two serious felony offenses: (1) one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h), which carries the penalty of the object of the conspiracy, which in this case is concealment money laundering, 18 U.S.C. § 1956(a)(1)(B)(i), which carries a maximum term of imprisonment of twenty years; and (2) one count of conspiracy to defraud the United States, in violation of 18 U.S.C. § 371, which carries a maximum term of imprisonment of five years. Defendant's conviction would also expose him to a significant financial penalty. *See* Gov't's Reply at 27; *see also United States v. Bikundi*, 47 F. Supp. 3d 131, 134 (D.D.C. 2014) (finding "substantial incentive to flee" where defendant faced 20-year maximum on money laundering charges); *United States v. Hong Vo*, 978 F. Supp. 2d 41, 43 (D.D.C. 2013) (finding detention appropriate for defendant facing high penalties for bribery and visa fraud).

The government points to other aspects of the nature and circumstances of defendant's offense conduct which are also highly probative of defendant's intent and risk and capability of flight and weigh in favor of detention. Specifically, the government proffers that the government's searches and seizures related to these charges revealed:

(1) defendant's cloud storage account, which held the file critical for the government to be able to seize the majority of the stolen funds, also held other incriminating documents, including "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," Gov't's Reply at 12–13;

(2) another file in the cloud storage account that is titled "VETTED VENDORS" contains a list of darknet vendors offering for sale identification documents, passports, and debit and bank cards, *id.* at 14–16, and corresponding evidence suggesting that defendants received a package containing identification information for Russian personas from a darknet vendor while they were in Ukraine in 2019, *id.* at 7, 14–17;

(3) the cloud storage account also had several folders containing Russian and Ukrainian persona information in the form of passports, identification information, and biographical information for numerous individuals, both male and female, *id.* at 13–14;

(4) law enforcement seized numerous items from defendants' residence that could be used to conceal their whereabouts and facilitate flight to foreign countries, including bags containing multiple cell phones and SIM cards, one of which was labeled "Burner Phone," as well as a substantial amount of foreign currency, *id*. at 17–21.

In sum, the alleged conduct underlying the charges strongly suggests that defendant is a sophisticated money laundering offender who is also savvy with technology and willing to accumulate and utilize multiple fictitious identities to bypass law enforcement efforts to detect his behavior.

Thus, the nature and circumstances of defendant's offense conduct weigh heavily in favor of pretrial detention.

(2) <u>The Weight of the Evidence Against the Person</u>:

The weight of the evidence against this defendant also strongly favors pretrial detention. The government has significant and strong direct and circumstantial evidence that defendant knowingly conspired to transfer and launder the proceeds of an unlawful activity, *i.e*., the stolen bitcoin from the 2016 hack of the victim VCE, through a series of complex financial transactions

designed to conceal the nature, location, source, ownership, or control of the proceeds. Key evidence strongly supporting the charges in this case include:

1. To secure their cryptocurrency assets, bitcoin owners keep confidential or otherwise protect the access credentials necessary for transferring their bitcoin. Defendant's conduct here makes this fact readily apparent. A file in defendant's cloud storage account listed "all of the addresses within Wallet [4s] and their corresponding private keys." Gov't's Reply at 11. That file was "secured with a strong encryption algorithm and a lengthy password," one that the government argues "would typically prevent even a well-resourced attacker from accessing the file within his lifetime." *Id*. The government used those addresses and keys to access and seize the remaining bitcoin held in Wallet 4s, the initial repository of all the stolen bitcoin. *Id*. This direct evidence of defendant's ownership and control of the original source of laundered funds contravenes defendant's argument that there is "nothing . . . resembling direct proof of the charges." Defs.' Opp'n to the Gov't's Mot. for Review of Their Bail Conditions ("Defs.' Opp'n") at 5, ECF No. 21.
2. Blockchain evidence showing the subsequent laundering of the stolen bitcoin through darknet markets, accounts at various VCEs, and conversion into anonymity-enhanced virtual currency and other currency. SOF at ¶¶ 9–50. Defendant contends that some of these transactions do not reflect criminal intent to conceal funds because they employ common techniques "used for legitimate purposes in thousands of transactions." Defs.' Opp'n at 5–6. This argument is simply unpersuasive as it ignores the context in which these transactions occurred: defendant's attempt to conceal the source of bitcoin stolen

from one of the largest VCE's in the world by purposefully using techniques that can obscure activity on the blockchain.

3. Financial records for defendants showing how numerous accounts held in both defendants' names received deposits traceable to the 2016 hack. Gov't's Reply at 27.
4. Evidence of purchases by both defendants that the government traced to the stolen bitcoin, including purchases of 70 one-ounce gold coins shipped to defendant at his home address. SOF at ¶¶ 21, 45–50.
5. A spreadsheet that detailed the log-in information and the status of many of the VCE accounts used to launder the stolen funds traced back to the hack, including notations confirming their status as frozen or emptied. Gov't's Reply at 11–12; SOF at ¶¶ 14–17. The government has also corroborated that spreadsheet accurately reflects the account status of accounts for which the relevant VCEs did freeze those accounts due to suspicious activity. SOF at ¶¶ 14–17, 28–29.
6. References in defendant's files to having some dirty and some clean wallets holding cryptocurrency, including wallets files with names that included variations of the word "dirty." Gov't's Reply at 12.
7. Both defendants' false statements to various VCEs attempting to conduct anti-money laundering due diligence into the nature of their account activity and the source of their account funds, which constitutes further evidence of defendants' consciousness of guilt. Gov't's Reply at 8–10; SOF at ¶¶ 31–39.

The strength of the government's evidence weighs heavily in favor of the government's contention that defendant presents a serious risk of flight. The nature of the offense, particularly the substantial criminal and financial penalties defendant faces, creates an incentive to flee. That

incentive only increases where, as here, the evidence the government has proffered at this stage of the case is overwhelmingly strong. Accordingly, the likelihood that there are conditions of release that will reasonably assure defendant's appearance correspondingly decreases.

In short, the weight of the evidence suggesting that defendant conspired to launder approximately 119,754 Bitcoin from the 2016 hack is very strong and favors pretrial detention.

(3) **The History and Characteristics of the Person**:

Defendant has no criminal convictions or prior arrests and has strong family ties connecting him to the United States. Defs.' Opp'n at 2. Although defendant was born in Russia, he spent the bulk of his childhood in Chicago, and his mother, father, and brother all reside and are employed in the United States. *Id.* at 2 n.2. Defendant also strongly asserts that any flight would "deprive [him] of the ability to vigorously contest," the charges against him, *id.* at 8, which defendant apparently considers to be filled with "significant holes," *id.* at 5. The Court appreciates that the complexity of this case and the likelihood of voluminous evidence renders defendant essential to his own defense and that of his co-defendant spouse, which may create a strong anchor to remain in the United States while they await trial. These factors would usually assuage concerns as to whether defendant poses a serious risk of flight. *See* 18 U.S.C. § 3142(f)(2)(A).

Yet, concerns about defendant's risk of flight and potential for obstructive conduct, *id.* § 3142(f)(2)(B), persist here given (1) defendant's apparent access to substantial financial resources that could be used to facilitate his flight, including 7,506 Bitcoin (currently valued at over $328 million) which the government determined was removed from Wallet 4s and directly

transferred to 24 virtual currency addresses,[1] and 70 one-ounce gold coins defendants purchased using virtual currency traced to the hack that the government could not locate when searching defendants' residence and storage unit, Gov't's Reply at 29–30, 32, (2) defendant's skillset and background in coding, reverse engineering hardware, and cryptocurrency, *id.* at 25, which demonstrates his ability to access and launder bitcoin "from anywhere in the world with an Internet connection," *id*. at 29; defendant's extensive international travel, Russian language skills, and ties to Russia, including citizenship and an active passport, *id.* at 30, (3) defendant's acquisition and use of biographical information and identification documents for numerous individuals, including Russian and Ukrainian personas, which obviously may be used for creating false identities to avoid law enforcement detection, *id.* at 14, (4) evidence demonstrating defendant's knowledge of darknet vendors who offer passports or identification cards for sale, *id.* at 12, and (5) files in defendant's cloud storage that indicate his access to numerous accounts at Russian financial institutions, *id.* at 30—all of which demonstrate that defendant "appear[s] to have taken meaningful steps toward establishing new identities and financial accounts in Ukraine and Russia to enable . . . flight," *id.* at 31–32. These considerations raise serious concerns about defendant's willingness to comply with even the most stringent release conditions.

Defendant contends that, even assuming he has the access and skillset to flee, he has "stayed put in [his] residence in . . . New York even after learning of the Government's investigation targeting [defendants] in this case." Defs.' Opp'n at 2–3, 8. The New York magistrate judge, in deciding to release defendants, relied almost exclusively on "the fact defendants have not to this date gone anywhere over the last two, three months," Rough Hearing Tr. (Feb. 8, 2022) at 65, ECF No. 21-3, despite "being aware of the investigation since at least

[1] Given the strong direct evidence of defendant's control of Wallet 4s, the government makes the reasonable assumption that the defendant also has the means to access and transfer this bitcoin as well.

November [2021], even after search warrants were executed in more than one location, and even after they knew specifically through counsel of the nature of this investigation, and the alleged seriousness of the investigation, and the allegation [that] the government was looking into their theft of millions of dollars," *id.* at 44–45, considering it "a strong factor that counsels in favor of allowing them to report on their own," *id.* at 45. The full chronology of events, however, merits a different assessment of defendant's flight calculus.

First, defendant's notification by an internet service provider in November 2021 that the government used a grand jury subpoena to seek records pertaining to defendants an entire year earlier would not raise sufficient red flags for defendant to flee immediately. Gov't's Reply at 33. The passage of a year from the grand jury subpoena without any criminal charges more likely gave defendant false confidence that the strong encryption used on inculpatory files worked and that the government had come up empty handed if able to see inside his electronic accounts. With the strength of the encryption protecting their incriminating files and defendants having no knowledge of any further actions taken against them, there was no serious motivation for them to flee at that point.

The government's execution on January 5, 2022, of a search warrant on defendants' residence and storage unit would be more cause for alarm. Gov't's Reply at 17. Indeed, during the search, defendant's wife actively attempted to make it difficult for law enforcement to conduct a search of her cell phone, indicating a heightened concern about the government's investigation. *Id*. Additionally, during January 11 through January 31, 2022, defendants' counsel and the government engaged in discussions concerning the investigation. Defs.' Opp'n at 3. On January 22, 2022, the government provided a written summary of its theory of how stolen bitcoin was traced through various transaction paths to numerous accounts controlled by

defendants, and counsel provided that written summary to defendants. *Id*. Thus, by then, defendants likely had awareness of the government's focus and belief that they were intimately involved with laundering the stolen bitcoin from the 2016 hack.

Still, at that point, defendants had no indication that the government had discovered and decrypted the highly inculpatory files in defendant's cloud storage directly linking them to the immense amount of stolen virtual currency from the 2016 hack. The government proffers that this decryption did not occur until January 31, 2022, and the earliest indication defendants would have had of the fact would have been late January 31 or early February 1, when the government initiated the seizure of the remaining stolen bitcoin in Wallet 4s and removed it—anyone watching the public blockchain ledger could see the movement of bitcoin. Gov't's Reply at 33. That realization could have easily changed the flight calculus for this defendant. Yet, at this time, the government had already seized significant resources during the January 5, 2022 search that could have enabled defendants' immediate flight, including defendants' passports, numerous electronic devices containing wallets holding cryptocurrency, cell phones, substantial amounts of foreign currency, and $40K in cash. *Id.* at 17–21.

Additional obstacles hindered defendants from fleeing, including (1) defendant Morgan's surgery on January 31, 2022, Defs.' Opp'n at 4, (2) defendant Morgan's suffering from limited mobility due to the surgery, *id*., (3) defendant Morgan's need to have follow-up appointments to ensure that there were no complications from surgery, *id.*, and (4) a major snowstorm on February 4, 2022, that caused widespread flight cancellations and made travel impracticable, Gov't's Reply at 33.

Now that these obstacles have been mostly mitigated and the government has revealed the strength of its evidence as well as its predictions concerning the significant financial and

criminal penalties both defendants potentially face, defendant's motivation to flee has increased exponentially, and his available resources and skillsets that could facilitate flight is of huge concern.

In response, defendant argues that the strict bail conditions set by the New York magistrate judge "make it virtually impossible for them to [flee] . . . as a logistical matter," and provide strong incentive for them to remain given that flight would "cause their parents to forfeit their homes." Defs.' Opp'n at 8. This argument fails to account for defendants' alleged access to millions of dollars in cryptocurrency and defendant's ability to access these funds "with an Internet connection from anywhere in the world," Gov't's Reply at 29, defendant's dozens of accounts set up at financial institutions around the world, including Ukraine and Russia, *id.* at 30–32, and defendant's "established history of creating and using fictitious identities and concealing their activities online," *id.* at 31, all of which show that defendant's compliance with release conditions is highly questionable and demonstrate that it is far "from virtually impossible" for defendant to flee. Furthermore, the government proffers that, during the course of this scheme, defendants have routinely "abandoned hundreds of thousands of dollars' worth of virtual currency at exchanges, after the exchanges flagged the funds as suspicious." *Id.* 32. In turn, the short-term loss of funds or his parents' house could easily be rectified once defendant successfully flees, accesses the millions of unaccounted for bitcoin, and sets up a new life abroad.

Thus, taken together, defendant's history and characteristics weigh in favor of pretrial detention.

(4) <u>The Nature and Seriousness of the Danger to Any Person or the Community that Would be Posed by the Person's Release:</u>

The nature and seriousness of the danger of obstructive conduct posed by defendant's release weigh in favor of detention. The strong evidence supporting the money laundering charge, under 18 U.S.C. §§ 1956(h) and 1956(a)(1)(B)(i), and the fraud charge, under 18 U.S.C. § 371, raises serious concerns about defendant's willingness to use his knowledge and skills to engage in similar conduct in the future to further obstruct law enforcement functions and judicial proceedings. Defendant's money laundering activities and deceitful statements to financial institutions demonstrate a willingness to take action to impede law enforcement's investigatory efforts regarding the proceeds of the 2016 hack, as well as a willingness to circumvent legal or regulatory requirements. All of which suggest that, if released, defendant would not hesitate to attempt to conceal or destroy evidence of the conspiracy in the future to further obstruct law enforcement functions and judicial proceedings. This risk of noncompliance is only increased by defendant's alleged continuing control over possibly millions of dollars in bitcoin, facility with darknet vendors, levels cryptocurrency sophistication, and pattern of establishing financial accounts with fictitious identities—means and resources that would be of substantial use in any attempts to engage in future obstruction.

Defendant therefore represents a danger of future obstructive conduct that can only be effectively prevented through pretrial detention and thus this final factor also weighs against his release.