UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

v.

ROMAN STERLINGOV,

Defendant.

Criminal Action No. 21-399 (RDM)

MEMORANDUM OPINION AND ORDER

This matter is before the Court on Defendant Roman Sterlingov's motion to revoke his pretrial detention. Dkt. 17. Sterlingov has been charged with money laundering, operating an unlicensed money transmitting business, and money transmission without a license, all in relation to his alleged operation of a Bitcoin mixer known as Bitcoin Fog. Dkt. 8. Sterlingov, a dual citizen of Sweden and Russia, Dkt. 1-1 at 1, was arrested on April 27, 2021, in Los Angeles, California, when he arrived at Los Angeles International Airport, Dkt. 5. Magistrate Judge Paul L. Abrams of the United States District Court for the Central District of California ordered that Sterlingov be detained pending trial. Dkt. 17-1 at 5. Sterlingov now moves to revoke that order and requests release on home detention, subject to various conditions including location monitoring and internet restrictions, pending trial.

For the reasons that follow, the Court will **DENY** Sterlingov's motion, Dkt. 17.

I. BACKGROUND

The following background is taken from the government's charging instruments, the affidavit of Special Agent Devon Beckett, the parties' briefs and proffers at the hearing held on October 25, 2021, and the exhibits tendered to the Court. *See United States v. Smith*, 79 F.3d

1208, 1209–10 (D.C. Cir. 1996) (defendant and the government may proceed by way of proffer); 18 U.S.C. § 3142(f) (providing that usual "rules concerning admissibility of evidence in criminal trials do not apply to the presentation and consideration of information at" a detention hearing). It bears emphasis, however, that the Court's description of the relevant facts is necessarily preliminary and incomplete and does not represent a determination on the merits, which is both premature and, in any event, the province of the jury.

The government alleges that Sterlingov operated "an illicit Bitcoin money transmitting and money laundering service" known as Bitcoin Fog. Dkt. 1-1 at 1; *see also* Dkt. 8 (indictment). "Bitcoin is a decentralized form of electronic or digital currency that exists only on the internet." *United States v. Harmon*, 474 F. Supp. 3d 76, 80 (D.D.C. 2020) (quotation marks and alterations omitted). The term "bitcoin" refers to both "a system" that facilitates financial transactions and "a unit" of currency. *Id.* Bitcoin the system "is a peer-to-peer network enabling proof and transfer of ownership—of units, or tokens, also called bitcoin—without involving a third-party such as a bank," *id.*, while bitcoin the unit is a virtual currency "transacted over the Internet using Bitcoin software," Dkt. 1-1 at 1 n.1.[1] This software permits users to create "'Bitcoin addresses,' roughly analogous to anonymous accounts," and to "securely transfer[] bitcoin from one Bitcoin address to another." *Id.* "[T]he identity of a Bitcoin address owner is generally anonymous," although "law enforcement can often identify the owner of a particular Bitcoin address by analyzing the blockchain," which "is essentially a distributed public ledger that keeps track of all Bitcoin transactions, incoming and outgoing, and . . . records every address that has ever received a bitcoin and maintains records of every transaction." *Id.* at 3 & n.3.

[1] "The Bitcoin network and its protocols are [typically] referred to with a capital B, while the units [of virtual currency] transmitted on the network are referred to with a lowercase b," a convention the Court adopts here. *Harmon*, 474 F. Supp. 3d at 81.

As explained in the affidavit of Devon Beckett, a Special Agent assigned to the Internal Revenue Service, Criminal Investigation (IRS-CI), Bitcoin Fog is a bitcoin mixer (or tumbler) that offers further anonymity to those engaged in bitcoin transactions. *Id.* at 1–2. Bitcoin Fog can only be accessed through a "Tor hidden website." *Id.* at 1. Tor "is a computer network designed to facilitate anonymous communication over the Internet," *id.* at 1 n.1, "by routing user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ('IP') address of the user," *United States v. Galarza*, No. 18-mj-146, 2019 WL 2028710, at *2 (D.D.C. May 8, 2019) (quotation marks omitted). Because of the sophisticated methods used by the Tor network to conceal both users and website hosts, "neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address—and therefore the location—of a computer server that hosts a hidden service." Dkt. 1-1 at n.1. "For these reasons, hidden services are often referenced as residing on the 'darknet' or 'Dark Web,' and ordinary Internet websites are often referenced as residing on the 'clearnet.'" *Id.*; *see also Harmon*, 474 F. Supp. 3d at 82 (describing the darknet).

Once users access Bitcoin Fog, the service enables them "to send bitcoins to designated recipients in a manner designed to conceal and obfuscate the sources of the bitcoins." Dkt. 1-1 at 1–2. Bitcoin Fog does this by "disassociating incoming bitcoin from particular Bitcoin addresses or transactions and then comingling that bitcoin with other incoming bitcoin prior to conducting further transactions." *Id.* at 2. "This process," according to the government, permits Bitcoin Fog "customers engaged in unlawful activities to launder their proceeds by concealing the nature, source, and location of their 'dirty' bitcoin." *Id.* Although the case is at a preliminary stage, the government has offered some evidence that Bitcoin Fog was aware of the nature of its customer base. At its launch, an announcement on an online Bitcoin forum advertised that

Bitcoin Fog's mixing services "can eliminate any chance of finding your payments[,] . . . making it impossible to prove any connection between a deposit and a withdraw[al] inside our service," *id.*, and a subsequent post on the same forum (dated a few months later) contrasted Bitcoin Fog with "legitimate, visible businesses, which will be forced to reveal information about [users'] funds, should such a request be made by the authorities," *id.* at 3. Such tactics would prove difficult with Bitcoin Fog, the second post continued, because "the authorities have to find [us] first." *Id.*; *see also* Dkt. 19 at 4 (Figure 3) (announcing as part of launch that "not only will we not cooperate with any authorities, the authorities will not actually be able to show up at our doorstep, because finding a [T]or doorstep has proven difficult"). According to the Beckett affidavit, over 1.2 million bitcoins—worth over $335 million at the time of the transactions—have been sent through Bitcoin Fog since the site's launch in 2011. Dkt. 1-1 at 3–4.

A substantial portion of that sum, Special Agent Beckett attests, has been linked to online marketplaces known to facilitate unlawful conduct. Federal law enforcement used blockchain analysis to "identify bitcoins sent directly to [Bitcoin Fog] from known darknet markets and bitcoins sent from [Bitcoin Fog] to known darknet markets," which "primarily traffic in illegal narcotics and other illegal goods and services." *Id.* at 4. One such darknet market, Silk Road, has been described elsewhere as "the most sophisticated and extensive criminal marketplace on the Internet." *United States v. Ulbricht*, 31 F. Supp. 3d 540, 549 (S.D.N.Y. 2014). According to the Beckett affidavit, the government has identified "$78 million in transactions" that Bitcoin Fog sent or received "involving known darknet markets, counting only direct transactions." Dkt. 1-1 at 4. The evidence further suggests that Bitcoin Fog had a relationship with the darknet market Agora, which the government describes as "one of the darknet's largest illegal marketplaces selling illegal narcotics and other goods." Dkt. 19 at 8. When Agora launched in

December 2013, for example, Bitcoin Fog explained to its users that "[t]he marketplace is operated by associates of ours in whom we have complete trust both in terms of not being a honeypot (if they were, we would be in jail) and in terms of their security expertise." *Id.* at 10 (Figure 8). Bitcoin Fog users encountered this message, in the form of an advertisement, when they logged into the service following Agora's launch. *Id.* at 9 (Figure 7).

Bitcoin Fog's founder and "principal operator," according to the government, was the Defendant in this case, Roman Sterlingov. Dkt. 1-1 at 7. As the Beckett affidavit recounts, when the site was founded in October 2011, a user with the pseudonym Akemashite Omedetou announced the launch on BitcoinTalk.org, an online forum. *Id.* at 2. The announcement included links to Bitcoin Fog's clearnet site, its Tor site, and its Twitter feed. *Id.* The clearnet site domain—its non-Tor website, *id.* at 1 n.1—was registered to the same pseudonym, Akemashite Omedetou, and paid for from a Liberty Reserve account, *id.* at 7. Liberty Reserve, which has since been shut down by U.S. law enforcement based on money laundering charges against its founder, "was a Costa Rica-based digital currency exchange service that allowed users to register and transfer money to other users with only a name, e-mail address, and birth date." *Id.* at 7 n.5. That Liberty Reserve account was traced, through a six-layered transaction involving four different currencies, to a different bitcoin account—this time the Japan-based Mt. Gox exchange—that Sterlingov "opened . . . in his true name." *Id.* at 8. *See generally id.* at 7–9 (describing law enforcement's efforts to determine the identity of the Liberty Reserve account holder); Dkt. 19 at 20 (diagramming the various transactions through which the government linked Sterlingov to the pseudonym Akemashite Omedetou). Investigators later obtained, via search warrant, the contents of a Google account linked to Sterlingov's telephone number. Dkt. 19 at 21. That account included, among other things, a "Russian language document . . .

describing how to layer funds" and an outline of the multilayered transaction used to pay for Bitcoin Fog's clearnet domain name. *Id.*

Special Agent Beckett further attests that Sterlingov's accounts, including his Mt. Gox account, sent "a series of small value transactions" through Bitcoin Fog in October 2011 as a way of "beta-test[ing] [the] new software" prior to the site's launch. Dkt. 1-1 at 10. And, throughout Bitcoin Fog's operation, the pseudonym Akemashite Omedetou posted on BitcoinTalk.org, praising the Bitcoin Fog's features, providing updates on the service, and responding to comments and critiques. *See id.* at 2; Dkt. 19 at 5–6 (Figure 4). In the government's view, this evidence supports its allegation that Sterlingov was Bitcoin Fog's founder and "principal operator." Dkt. 1-1 at 7.

This is a significant allegation for present purposes because there is reason to believe that Bitcoin Fog has generated massive profits. According to the Beckett affidavit, Bitcoin Fog charges "a variable fee" between 2% and 2.5% on each deposit. Dkt. 1-1 at 11. Based on the service's transaction activity, Special Agent Beckett calculates that these fees would have exceeded $8 million in value, if they were converted into cash at or near the time of the relevant transactions. *Id.* But bitcoin has appreciated dramatically since Bitcoin Fog's launch—from $2 during the fall of 2011 to a current value of between $40,000 and $50,000—and so Special Agent Beckett estimates that Sterlingov's total assets within Bitcoin Fog could approach $70 million. *Id.*

The government charged Sterlingov by criminal complaint on April 26, 2021, with money laundering, in violation of 18 U.S.C. § 1956(a)(3)(A); operating an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(a); and money transmission without a license, in violation of D.C. Code § 26-1023(c). Dkt. 1; *see also* Dkt. 8. Sterlingov was arrested on April 27, 2021, when he arrived at Los Angeles International Airport following a direct flight from Moscow, Russia. Dkt. 19 at 24. At the time of his arrest, Sterlingov was carrying "four passports—two Russian and two Swedish." Dkt. 17 at 16–17 n.8. Sterlingov's luggage, which the Customs and Border Patrol officers subjected to an inventory search, included Google account recovery codes, bitcoin debit cards, multiple laptops, Raspberry Pi microcomputers, roughly 15 memory cards, multiple cell phones, and "an unusual cellular modem device" that, the government says, "appears to be designed to combine up to four separate cellular Internet connections in order to anonymize a computer's Internet traffic or connections to other servers." Dkt. 19 at 25. The Google account recovery codes were for the Google account that investigators linked to the purchase of Bitcoin Fog's clearnet domain name. *Id.* at 21–22. Sterlingov's electronic devices, moreover, "contained programs for location spoofing, including GPS spoofing." *Id.* at 25.

Sterlingov, for his part, strenuously resists the implication that there is "something untoward" about the contents of his luggage. See Dkt. 22 at 11–12 n.7. The "location spoofing" programs, Sterlingov explains, are "readily available and popular applications" that may be used "for online games such as Pokemon Go," while the cellular modem device described as "unusual" by the government is "a mass-produced travel modem" that "helps provide a steady and reliable internet connection when streaming movies or conducting Internet calls." *Id.* He further notes that, under Swedish and Russian law, he is permitted to possess multiple passports and that he had legitimate reasons for possessing two Swedish passports and two Russian passports. Dkt. 17 at 16-17 n.8.

Following a detention hearing, Magistrate Judge Paul L. Abrams ordered Sterlingov detained pending trial. Magistrate Judge Abrams found that Sterlingov represented a serious risk of flight, based on the following four findings: "(1) defendant is not a U.S. citizen; (2) insufficient ties to US to reasonably assure defendant's appearance; (3) inadequate bail resources proffered; and (4) alleged access to and use of false identification, including possession of multiple passports at time of arrest." Dkt. 17-1 at 4 (Detention Order).

II. LEGAL STANDARD

Under 18 U.S.C. § 3145(b), a defendant ordered detained by a magistrate judge may file "a motion for revocation or amendment of the order" with "the court having original jurisdiction over the offense." 18 U.S.C. § 3145(b). Although the D.C. Circuit has yet to opine on the question, *see United States v. Munchel*, 991 F.3d 1273, 1280 (D.C. Cir. 2021), substantial precedent supports the view that a magistrate judge's detention order is subject to *de novo* review by the district court, *see United States v. Hunt*, 240 F. Supp. 3d 128, 132–33 (D.D.C. 2017) (identifying cases supporting this proposition from the Second, Third, Fourth, Fifth, Sixth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits), and this Court has adopted that view, *United States v. Taylor*, 289 F. Supp. 3d 55, 66 (D.D.C. 2018).

The Bail Reform Act permits pretrial detention in only "carefully defined circumstances." *United States v. Simpkins*, 826 F.2d 94, 95–96 (D.C. Cir. 1987). The question for the Court is whether any "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). If not, the Court "shall order the detention of the [defendant] before trial." *Id.* "The facts the judicial officer uses to support a finding . . . that no condition or combination of conditions will reasonably assure the safety of any other person and the community [must] be supported by clear and convincing evidence," and the government bears the burden of proof as to that evidence. *Id.* § 3142(f)(2)(B). Only a preponderance of the evidence, however, is required to support "[a] determination that an individual is a flight risk." *United States v. Vasquez-Benitez*, 519 F.3d 546, 551 (D.C. Cir. 2019).

"In our society liberty is the norm, and detention prior to trial or without trial is the carefully limited exception." *United States v. Salerno*, 481 U.S. 739, 755 (1987); *see also Taylor*, 289 F. Supp. 3d at 62 ("The default position of the law . . . is that a defendant should be released pending trial.") (internal quotation marks and citation omitted).

III. ANALYSIS

The government does not contend that Sterlingov's detention is necessary to ensure "the safety of any other person and the community," and, thus, the sole question before the Court is whether any "condition or combination of conditions" or pretrial release "will reasonably assure the appearance of the person as required." 18 U.S.C. § 3142(e). In determining whether Sterlingov should be detained, the Court must consider: (1) the nature and circumstances of the offense charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. 18 U.S.C. § 3142(g). Although a close question, the Court concludes that these factors weigh in favor of continued detention.

A. Nature and Circumstances of the Offense

The first factor—the nature and circumstances of the offense—weighs in favor of detention. Sterlingov is charged with founding and operating a sophisticated Bitcoin mixing service that facilitated more than $335 million in untraceable transactions, including more than $78 million sent directly to or from darknet markets (such as Silk Road) that primarily trafficked in illegal narcotics and other illegal goods and services. Dkt. 1-1 at 3–5. According to the government (and as supported by the Beckett affidavit), these illicit transactions did not find their way to Bitcoin Fog by accident; instead, Bitcoin Fog's advertised purpose was to enable users to evade detection by legal authorities as they conducted business with bitcoin. *See* Dkt. 19 at 3–6 (Figures 2–4). Consistent with this illicit purpose and user base, Sterlingov allegedly went to extraordinary lengths to evade detection as Bitcoin Fog's administrator. As explained in the Beckett affidavit, Sterlingov paid for the clearnet domain that hosted Bitcoin Fog, for example, through a six-layered transaction involving four forms of currency, three virtual currency payment services, and accounts registered with three different burner email accounts. *See* Dkt. 1-1 at 8 (describing and diagramming this transaction). Sterlingov's efforts, Special Agent Beckett estimates, left him potential gains approaching $70 million in bitcoin. *Id.* at 11.

According to the government, Sterlingov's alleged crimes did more than just enrich him. In addition, the government alleges, Bitcoin Fog enabled tens of millions of dollars in transactions through darknet marketplaces, such as Silk Road and Agora, known to "primarily traffic in illegal narcotics and other illegal goods and services." *Id.* at 4; *see also Ulbricht*, 31 F. Supp. 3d at 549. Although Sterlingov dismisses the government's discussions of darknet marketplaces such as Silk Road and Agora as an effort to use "the wrongdoing doing of others . . . to literally paper over the fact that the government has no proof when it comes to its case-in-chief," Dkt. 22 at 6, the Court cannot agree. According to the Beckett affidavit, Bitcoin Fog derived a substantial portion of its business from direct transactions to and from these darknet marketplaces, Dkt. 1-1 at 4, and so the wrongdoing facilitated by those marketplaces cannot be so cleanly severed from the service Sterlingov stands accused of founding and operating. Indeed, the dangers attendant to unfettered, untraceable financial transactions are the very reason Congress added licensing requirements to the laws prohibiting money laundering; the federal ban on unlicensed money transmitting businesses was enacted "in order to combat the growing use of money transmitting businesses to transfer large amounts of the monetary proceeds of unlawful enterprises." *United States v. Velastegui*, 199 F.3d 590, 593 (2d Cir. 1999); *see also* S. Rep. No. 101-460 (1990) ("Increasingly, money launderers are using money transmitters, check cashers, money exchanges and other nonbank financial companies for initial placement and the number of such businesses is growing rapidly in some States.").

If the government proves its case, moreover, Sterlingov's exposure to criminal penalties is substantial. The government estimates that the Sentencing Guidelines recommendation for Sterlingov, if he is convicted on all counts, may be "as long as 30 years," largely due to the amount of money—$335 million—in illicit bitcoin transactions the government attributes to Bitcoin Fog. Dkt. 19 at 35; *see also id.* at 35 n.12 (explaining this calculation). Sterlingov objects that the government arrives at this number only after "giving itself the benefit of every doubt and making a long string of unsupported assumptions for which it lacked any real proof." Dkt. 22 at 6. But, contrary to Sterlingov's assertions, the government has offered some evidence supporting its contentions, including evidence that Sterlingov knew "he was in the business of money laundering." Dkt. 17 at 14. According to the Beckett affidavit, the government's blockchain analysis has traced "$78 million in transactions" that Bitcoin Fog sent or received to "known darknet markets," Dkt. 1-1 at 4, and Bitcoin Fog actively directed its users to the darknet marketplace Agora, Dkt. 19 at 8–9 (Figure 7). Perhaps the best evidence that Bitcoin Fog (and, thus, arguably Sterlingov) knew its business did not comply with applicable laws and regulations is its post regarding the launch of the Agora darknet marketplace: "The marketplace is operated by associates of ours in whom we have complete trust both in terms of not being a honeypot (if they were, *we would be in jail*)." *Id.* at 10 (Figure 8) (emphasis added).

For present purposes, the Court need not—and does not—express a view on the precise exposure Sterlingov faces or the applicable Sentencing Guidelines ranges. The Court is convinced, however, that, given the vast sums of money that Bitcoin Fog allegedly processed, Sterlingov's potential sentence is sufficiently lengthy to create a substantial incentive to flee.

The nature and circumstances of Sterlingov's offense, accordingly, weigh in favor of pretrial detention.

B. Weight of Evidence Against the Defendant

The second factor—the weight of evidence against the defendant—also weighs in favor of detention. The government has offered substantial evidence that Sterlingov was Bitcoin Fog's founder. *See* Dkt. 19 at 17–22. That evidence includes a detailed explanation of the investigation that linked Sterlingov to Bitcoin Fog's clearnet domain name, Dkt. 1-1 at 8; Dkt. 19 at 19, along with printouts of Google recovery codes that Customs and Border Patrol officers discovered in Sterlingov's luggage that further link him to one of the Mt. Gox accounts included in that same transaction, Dkt. 19 at 21–22. Sterlingov responds that the government's evidence is limited to his "allegedly paying the domain fees for www.bitcoinfog.com through a third-party host." Dkt. 22 at 5. But the government has also offered evidence that appears to trace some of Bitcoin Fog's "earliest transactions" to Sterlingov through the same Mt. Gox account, Dkt. 1-1 at 10. These transactions, though small, are revealing because they seemingly represent the type of "beta testing" that is often "conducted to confirm that a site's features work" and that was arguably conducted here "to ensure [that] the tumbler's algorithm [was] properly working." *Id.* This kind of testing, Special Agent Beckett attests, is generally done by "software and web developers," *id.*, suggesting that Sterlingov did far more for Bitcoin Fog than simply purchase the clearnet domain name, *see also* Dkt. 19 at 23 ("[B]eta testing would typically only be conducted [by] an individual involved in administrating a website or service."). Throughout Bitcoin Fog's existence, moreover, the pseudonym Akemashite Omedetou posted on behalf of the service on online forums, and law enforcement traced that pseudonym—through the email account under which it was registered—to Sterlingov. Dkt. 1-1 at 7–8; Dkt. 19 at 18.

The asserted connection between Bitcoin Fog and Sterlingov outlined in the Beckett affidavit is important because there seems to be little dispute (at least on the present record) that Bitcoin Fog failed to register with the federal authorities or obtain a license from the District of Columbia, as required by 18 U.S.C. § 1960(a) and D.C. Code § 26-1023(c), respectively. Although the application of these statutes to bitcoin mixers is (like the virtual currency itself) a recent development, the only authority the parties have identified for the Court concluded, after a thorough analysis, that those statutes do apply to services like Bitcoin Fog. *See United States v. Harmon*, 474 F. Supp. 3d 76, 88, 99 (D.D.C. 2020). And Sterlingov offers no response (at least at present) to the government's argument that neither statutory provision allows for an "ignorance-of-the-law defense" as to these registration and licensing requirements. *See* Dkt. 19 at 38–39 & n.13 (collecting cases). As for the money laundering charge against Sterlingov, the government has introduced the results of blockchain analysis by its cyber analysts tracing tens of millions of dollars from darknet marketplaces, known for the exchange of illegal goods and services, to and from Bitcoin Fog. *See* Dkt. 1-1 at 4.

Although the evidence before the Court is undoubtedly incomplete at this early stage of the proceeding, the Court is persuaded that the weight of that evidence further supports pretrial detention.

C. History and Characteristics of the Defendant

The third factor—the history and characteristics of the defendant—likewise weighs in (at least modestly) favor of pretrial detention. In evaluating this factor, the Court must "take into account the available information concerning" the defendant's "character, physical and mental condition, family ties, employment, financial resources, length of residence in the community, community ties, past conduct, history relating to drug or alcohol abuse, criminal history, and record concerning appearance at court proceedings." 18 U.S.C. § 3142(g)(3)(A).

This factor presents a closer question than the first two. There is no indication, for example, that Sterlingov has any "history relating to drug or alcohol abuse" or "criminal history," *id.* As for his "community ties," *id.*, however, Sterlingov is a dual citizen of Sweden and Russia who has lived in Sweden (and, perhaps, elsewhere in Europe) since he was 14. Dkt. 22 at 2 n.2. Sterlingov points to a cousin in Boston, Massachusetts, to suggest strong family ties to the United States, Dkt. 17 at 7, but at the motions hearing, Sterlingov's cousin acknowledged the two had not seen each other in person since 2016. The parties dispute the extent of Sterlingov's ties to Sweden. The government claims that Sterlingov's recent residences include Spain and Germany, rather than Sweden, *see* Dkt. 19 at 43–45, while Sterlingov responds that he "frequently travels to," but does not live in, "Spain and Germany" and that he "once used a German address to receive packages while at a seminar," Dkt. 22 at 2 n.2. Regardless, however, there seems little dispute that Sterlingov's ties to the United States—beyond his family in Boston—are tenuous. Sterlingov's lack of significant ties to the United States distinguishes this case from the principal case on which Sterlingov relies, *United States v. Larry Harmon*, No. 19-cr-395 (D.D.C.), which involved a defendant who was a U.S. citizen and lifelong resident of

Ohio.[2] Although Sterlingov is correct that pretrial detention on the basis of a defendant's foreign nationality alone is improper, *see* Dkt. 22 at 3 (collecting cases), Sterlingov's lack of meaningful ties to the United States bears on the Court's decision.

The government claims, moreover, that Sterlingov has access to substantial funds from his operation of Bitcoin Fog, which he would be able to use to flee the country should he be released. Dkt. 19 at 40–41. This sum, according to the government, includes "at least $8 million"—and as much as almost $70 million—"in cryptocurrency proceeds from the transaction fees charged by Bitcoin Fog." *Id.* at 40; *see also* Dkt. 1-1 at 11. And, although the Court appreciates that Sterlingov's cousin has volunteered to post his ownership interest in both an investment property in Missouri and his condo in Boston as bond, Dkt. 17 at 7–8 & n.3; Dkt. 24 at 1, the value of those properties is dwarfed by the millions the government contends that Sterlingov has accrued through Bitcoin Fog. Sterlingov responds that the government has little in the way of "admissions" or "first-hand testimony" to prove the full amounts of Sterlingov's assets and that the government "has frozen or seized all of [his] funds." Dkt. 22 at 4. Sterlingov is correct that the government lacks any admissions or direct evidence of his assets. But Sterlingov stands accused of operating a highly sophisticated Bitcoin mixing service the purpose of which was to conceal financial transactions, and a grand jury has already found the evidence sufficient to return an indictment on those charges. *See* Dkt. 8. The prospect that the government has not located all of Sterlingov's assets, particularly his cryptocurrency accounts, is thus unsurprising.

[2] Although the public docket in *Harmon* does not include a transcript of the hearing at which the Court issued its oral ruling, the underlying motion to revoke pretrial detention emphasized that the defendant was a "36-year-old citizen" whose "lifelong residence [was] in Ohio" and that his "immediate family—his wife, parents[,] and siblings—all live[d] in and around Akron, Ohio." Def.'s Mot. at 1, 8, *United States v. Larry Harmon*, No. 19-cr-395 (D.D.C.) (Dkt. 15 at 1, 8).

Sterlingov's counsel points to the fact that he lacked sufficient funds to retain private counsel as evidence that lacks the enormous wealth that the government posits. The facts, however, undercut the premise of this argument and, if anything, support the government's contention that Sterlingov has not accounted for all of his assets. Particularly troubling is the fact that the government located (and seized) over $800,000 in U.S. dollars and cryptocurrency in June 2021, Dkt. 19 at 41, several months *after* Sterlingov submitted his financial disclosure form attesting that his assets were limited to two vehicles and checking and savings accounts containing less than ten percent of this amount, Dkt. 12. At the motions hearing, Sterlingov's counsel suggested that Sterlingov did not disclose all of his assets because he believed the government would soon freeze them and thus, in his mind, they were unavailable to pay counsel. But that explanation cannot be squared with Sterlingov's decision to disclose some—but far from all—of his assets. And the government's evidence strongly suggests that Sterlingov is adept at funneling money through various accounts and currencies in order to disguise their origins. The Court concludes, therefore, that it is likely that Sterlingov has additional funds that the government has yet to identify, which could be available to fund an effort to flee the country.

In addition to these funds, Sterlingov has a demonstrated familiarity with the darknet, where, as the government indicates, "[f]alse identification documents, including passports, are readily available on those markets." Dkt. 19 at 42. This is particularly true given Bitcoin Fog's close relationship with the darknet marketplace Agora. *See id.* at 8–11 (Figures 7 & 8). Sterlingov's familiarity with darknet marketplaces, along with his history "of creating numerous limited-use identities to obfuscate, conceal, and compartmentalize his activities online," *id.* at 42, suggest that pre-trial services would be unable effectively to enforce any internet restrictions the Court might place on Sterlingov were he released pending trial. Notably, pre-trial services does not have at its disposal the substantial resources that were necessary to trace the payment of Bitcoin Fog's clearnet domain name to Sterlingov, a single transaction that included six layers and four currencies. Dkt. 1-1 at 8. The Court cannot, as a result, be confident that pre-trial services would be able to adequately monitor Sterlingov's online activities.

At the time of his arrest, moreover, Sterlingov's luggage included a bevy of sophisticated electronic devices, along with four different passports. *See* Dkt. 17 at 16 –17 n.8; Dkt. 19 at 41–42. To be sure, Sterlingov has offered explanations for these devices, Dkt. 22 at 11–12 n.7, and this unusual number of passports, Dkt. 17 at 16–17 n.8. But whether devices such as the cellular modem or the "location spoofing" equipment also have benign uses, Sterlingov does not dispute that one of the functions of these instruments is to disguise one's Internet activity or location. Other evidence offered by the government, moreover, suggests that Sterlingov has gone to great lengths in the past to obscure his Internet activity. And although Sterlingov argues that he possessed two Swedish passports "to be able to vacation in both Israel and Arab countries," *id.*, at the motion hearing Sterlingov's counsel acknowledged that Sterlingov had never been to an Arab country.

The history and characteristics of the defendant, accordingly, likewise weigh in favor of pretrial detention—although perhaps less so than the first two factors considered above.

D. Danger to the Community

The final factor that the Court must consider is "the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release." 18 U.S.C. § 3142(g). In cases in which the government seeks to detain a defendant pretrial to ensure "the safety of any other person and the community," *id.* § 3142(e), "[c]onsideration of this factor encompasses much of the analysis set forth above, but it is broader in scope," requiring an "open-ended assessment of the 'seriousness' of the risk to public safety," *United States v. Taylor*, 289 F. Supp. 3d 55, 70 (D.D.C. 2018). Where, as here, the government instead argues that pretrial detention is necessary to "assure the appearance" of the defendant at future proceedings, 18 U.S.C. § 3142(e), the role of this factor is less clear, *see United States v. Amar*, 300 F. Supp. 3d 287, 292 (D.D.C. 2018) (ordering defendant detained pretrial due to flight risk without explicit consideration of danger to community posed by defendant); *United States v. Holguin*, 791 F. Supp. 2d 1082, 1093 (D.N.M. 2011) (ordering defendant detained pretrial due to flight risk despite separate finding that the government's evidence was insufficient that defendant was a danger to the community). The D.C. Circuit has, however, included this factor in its analysis when reviewing decisions predicated on flight risk, *see United States v. Vasquez-Benitez*, 919 F.3d 546, 551 (D.C. Cir. 2019), and so the Court will do the same here.

The government does not argue that Sterlingov's release would directly endanger the community, and the Court has before it no evidence even hinting that Sterlingov might be prone to violence. But the government's case does include evidence that Bitcoin Fog facilitated millions of dollars in transactions with darknet marketplaces like Silk Road and Agora, which are known to "primarily traffic in illegal narcotics and other illegal goods and services." Dkt. 1-1 at 4. And the government has offered evidence that Sterlingov operated Bitcoin Fog. *Id.* at 7. That unlawful activity, in turn, itself poses a "danger . . . the community," 18 U.S.C. § 3142(g). To be sure, this potential risk to the community is both indirect and theoretical. But, at the same time, the Court cannot discount the risk entirely. The Court, accordingly, concludes that the fourth factor, even if applicable, does not tip decisively against continued pretrial detention.

*   *   *

Because three of the four factors weigh in favor of pretrial detention, and because the fourth factor carries little weight in the present context, the Court concludes that no conditions or combination of conditions will reasonably assure the appearance of Sterlingov as required.

CONCLUSION

For the foregoing reasons, Defendant Roman Sterlingov's motion to revoke pretrial detention, Dkt. 17, is **DENIED**.

SO ORDERED.

/s/ Randolph D. Moss
RANDOLPH D. MOSS
United States District Judge

Date: November 10, 2021