UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**CRIMINAL NO. 23-cr-239-1 (CKK)**
	:	
ILYA LICHTENSTEIN,	:	
	:	
Defendant.	:	

GOVERNMENT'S MOTION FOR DOWNWARD DEPARTURE
AND MEMORANDUM IN AID OF SENTENCING

The United States of America, by and though the United States Attorney for the District of Columbia, respectfully submits its Memorandum in Aid of Sentencing. In light of the defendant's substantial assistance, the government moves pursuant to Section 5K1.1 of the U.S. Sentencing Guidelines for a downward departure from the advisory Guidelines range and recommends a sentence of 60 months at offense level 25. The government respectfully submits that such a sentence would adequately serve the interests of justice as codified in 18 U.S.C. § 3553(a). In support of this motion, and to assist the Court in fashioning an appropriate sentence, the government submits the following motion and a sealed supplement.

FACTUAL AND PROCEDURAL BACKGROUND

A. Introduction

As detailed in the Statement of Offense, in August 2016, Ilya Lichtenstein ("the defendant") hacked into a virtual currency exchange and stole approximately 120,000 bitcoin ("BTC"). Following the theft, the defendant devised a sophisticated plan to launder the funds, involving extensive layering of transactions, cryptocurrency mixers and non-compliant cryptocurrency exchanges, darknet markets, and bank accounts in the U.S. as well as overseas. The defendant enlisted the assistance of his wife, co-defendant Heather Rhiannon Morgan, to clean

the money. The defendant continued to conspire with Ms. Morgan to launder the funds until in or around February 2022, when the defendant and Ms. Morgan were arrested.

B. Factual Background

a. The Theft

Beginning in or around late winter and early spring of 2016, the defendant embarked on a scheme to steal money from Bitfinex, one of the largest virtual currency exchanges in operation at the time. The defendant conducted online research and reconnaissance to gather information about computer infrastructure used by Bitfinex. Through these efforts, and applying his significant technical skills, the defendant identified and compromised computer servers outside the United States which belonged to Bitfinex. Those servers did not have direct access to Bitfinex's cryptocurrency wallets; however, the defendant was able to use his access to those servers to compromise additional servers and subsequently defeat numerous security measures on Bitfinex's network.

The defendant eventually gained access to the keys, or credentials, used to authorize transactions involving virtual currencies held by Bitfinex. In or about August 2016, the defendant used his access to Bitfinex's keys to fraudulently authorize more than 2,000 transactions in which approximately 119,754 BTC was transferred from Bitfinex's wallets to a self-hosted virtual currency wallet (the "Bitfinex Hack Wallet") under the defendant's custody and control. At the time of the hack, the stolen virtual currency was valued at approximately $71 million.

b. The Money Laundering

For several months after the theft, the defendant left the stolen funds sitting dormant in the Bitfinex Hack Wallet. The defendant considered how transactions are traced on the blockchain

and formulated a detailed plan to launder the funds. The plan, which evolved over time, utilized multiple laundering techniques across a complex, multi-step laundering process.

Beginning in or around January 2017, the defendant began to move a portion of the stolen BTC out of the Bitcoin Hack Wallet in a series of small, complex transactions across multiple accounts and platforms. This shuffling, which created a voluminous number of transactions, was designed to conceal the path of the stolen BTC, making it difficult for law enforcement to trace the funds. Over the next several years, the defendant gradually withdrew funds totaling about 25,000 BTC from the Bitfinex Hack Wallet. He laundered those stolen funds using a variety of sophisticated means, including laundering through complex transactions, non-compliant virtual currency exchanges, darknet markets, and mixers and tumblers, including Bitcoin Fog, Helix, and ChipMixer. The defendant enlisted Ms. Morgan's help in cleaning the stolen funds.

To obscure his funds' ties to the Bitfinex hack, the defendant, at times with Ms. Morgan's assistance, employed numerous money laundering techniques, including, but not limited to: (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 amounts; (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 currency, in a practice known as "chain hopping"; and (6) using U.S.-based business accounts to legitimize activity.

The defendant and Ms. Morgan took the following steps in furtherance of the money laundering scheme:

i. Setting up numerous accounts at virtual currency exchanges and other financial institutions to stay below transaction thresholds that would require enhanced customer due diligence by financial institutions;

ii. Converting stolen funds into fiat currency through Russian and Ukrainian bank accounts and then withdrawing the laundered funds in the United States, including at U.S. ATMs;

iii. Converting stolen BTC into a virtual currency named Monero (XMR), which is an anonymity-enhancing virtual currency with a nontransparent blockchain, via virtual currency exchanges that did not require know-your-customer ("KYC") data upon registration;

iv. Using intermediate virtual currency wallets to avoid exchange-to-exchange transactions that would undermine the anonymity benefits of using Monero, darknet markets, and virtual currency mixing services, such as Bitcoin Fog, Helix, and ChipMixer;

v. Converting a portion of the stolen funds to Tether (USDT) and USDC tokens, which are both stablecoins pegged to the U.S. dollar, as a means of avoiding the price volatility associated with holding other virtual currencies, such as BTC, the price of which fluctuates daily;

vi. Using virtual currency exchanges with high sale limits and setting up multiple accounts at numerous virtual currency exchanges in order to launder large amounts stolen of funds;

vii. Using pre-existing, verified accounts purchased from illicit vendors offering profiles designed to defeat exchange anti-money laundering ("AML") controls;

viii. Using accounts at virtual currency exchanges and other financial institutions opened under the defendant's and Ms. Morgan's true names and/or the names of their businesses; and

ix. Converting a portion of the stolen funds into gold coins, which were further concealed by Ms. Morgan when she buried them at a location that has since been disclosed to law enforcement, which has recovered the precious metal assets in full.

c. The Defendant's False Statements and Deception to Financial Institutions

During the period from in or around August 2016 through in or around February 2022, the defendant and Ms. Morgan used false and fictitious identifying information to establish accounts, made false and fraudulent representations, and lied to and deceived virtual currency exchanges and other financial institutions that they used to launder the illegal proceeds of the 2016 hack of Bitfinex, including the following:

i. Between on or about August 22, 2016, and on or about April 20, 2017, the defendant established multiple accounts at a virtual currency exchange ("VCE 1"), using email addresses from an India-based email provider and in the names of third parties unrelated to the defendant.

ii. In or around February and March 2017, the defendant declined to respond to inquiries from VCE 1's employees requesting that the registered accountholders for seven of the accounts provide additional identifying information to verify their account ownership. As a result, VCE 1 froze the accounts.

iii. On or about February 28, 2017, in response to inquiries from employees from another

virtual currency exchange ("VCE 7"), the defendant falsely and fraudulently represented that he would be using his VCE 7 account to trade only his own virtual currency that he had acquired through his early investment in BTC.

iv. In or around February 2018, the defendant established an account at a U.S. financial institution ("USFI 5") for the defendant and Ms. Morgan's company, Endpass, and in doing so represented to USFI 5 that the primary payments into the account would be from software-as-a-service customer payments. In actuality, the defendant and Ms. Morgan used the account to launder the proceeds of the hack of Bitfinex.

v. On or about January 8, 2019, in response to a KYC verification email from a virtual currency exchange ("VCE 10"), the defendant wrote to representatives from VCE 10, falsely and fraudulently stating that he has "been investing in and mining [BTC] since 2013, so the source of funds would be those early crypto assets."

vi. On or about June 27, 2019, in response to an inquiry from a representative from VCE 7 about how her business (SalesFolk) interacted with virtual currency and how her new institutional account would be used, Ms. Morgan falsely and fraudulently responded, "SalesFolk has some B2B customers that pay with cryptocurrency," when in fact that was not the case. Ms. Morgan further responded, "Additionally, I also have some personal cryptocurrency of my own that I would like to sell to finance the development of some new software that we are beginning to build. Because the company is an LLC taxed as an S corp it has pass-through taxation and I am the sole owner. I was going to use some of my personal crypto to fund out new software projects."

vii. On or about July 2, 2019, Ms. Morgan further represented to VCE 7 the following

information about the source of her virtual currency deposits: "My boyfriend (now husband) gifted me cryptocurrency over several years (2014, 2015,), [sic] which have appreciated. I have been keeping them in cold storage." Those funds were in fact proceeds of the hack of Bitfinex.

At all times relevant to the conspiracies to which the defendant has pled guilty, VCE 1, VCE 7, VCE 10, and USFI 5 were financial institutions doing business in the United States, were subject to the Bank Secrecy Act, and were registered with the Financial Crimes Enforcement Network.

d. The Foreign Account Packages

As noted above, the defendant, at times with Ms. Morgan's assistance, converted stolen funds through the use of debit cards linked to foreign bank accounts. The foreign bank accounts were registered to Russian and Ukrainian money mules, who worked for brokers and who typically created the accounts in-person at the foreign banks. The accounts were then offered for sale by brokers on darknet markets and cybercriminal forums. The defendant acquired numerous accounts through such platforms. The purchased account packages generally each included a debit card, as well as identity document scans and the SIM cards associated with the phone used to establish the account. The defendant took trips with Ms. Morgan to Kazakhstan and Ukraine and had the packages delivered to him during those trips. The packages were typically shipped via a shipping service or handed off by a courier in a prearranged public meeting place, such as a train station. The defendant then sent BTC to Russian- and Eastern-European-based instant exchange platforms, which converted the BTC to fiat currency and deposited the corresponding fiat funds into the Russian and Ukrainian bank accounts. The defendant and Ms. Morgan would travel to ATMs in the United States and use the purchased debit cards to withdraw funds. The defendant and Ms.

Morgan would bring multiple cards per trip and used only one card per ATM to avoid suspicion.

e. The Defendant's Additional Relevant Conduct

In or around November 2021, the defendant and Ms. Morgan learned that records related to an account held in the defendant's name and used in furtherance of the conspiracies had been disclosed to U.S. law enforcement. The provider controlling the account failed to process a valid and timely extension of a non-disclosure order issued by the U.S. District Court for the District of Columbia and ultimately notified the defendant in violation of the court order. Upon receipt of the notice, the defendant and Ms. Morgan took steps to further conceal their activity. For example, the defendant deleted data from devices in the United States and abroad, and the defendant and Ms. Morgan threw a computing device down a garbage chute, when said computing device contained relevant, inculpatory evidence related to this criminal scheme.

C. Procedural History

In or around September 2020, the U.S. Attorney's Office for the District of Columbia, along with IRS-CI, FBI, and HSI, began an investigation into the 2016 Bitfinex hack. Between September 2020 and December 2021, the case team uncovered evidence indicating that the defendant and Ms. Morgan were involved in a conspiracy to launder funds stolen from Bitfinex.

In January 2022, IRS-CI, FBI, and HSI executed a search warrant at the defendant and Ms. Morgan's residence.

In late January and early February 2022, the case team uncovered evidence proving that the defendant and Ms. Morgan had access to the funds remaining in the Bitfinex Hacker Wallet (*i.e.*, most of the funds stolen from Bitfinex in 2016).

On or about February 7, 2022, the defendant and Ms. Morgan were charged by criminal complaint with violations of 18 U.S.C. § 1956(h) (Money Laundering Conspiracy) and 18 U.S.C.

§ 371 (Conspiracy to Defraud the United States). The defendant and Ms. Morgan were arrested on the complaint on or about February 8, 2022.

On or about August 3, 2023, the defendant pled guilty to one count of Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h).

The defendant's sentencing is scheduled for November 14, 2024.

SENTENCING GUIDELINES

A. Statutory Maximums and Mandatory Minimums

A violation of Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h) predicated on conspiracy to violate 18 U.S.C. § 1956(a)(1)(B)(i), carries a maximum sentence of 20 years of imprisonment; a fine of $500,000 or twice the value of the property involved in the transaction, pursuant to 18 U.S.C. § 1956(a)(1); a term of supervised release of not more than 3 years, pursuant to 18 U.S.C. § 3583(b)(2); mandatory restitution under 18 U.S.C. § 3663A; and an obligation to pay any applicable interest or penalties on fines and restitution not timely made.

B. Sentencing Guidelines Calculation

a. The Government's Guidelines Calculation

As calculated in the Plea Agreement, this offense level is calculated as follows:

§§ 2X1.1(a) & 2S1.1(a)(1)	Base offense level for wire fraud (§ 2B1.1(a)(2))	6
Specific offense characteristics for wire fraud:		
§ 2B1.1(b)(1)(M)	More than $65 million	+24
§ 2B1.1(b)(2)(A)(iii)	Substantial financial hardship to 1 victim	+2
§ 2B1.1(b)(10)(C)	Sophisticated means	+2
§ 2S1.1(b)(2)(B)	Convicted of § 1956	+2
§ 2S1.1(b)(3)	Sophisticated laundering	+2
§ 2X1.1(b)(2)	Incomplete conspiracy	-3
Total Offense Level:		**35**
§ 3E1.1	Acceptance of Responsibility	-3
Adjusted Offense Level:		**32**

The government agrees with the PSR (¶ 75) that the defendant has no criminal history points and falls within Criminal History Category I.

At offense level 32 and Criminal History Category I, the defendant's pre-departure Guidelines range would be **121-151 months of imprisonment**.

b. Areas of Disagreement with the PSR

Though the PSR's Guidelines calculations in many areas track the numbers set forth above, the PSR diverges from the parties' Guidelines calculation in several respects. These are addressed below:

1. Role Enhancement

The government objects to the +2 adjustment for the defendant's role in the offense. *See* PSR ¶ 66. The PSR contends that the defendant was an "organizer, leader, manager, or supervisor in any criminal activity. *Id.* The government does not believe an aggravating role adjustment under U.S.S.G. § 3B1.1(c) is necessary to account for the relative culpability of the defendant as compared to his co-conspirator, Heather Morgan, especially where Ms. Morgan is receiving a mitigating role adjustment under § 3B1.2. In a two-person conspiracy, there is very little difference between an average participant and a manager or organizer, and the additional aggravating role adjustment is unnecessary based on the facts of the case.

2. Incomplete Conspiracy

The government disagrees with the PSR's omission of the adjustment for an incomplete conspiracy available under **§ 2X1.1(b)(2)**. The general conspiracy Guideline, § 2X1.1, provides for a -3 adjustment "unless the defendant or a co-conspirator completed all the acts the conspirators believed necessary on their part for the successful completion of the substantive offense, or the

circumstances demonstrate that the conspirators were about to complete all such acts but for apprehension or interruption by some similar event beyond their control." U.S.S.G. § 2X1.1(b)(2).

As the Ninth Circuit has construed this adjustment, "unless the remaining steps to be taken in the commission of a crime are so insubstantial that the commission of the substantive offense is inevitable, barring an unforeseen occurrence that frustrates its completion, the conspirators are not about to complete the requisite acts and the defendant must be granted the three point reduction." *United States v. Martinez-Martinez*, 156 F.3d 936, 939 (9th Cir. 1998); *see also, e.g.*, *United States v. Susany*, 893 F.3d 364, 367 (6th Cir. 2018) (citing *Martinez-Martinez*); *United States v. Downing*, 297 F.3d 52, 62-63 (2d Cir. 2002) (same).

In the specific context of money laundering conspiracy, several courts have applied § 2X1.1(b)(2) to situations where defendants successfully laundered only a portion of a larger body of criminal proceeds. *See, e.g.*, *United States v. Khawaja*, 118 F.3d 1454 (11th Cir. 1997) (applying § 2X1.1(b)(2) where defendants conspired to launder $2 million but "only completed the acts necessary to launder $570,556"); *United States v. Puche*, 350 F.3d 1137 (11th Cir. 2003) (applying § 2X1.1(b)(2) where defendants conspired to launder $6 million but only completed laundering of $714,500). In *Khawaja*, for instance, the court explained that the defendants had not completed specific "crucial steps" necessary to engage in further transactions to launder the remaining funds: "the conspirators had not taken crucial steps (including for example, preparing falsified documentation, securing cashier's checks, or arranging meetings for the exchange) to launder the remaining balance of $2 million." 118 F.3d at 1458.

These authorities support application of § 2X1.1(b)(2) here. First, the defendant and Ms. Morgan engaged in a complex laundering scheme, requiring manual transactions (or writing scripts to automate transactions) to move the stolen cryptocurrency through, *inter alia*, multi-step peel

chains; darknet market accounts; Bitcoin mixers; cryptocurrency exchange accounts set up with false names and email addresses; and conversion of the funds from Bitcoin to other forms of cryptocurrency such as Monero, an anonymity-enhanced cryptocurrency. Second, at the time of their arrest, the defendant and Ms. Morgan had completed the laundering of only a portion of the criminal proceeds. To launder the remaining proceeds, they would have had to engage in additional, largely manual transactions. Under these facts, the government believes the defendants were not "about to" complete "all" the acts necessary for completion of the money laundering conspiracy.

The PSR takes the contrary position, relying on the provision in § 2X1.1 that states, "when an attempt, solicitation, or conspiracy is expressly covered by another offense guideline section, apply that guideline section." U.S.S.G. § 2X1.1(c)(1). This provision, however, refers to other guidelines that explicitly cover conspiracies, solicitations, or attempts as distinct from completed offenses. Thus, Application Note 1 identifies guidelines that "expressly cover" attempts, solicitations, or conspiracies, such as § 2A2.1 (Assault with Intent to Commit Murder; Attempted Murder); § 2D1.1 (Unlawful Manufacturing, Importing, Exporting, or Trafficking (Including Possession with Intent to Commit These Offenses); Attempt or Conspiracy); and § 2A1.5 (Conspiracy or Solicitation to Commit Murder). U.S.S.G. § 2X1.1, Application Note 1. Notably absent from the list in Application Note 1 is the money laundering guideline applicable in this case, § 2S1.1. That is because § 2S1.1 contains no separate adjustment for attempts, solicitations, or conspiracies—and therefore the guideline itself does not "expressly cover" conspiracies.

The PSR relies on *United States v. Grzegorczyk*, 800 F.3d 402 (7th Cir. 2015), but *Grzegorczyk* underscores the limited nature of the carve-out in § 2X1.1(c)(1). There, the defendant pled guilty to, *inter alia*, using interstate commerce facilities in the commission of murder-for-

hire, in violation of 18 U.S.C. § 1958(a). *Id.* at 404. The Seventh Circuit held that the defendant was properly sentenced under the guideline that expressly applies to the solicitation of murder for hire, § 2A1.5 (Conspiracy or Solicitation to Commit Murder), and not the incomplete conspiracy adjustment under § 2X1.1. The Seventh Circuit offered two rationales for its holding. First, § 2A1.5 "is listed in the Application Notes to § 2X1.1 among the specific offense Guidelines that expressly cover solicitation." *Id.* at 405-06 (citing Application Note 1 to U.S.S.G. § 2X1.1). Second, the solicitation guideline, § 2A1.5, "already accounts for instances where the acts necessary for the completion of the crime solicited have not occurred," through a cross-reference that imposes a higher offense level if the solicitation resulted in an attempt or completed murder. *Id.* at 406. Neither rationale cited in *Grzegorczyk* applies here: the money laundering guideline, § 2S1.1, is not listed in the Application Notes to § 2X1.1 as one of the guidelines that "expressly cover[s]" conspiracies; and § 2S1.1 does not distinguish between completed money laundering offenses and conspiracies. Accordingly, consistent with *Grzegorczyk*, the Court should apply the incomplete conspiracy adjustment here under § 2X1.1(b)(2).

Finally, the government also notes that the PSR for the defendant's co-defendant, Heather Morgan, agreed with the government that an incomplete conspiracy adjustment should be applied to her guideline calculation pursuant to § 2X1.1(b)(2). The government urges the Court to treat both co-conspirators consistently in applying § 2X1.1(b)(2).

3. Adjustment for Obstruction of Justice

The government objects to the applicability of the adjustment for obstruction to justice for the same reasons set out in the government's sentencing memorandum pertaining to Ms. Morgan, ECF No. 143 at 12-14, which are restated herein. The parties did not apply an adjustment for obstruction of justice in their Plea Agreement calculation. The PSR, however, applies a 2-level

enhancement pursuant to § 3C1.1. *See* PSR, ¶ 67. This enhancement is based on conduct outlined in the Statement of Offense in which the defendants deleted data from devices and threw a computing device containing relevant, inculpatory evidence down a garbage chute after being tipped off to the existence of the government's investigation. *See* ECF No. 100, ¶ 23.

As a preliminary matter, the government notes that the defendants' conduct did not ultimately hinder the investigation. The government acknowledges that the authority cited by the PSR, *United States v. Owens*, 308 F.3d 791 (7th Cir. 2002), holds that "*actual* prejudice to the government resulting from the defendant's conduct is not required." *Id.* at 794 (emphasis in original).

Most significantly to the applicability of the obstruction enhancement under § 3C1.1, the government would not have been aware of the defendants' actions[1] but for statements made by both defendants during their voluntary debriefings following arrest. The debriefings were governed by a standard proffer letter, which set forth that, barring specific carve-outs, "no statements made by or other information provided by your client during the voluntary debriefing(s) will be used directly against your client in any criminal proceeding." Section 1B1.8 provides the baseline rule for the use of such incriminating information in calculating a guidelines range, stating:

> Where a defendant agrees to cooperate with the government by providing information concerning unlawful activities of others, and as part of that cooperation agreement the government agrees that self-incriminating information provided pursuant to the agreement will not be used against the defendant, then *such information shall not be used in determining the applicable guideline range*, except to the extent provided in the agreement.

U.S.S.G. § 1B1.8(a) (emphasis added).

[1] The government had evidence that information was deleted from a server, but it likely would have been unable to prove that the deletion was an attempt at obstruction.

The plea agreement in this case included a waiver of the standard protections under U.S.S.G. § 1B1.8, but it is a waiver that may be exercised at the government's discretion:

> The Government and your client agree, in accordance with U.S.S.G. § 1B1.8, that *the Government* will be free to use against your client for any purposes at the sentencing in this case or any related criminal or civil proceedings, any self-incriminating information provided by your client pursuant to this Agreement or during the course of debriefings conducted in anticipation of this Agreement …

ECF No. 101 at 10 (emphasis added). Under the plain text terms of the plea agreement, the protections of 1B1.8 stay in place for sentencing unless "the Government" seeks to use the information. The government is not seeking to use the information in this manner here, so the baseline rule in § 1B1.8 remains in force. The government's intention and the parties' understanding is reflected in the agreed-upon guidelines calculation in the plea agreement, which omitted any obstruction enhancement.

The information regarding the defendants' actions was included in the sworn-to Statement of Offense, as the government felt it was important for the Court and others to be aware of the full scope of the defendants' relevant conduct. The Application Notes for § 1B1.8 envision precisely such a scenario, noting, "This provision *does not authorize the government to withhold information from the court* but provides that self-incriminating information obtained under a cooperation agreement is not to be used to determine the defendant's guideline range." U.S.S.G. §1B1.8 App. N. 1 (emphasis added). The Application Notes further observe that the re-presentation of the information outside of a debriefing setting does not invalidate the relevant protections:

> The guideline operates as a limitation on the use of such incriminating information in determining the applicable guideline range, and not merely as a restriction of the government's presentation of such information (*e.g.*, where the defendant, subsequent to having entered into a cooperation agreement, provides such information to the probation officer preparing the presentence report, *the use of such information remains protected by this section*).

U.S.S.G. § 1B1.8 App. N. 5 (emphasis added).

SENTENCING RECOMMENDATION

A. Sentencing Factors

In *United States v. Booker*, 543 U.S. 220 (2005), the Supreme Court held that the Sentencing Guidelines are no longer mandatory. However, the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions" and "should be the starting point and the initial benchmark" in determining a defendant's sentence. *United States v. Gall*, 552 U.S. 38, 46, 49 (2007). Accordingly, this Court "should begin all sentencing proceedings by correctly calculating the applicable Guidelines range." *Id.* at 49.

Next, the Court should consider all of the applicable factors set forth in 18 U.S.C. § 3553(a). *Id.* at 49-50. The Guidelines themselves are designed to calculate sentences in a way that implements the considerations relevant to sentencing as articulated in § 3553(a). *United States v. Rita*, 551 U.S. 338, 347-351 (2007). The § 3553(a) factors include, *inter alia*: (1) the nature and circumstances of the offense; (2) the history and characteristics of the defendant; (3) the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct and protect the public from further crimes of the defendant, and to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner; (4) the need to avoid unwarranted sentencing disparities among defendants with similar records who have been found guilty of similar conduct; and (5) the need to provide restitution to any victims of the offense. *See* 18 U.S.C. § 3553(a)(1)-(7).

a. The Nature and Circumstances of the Offense

The nature and circumstances of the defendant's offense are gravely serious. The defendant perpetrated what was at the time one of the largest thefts from a virtual currency exchange—the culmination of a pattern of increasingly serious criminal behavior, as described in further detail below. The defendant then engaged in an extraordinarily meticulous and complex laundering scheme spanning approximately five years, enlisting his wife and co-conspirator, Ms. Morgan, and laundering millions of dollars' worth of stolen funds.[2]

Neither the hack nor the laundering scheme was an impulsive decision. The defendant spent months attempting to gain access to Bitfinex's infrastructure and get the accesses and permissions he needed in order to orchestrate his hack. He and Ms. Morgan then devoted significant time over the subsequent five years—from January 2017 through their arrest in February 2022—trying to liquidate portions of the stolen funds in a manner that allowed them to profit from the defendant's theft without being detected and apprehended. Over half a decade, the defendant engaged in what IRS agents described as the most complicated money laundering techniques they had seen to date. He enlisted his wife's assistance and set up numerous accounts across the globe; converted the cryptocurrency to other forms of value; researched money laundering techniques used by other criminals and considered how to use and improve upon them; wrote customized scripts to move his funds; and concocted various false explanations for the source of funds which he provided to financial institutions. Even while on vacations with his wife,

[2] The two co-conspirators successfully laundered approximately 25,111 BTC out of the 119,754 BTC initially stolen from Bitfinex in or about August 2016. Because the laundering occurred through complex and varied transactions over five years, during which the price of Bitcoin fluctuated widely, it is difficult to assign contemporaneous values to the amount of stolen money successfully laundered. Even at 2016 prices, 25,111 BTC represents a sum of at least $14 million, while its value at the time of the defendants' arrest on February 8, 2022 would have been more than $1 billion.

the defendant was preoccupied with cleaning the dirty funds. He used family trips to Kazakhstan and Ukraine as opportunities to meet up with couriers delivering money mule account packages for Russian and Eastern European bank accounts, which he then smuggled back into the United States. The massive scale, extraordinary sophistication, and continuous and deliberate nature of the defendants' criminal actions weigh in favor of a strong sentence.

These actions, moreover, caused significant harm. The defendant's hack and theft caused serious solvency issues at Bitfinex. And the scope of his and Ms. Morgan's laundering conspiracy encompassed the entire 119,754 BTC stolen from Bitfinex, valued at approximately $71 million at the time of the theft. As the D.C. Circuit and other courts have recognized, the laundering of illegal proceeds represents a distinct injury to society—concealing and facilitating the underlying crimes and frustrating law enforcement's ability to detect illicit abuse of the financial system. *See United States v. Braxtonbrown-Smith*, 278 F.3d 1348, 1355 (D.C. Cir. 2002) ("'Section 2S1.1 measures the harm to society that the money laundering causes to law enforcement's efforts to detect the use and production of ill-gotten gains . . . .'") (quoting *United States v. Allen*, 76 F.3d 1348, 1369 (5th Cir. 1996); *United States v. Martin*, 320 F.3d 1223, 1227 (11th Cir. 2003) ("Unlike the 1998 Sentencing Guidelines for theft or fraud, which compute the offense level according to the 'loss' incurred by the victim, see U.S.S.G. §§ 2B1.1(b)(1), 2F1.1(b)(1), the 1998 Sentencing Guidelines for money laundering compute the base offense level according to the 'value of the funds,' U.S.S.G. § 2S1.1(b)(2). This is so because the harm from such a transaction does not generally fall upon an individual, but falls upon society in general. Each unlawful monetary transaction harms society by impeding law enforcement's efforts to track ill-gotten gains.") (cleaned up).

The PSR claims that the defendants "spent almost nothing of what funds were stolen from Bitfinex"—apparently repeating self-serving statements made by the defendant during his presentence interview. *See* PSR ¶ 58, p. 41. First, the defendants successfully laundered about 21 percent of the funds stolen from Bitfinex—approximately 25,111 BTC out of the 119,754 BTC initially stolen—valued at anywhere between $14 million (in 2016 prices) and $1 billion (in 2022 prices). They spent millions of dollars from this rapidly appreciating pot of stolen assets to fuel their luxurious lifestyle. Second, to the extent they had not spent *all* of the laundered funds by the time of their arrest, that was primarily a product of the defendant's meticulous attention to the laundering process and insistence on maintaining the utmost level of operational security. And finally, it is obvious that the defendants had no plans to return any of the stolen funds to Bitfinex. While the defendants have certainly cooperated with the government in recovering the residue of the stolen funds *following their arrests*, it was law enforcement intervention—not any sort of spontaneous remorse on the part of the defendants—that has facilitated those recoveries. The defendant should be held accountable for the full scope of his complex and extensive money laundering conspiracy.

b. The History and Characteristics of the Defendant

The defendant is a highly skilled computer expert with a history of entrepreneurship, as well as an unfortunate history of other uncharged cyber criminal activity.

The defendant overcame a challenging early childhood in Russia, but moved to the United States at a young age and benefitted from the support of family members. The defendant was entrepreneurial from an early age. In high school, the defendant ran a successful online computer recycling and refurbishing business. In college, he ran a digital marketing agency from his dorm room, the profits from which he used to help pay off his student loans. After graduation, he co-

founded a software company and, as CEO, grew the business to 30 employees. The defendant's business pursuits encountered challenges, but overall, he had a promising future working in as in the tech industry. His decision to use his skills for criminal ends is thus particularly disappointing, but it gives hope for continued successful rehabilitation.

The defendant has no official criminal history, but the theft from Bitfinex was not his first hack. Beginning as a juvenile, the defendant experimented with other hacking and financial fraud activity. In or around 2015, the defendant illicitly obtained and transferred a small amount of PayCoin, an alternative form of virtual currency. In or around sometime prior to 2016, the defendant acquired credentials to another virtual currency exchange's application programming interface (API) and stole approximately $200,000. And during his preparation for the theft from VICTIM VCE, the defendant gained access to VICTIM VCE's customer login credentials and used them to steal another estimated several hundred thousand dollars from accounts at yet another virtual currency exchange. In short, the defendant has exhibited a pattern of increasingly serious criminal activity, culminating in the instant hack and theft of more than $71 million dollars' worth of cryptocurrency from Bitfinex and an extraordinarily sophisticated and extensive money laundering conspiracy, into which the defendant eventually drew his wife and co-conspirator. And this pattern was interrupted only after the defendant and his wife were arrested in this case. This troubling patten weighs in favor of a significant sentence.

c. The Need for the Sentence Imposed To Reflect the Seriousness of the Offense, To Promote Respect for the Law, To Provide Just Punishment for the Offense, To Afford Adequate Deterrence to Criminal Conduct and Protect the Public from Further Crimes of the Defendant, and To Provide Needed Training and Treatment

1. Seriousness of Offense

As described further above, the defendant's criminal conduct was significant, sophisticated, and deliberate. A significant period of incarceration is needed to reflect the seriousness of the offense.

2. General Deterrence

A sentence of imprisonment is necessary in this case to afford adequate general deterrence to criminal conduct. *See* 18 U.S.C. § 3553(a)(2)(B). "Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expedited benefits of a crime and hence the punishment required to deter it." *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994). General deterrence is a "crucial factor in sentencing decisions for economic" crimes. *United States v. Morgan*, No. 13-6025, 635 F. App'x 423, 450 (10th Cir. Nov. 6, 2015) (unpublished). The legislative history of § 3553 documents Congress's emphasis on general deterrence in white-collar crime. *See* S. REP. 98-225, 76, 1984 U.S.C.C.A.N. 3182, 3259 (need to deter others is "particularly important in the area of white collar crime"). *See also United States v. Mueffelman*, 470 F.3d 33, 40 (1st Cir. 2006) (deterrence of white-collar crime is "of central concern to Congress"). "Because economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (internal quotations and citation omitted).

General deterrence should be an important consideration for the court when sentencing the defendant. Many criminals believe that they can outsmart law enforcement and get away with their crimes; that belief is particularly pernicious in the area of cyber and cryptocurrency-related crimes. Hacks and thefts are alarmingly frequent occurrences in the cryptocurrency ecosystem, resulting in billions of dollars of loss each year. Criminals engaging in a wide array of underlying illicit activity turn to cryptocurrency to help them profit from their crimes while concealing their involvement in the criminal activity. For years, the defendant was able to conceal his activity; his technical abilities and laundering skills were so advanced that he made it extremely difficult to tie anything back to him. Law enforcement was able to identify the defendant and recover the stolen assets only through great effort by highly skilled personnel committed to leaving no stone unturned. Such investigations are lengthy and resource-intensive, and the government lacks the personnel and resources needed to successfully investigate every complex scheme or major theft. A sentence of incarceration in this matter will send a needed message to other crypto criminals who might otherwise believe they can commit crimes with impunity.

The need for general deterrence is particularly acute when considering the sentence's perception by juveniles starting to head down a path similar to the defendant's. Unfortunately, the defendant fits the profile of many cyber criminal defendants that the government has encountered. Many of these individuals start out as young men who develop impressive technical expertise from an early age. As teens, they feel socially isolated and seek out community online. They are exposed to criminal activity in those online spaces, and the activity is normalized in a way that trivializes the impact on the victims. They begin dabbling in online crime as juveniles, and become emboldened by their success—both in perpetrating the crime, and in not getting caught. The criminal activity escalates, as they feel invincible and pursue new challenges. Anecdotally, self-

medication and abuse of ADHD medication often appear to fuel the activity in many cyber crime cases the government has prosecuted. The difficulty faced by law enforcement in detecting and prosecuting lower-level cyber crimes often leads to a sense of impunity among perpetrators, leading—as here—to a pattern of increasingly serious and harmful criminal activity. A strong sentence in this case will help to break this cycle.

While this need for general deterrence weighs strongly in favor of a sentence of further incarceration, it is also important for the United States to fairly and accurately acknowledge substantial assistance provided by individuals charged with this type of non-violent offense. The defendant took full responsibility for his actions almost immediately after his arrest. As discussed in the accompanying sealed filing, the defendant's assistance has benefitted numerous investigations. To the extent that the sentence in this matter will send a message to other cyber criminals, that message should include the significant benefits to early and fulsome cooperation with the government.

3. Specific Deterrence and Need To Protect the Public

The sentence imposed in this case should also be fashioned to provide specific deterrence to the defendant. The government recognizes and appreciates that the defendant committed the initial hack as a younger man while under the influence of substances he was abusing, and that his life and family circumstances have changed in that intervening time. Furthermore, the defendant's prompt acceptance of responsibility and significant assistance to the government suggests that the risk of recidivism is low. The government believes that the defendant will be able to use his considerable skillsets for legitimate ends, and hopes that he will make positive contributions to the cybersecurity and anti-money laundering industries following his sentence

However, it is significant that the defendant and Ms. Morgan's money laundering conspiracy was interrupted only because they were arrested and the remaining funds in the Bitfinex Hacker Wallet were seized by law enforcement. But for this intervention, the defendants' laundering activity likely would have continued indefinitely.

Further, if the defendant were to revert to criminal activity, the government has no illusions regarding the serious danger that he could pose. Bitfinex had extensive security protections in place to safeguard its digital assets. The defendant was nevertheless able to overcome them. Over the course of months, the defendant gained access to Bitfinex systems, pivoted from one system to another, and was able to get access to highly secured assets. He then proceeded to outwit the anti-money laundering controls at numerous financial institutions. He became one of the greatest money launderers that the government has encountered in the cryptocurrency space. He successfully avoided detection for years. If the defendant were to take what he has learned from this prosecution and incorporate it into a future money laundering scheme, he would be even better-equipped to conceal his activity while monetizing his crimes. The sentence in this case should serve as a strong reminder to the defendant that such a return to crime carries the risk of a serious punishment, sufficient to deter the defendant from returning to criminal activity.

4. Treatment

The defendant was abusing Adderall at the time of the offense, which may have contributed to the activity. The government recommends that any sentence imposed include the possibility for continued treatment, which the government understands the defendant is also seeking.

d. The Need To Avoid Unwarranted Sentence Disparities Among Defendants with Similar Records Who Have Been Found Guilty of Similar Conduct

"The best way to curtail 'unwarranted' disparities is to follow the Guidelines, which are designed to treat similar offenses and offenders similarly." *United States v. Otunyo*, 63 F.4th 948,

960 (D.C. Cir. 2023) (quoting *United States v. Bartlett*, 567 F.3d 901, 908 (7th Cir. 2009)); *see also Gall v. United States*, 552 U.S. 38, 52 (2007) ("As with the seriousness of the offense conduct, avoidance of unwarranted disparities was clearly considered by the Sentencing Commission when setting the Guidelines ranges. Since the District Judge correctly calculated and carefully reviewed the Guidelines range, he necessarily gave significant weight and consideration to the need to avoid unwarranted disparities."). A sentence within the Guidelines range is "presumptively reasonable." *United States v. Fry*, 851 F.3d 1329, 1333 (D.C. Cir. 2017).

The government is unaware of any factually analogous money laundering conspiracy or conspiracy to defraud cases involving the same elements as here, such as the massive scale and technical sophistication of the cryptocurrency laundering operation, on the one hand, and the defendants' acceptance of responsibility and decision to cooperate with law enforcement, on the other. The Court's primary consideration in avoiding unwarranted sentencing disparities should be to address the relative culpability between the defendant and his wife. Their different levels of culpability have been taken into account through their respective plea agreements and will be reflected in the government's sentencing allocution as to each.

e. The Need to Provide Restitution

The government requests that the Court order that the defendants return the cryptocurrencies seized by the government directly from the Bitfinex Hack Wallet—including approximately 94,643.29837084 BTC, 117,376.52651940 Bitcoin Cash (BCH), 117,376.58178024 Bitcoin Satoshi Vision (BSV), and 118,102.03258447 in Bitcoin Gold (BTG), collectively valued at more than $6 billion at current prices—as in-kind restitution to Bitfinex. This represents the return of lost property to the owner of that property and is consistent with the statutory text and purpose of the Mandatory Victim Restitution Act (MVRA), 18 U.S.C. § 3663A.

As described in further detail below, the government anticipates that Bitfinex and/or other claimants will likely have meritorious claims to the remaining seized assets in the third-party ancillary forfeiture proceeding following sentencing.

In proposing this remedy, the government is guided by several considerations outlined below.

1. Authority To Order Restitution

First, Bitfinex is not a "victim" for purposes of the MVRA for the specific offenses charged in this proceeding. The MVRA sets forth a mandatory restitution obligation that is specific to the offense or offenses of conviction. This limitation is apparent from the statutory text, which authorizes the Court to order restitution "when sentencing a defendant convicted of an offense defined in [18 U.S.C. § 3663A(c)" to "the victim *of the offense*"—that is, the victim of "the offense" for which the defendant was "convicted." 18 U.S.C. § 3663A(a)(1) (emphasis added). It is further confirmed by the definition of "victim" as "a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered." 18 U.S.C. § 3663A(a)(2). Consequently, "[c]ourt decisions reviewing awards of restitution to 'victims' under the . . . MVRA have generally required a direct nexus between the offense of conviction and the loss being remedied." *United States v. Randle*, 324 F.3d 550, 556 (5th Cir. 2003); *see also United States v. Benns*, 740 F.3d 370, 377 (5th Cir. 2014) ("[R]estitution to victims of the offense . . . can encompass only those losses that results directly from the offense for which the defendant was convicted."); *United States v. Lutz*, 237 Fed. App'x 849, 852 (4th Cir. 2007) ("[I]t is the 'offense of conviction,' not the 'relevant conduct,' that must be the cause of losses attributable as restitutionary liability") (quotation, citation omitted); *United States v. Murry*, 395 F.3d 712, 721 (7th Cir. 2005) ("[R]estitution may not be ordered for relevant conduct.").

Here, neither the defendant nor his co-defendant wife was convicted of the underlying wire fraud representing the hack and theft of BTC from Bitfinex. Instead, the defendant was convicted of Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h). This crime occurred *after* the hack of Bitfinex. Such subsequent conduct did not "directly and proximately" cause Bitfinex's losses, 18 U.S.C. § 3663(a)(2). Thus, because the defendant was not convicted of any offense that directly caused harm to Bitfinex, he cannot be ordered to provide restitution under § 3663A(a)(1). *See generally United States v. Hensley*, 91 F.3d 274, 276 (1st Cir. 1996) ("Federal courts possess no inherent authority to order restitution, and may do so only as explicitly empowered by statute.").

Second, however, the MVRA expands the Court's authority to order restitution to the extent it is agreed to by the parties in a plea agreement. *See* 18 U.S.C. § 3663A(a)(3) ("The court shall also order, if agreed to by the parties in a plea agreement, restitution to persons other than the victim of the offense."); *see Randle*, 324 F.3d at 556 (explaining that one of the situations in which the MVRA authorizes restitution is "if the parties so agreed in a plea agreement"). That is the case here, where the defendant agreed in the Plea Agreement: "Apart from [the] determination of mandatory restitution, [the defendant] agrees to pay restitution to Bitfinex in an amount to be determined at sentencing." ECF No. 96, at 10.

2. Determination of Voluntary Restitution Order

Where restitution is ordered pursuant to the parties' plea agreement, the Court has the discretion to issue an appropriate restitution order. *See United States v. Peterson*, 268 F.3d 533, 535 (7th Cir. 2001) (affirming restitution order issued pursuant to plea agreement in which amount was determined by the district court at sentencing, noting that the defendant "agreed to make restitution to all victims of his entire course of conduct, and agreed further that the district judge could make decisions that proved necessary to implement this choice").

At a minimum, the government believes such a restitution order should include the residue of the property that was stolen from Bitfinex in the 2016 hack. This is consistent with the provision in the MVRA which provides that "in the case of an offense resulting in damage to or loss or destruction of property of a victim of the offense," the Court should order the defendant to "return the property to the owner of the property or someone designated by the owner." 18 U.S.C. § 3663A(b)(1)(A). What constitutes "the property" under this provision is construed narrowly. *See Robers v. United States*, 572 U.S. 639, 640-41 (2014) (defining "any part of the property" in adjacent provision of the MVRA as "refer[ring] only to the specific property lost by a victim").

Here, the defendant stole approximately 119,754 BTC from Bitfinex. He initially transferred the 119,754 BTC into the Bitfinex Hack Wallet. He subsequently withdrew and laundered approximately 25,000 BTC from the Bitfinex Hack Wallet. When the government executed a seizure of the Bitfinex Hack Wallet on or about January 31, 2022, the wallet still contained approximately 94,643.29837084 BTC from the hack, plus the Bitcoin Cash, Bitcoin Satoshi Version, and Bitcoin Gold amounts generated from several hard forks in the interim. These amounts represent "the specific property lost" by Bitfinex as a result of the hack.

The other assets seized by the government (which are listed, in part, in the Plea Agreement and Consent Order of Forfeiture) represent property that the defendants laundered through a variety of complex and technologically sophisticated means, including laundering through extensive peel chain transactions, non-compliant virtual currency exchanges, darknet markets, and mixers and tumblers, as well as comingling in the defendants' business and personal accounts. Because of the complexity of the laundering transactions, these remaining assets cannot be characterized as "the specific property lost" by Bitfinex, *see Robers*, 572 U.S. at 640-41.

Given the very unique facts of this case, the government does not believe that the voluntary restitution order ordered pursuant to the parties' Plea Agreement should include an additional monetary restitution order. Bitfinex suffered a loss of approximately 119,754 BTC in 2016, and, at current market prices, that loss would be valued at more than $7.6 billion. The government is aware that the MVRA normally requires a monetary restitution order for "the greater of" the value of any lost property as of the date of loss *or* as of "the date of sentencing," less the value of any property returned to the victim. 18 U.S.C. § 3663A(b)(1)(B)(i)-(ii). Here, the value of the cryptocurrency seized directly from the Bitfinex Hack Wallet should comfortably exceed $6 billion—but that would still leave a gap of approximately $1.6 billion corresponding to the value of the missing 25,000 BTC, as valued "on the date of sentencing." *Id.*

It is unclear, however, whether § 3663A(b)(1)(B)(i)-(ii) applies of its own force in this context, where restitution is ordered *only* pursuant to the parties' agreement in their Plea Agreement. The government is concerned that, while the defendants have other seized assets that could partially bridge the gap, those assets will still fall short of $1.6 billion. Should the Court impose a monetary restitution order in addition to the in-kind return of the remaining stolen property, the defendants could be faced with a restitution obligation that exceeds their available assets (including seized assets) by hundreds of millions of dollars. Where the Court is ordering restitution to a party *other than* a party directly and proximately harmed by the offenses of conviction, the government is concerned that a restitution obligation for hundreds of millions of dollars beyond the defendants' available assets could raise constitutional questions under the Excessive Fines Clause of the Eighth Amendment.

Accordingly, because restitution is only authorized pursuant to the parties' Plea Agreement and § 3663A(a)(3), because Bitfinex will receive cryptocurrencies valued at more than $6 billion

under the government's proposal, and because Bitfinex and/or other claimants will likely have meritorious claims to the remaining assets in the third-party ancillary forfeiture proceeding, the government believes the proposed remedy is appropriate to compensate Bitfinex pursuant to the Plea Agreement.

3. Joint and Several Liability

The government requests that the defendant and Ms. Morgan be jointly and severally liable for any restitution obligation. *See United States v. Yalincak*, 30 F.4th 115, 122 (2d Cir. 2022) (noting that MVRA authorizes joint and several liability "although the MVRA does not use that term").

f. Additional Considerations Surrounding the Defendant's Cooperation

The defendant has not only taken responsibility for his criminal conduct by pleading guilty, but he has also provided substantial assistance to law enforcement, the details of which are discussed in a separate filing, and the Government's sentencing recommendation takes his efforts into account.

B. Forfeiture

1. Forfeiture of Specific Properties

In his Plea Agreement and the Consent Preliminary Order of Forfeiture entered at the time of the defendant's plea, the defendant agreed to the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to the Money Laundering Conspiracy alleged in Count One. As part of this, the defendant agreed to the forfeiture of the specific properties listed in Attachment A to the Consent Preliminary Order of Forfeiture, including the Bitcoin and other cryptocurrencies recovered from the Bitfinex Hack Wallet (approximately 94,643.29837084 BTC, 117,376.52651940 BCH, 117,376.58178024 BSV, and 118,102.03258447

BTG), as well as other cryptocurrency, gold coins, and U.S. dollar assets seized from the defendants and traceable to the illegal proceeds stolen from Bitfinex in 2016. The defendant also agreed to the entry of a forfeiture money judgment in the amount of $72,618,825.60 and that the net proceeds realized by the United States from the forfeiture of any specific properties will be credited toward the forfeiture money judgment. *See* ECF No. 104.

Since the entry of the Consent Preliminary Order of Forfeiture, the government has taken additional steps (with the cooperation of the defendants) to unwind certain cryptocurrency investments to make those assets available for forfeiture. The government seeks an amended Preliminary Order of Forfeiture to incorporate these additional specific properties subject to forfeiture. The government is filing a separate motion and proposed Amended Preliminary Order of Forfeiture addressing forfeiture for both defendants concurrent with this sentencing memorandum. *See* Fed. R. Crim. P. 32.2(b)(2)(B) ("Unless doing so is impractical, the court must enter the preliminary order sufficiently in advance of sentencing to allow the parties to suggest revisions or modifications before the order becomes final as to the defendant . . . .").

2. Potential Claimants Will Have Opportunity To Assert Claims Over Forfeited Properties During Third-Party Ancillary Proceeding

Entry of the Preliminary Order of Forfeiture at sentencing will extinguish any claim the defendants have in the specific properties subject to forfeiture. *See United States v. Petlechkov*, 72 F.3th 699, 705 (6th Cir. 2023) ("The first part of the process—which focuses on the defendant's interest in the property—ends with the entry of a preliminary forfeiture order. . . . The order then becomes final when the defendant is sentenced (or sooner, if the defendant consents). When the order becomes final, the defendant's interest in the property is extinguished, and the government receives 'clear title to the property that is the subject of the order of forfeiture.'") (quoting 21 U.S.C. § 853(n)(7)).

Following sentencing, third parties who intend to assert claims over the forfeited properties will have an opportunity to do so in the third-party ancillary proceeding, pursuant to Fed. R. Crim. P. 32.2(c) and 21 U.S.C. § 853(n). The government will "publish notice of the [forfeiture] order and send notice to any person who reasonably appears to be a potential claimant with standing to contest the forfeiture in the ancillary proceeding." Fed. R. Crim. P. 32.2(b)(6)(A). Third parties asserting ownership interest over the forfeited property will then have an opportunity to file claims and have those claims adjudicated by the Court:

> Once the court or jury finds that the property is subject to forfeiture, and the court enters a preliminary order of forfeiture in accordance with Rule 32.2(b)(2), the government may publish notice of the forfeiture to third parties and commence an ancillary proceeding. The burden of proof is on the third party to demonstrate that he falls within one of two categories of third party claimants described in § 853(n)(6). To succeed, third parties must prove by a preponderance of the evidence that either (1) they had an interest in the property at the time of the offense that is superior to the government's interest; or (2) they acquired the interest after the offense as a bona fide purchaser for value. If the third party meets the burden of proof, the court will amend the preliminary order of forfeiture. Once the third party hearings have been held, or time for filing third party claims has passed, the government has clear title to the property forfeited.

United States v. Wittig, 525 F. Supp. 2d 1281, 1287-88 (D. Kan. 2007) (citations omitted). The standard for a valid third-party claim is different from the definition of "victim" under the MVRA, as it has to do with the claimant's ownership interest in the property, *see* 21 U.S.C. § 853(n)(6)(A)-(B). Therefore, the government anticipates that one or more parties may be able to assert valid claims in the third-party ancillary proceeding regardless of whether they would be considered "victims" entitled to restitution under the MVRA.

3. Forfeiture Money Judgment

"If the government seeks a personal money judgment, the court must determine the amount of money that the defendant will be ordered to pay." Fed. R. Crim. P. 32.2(b)(1)(A). As then-U.S. District Judge Ketanji Brown Jackson explained in *United States v. Young*, 330 F. Supp. 3d

424 (2018), the purpose of a forfeiture money judgment is to ensure that "a convicted criminal defendant should not be able to evade the economic impact of criminal forfeiture by rendering the forfeitable property unavailable." *Id.* at 432. Money judgments are often used "when there is some known, forfeitable asset—*e.g.*, the proceeds of, or other property derived from the proceeds of, an established criminal offense—that the defendant should possess but that the government has not been able to recover because the defendant has made it unavailable." *Id.* at 433.

In this case, the government has seized specific properties with an approximate current market value of $7.6 billion, and it anticipates returning most if not all of those assets to Bitfinex and/or other potential owners through restitution and the third-party ancillary proceeding discussed above. The value of those specific properties will vastly exceed the $72,618,825.60 forfeiture money judgment contained in the original Consent Preliminary Order of Forfeiture.[3] Accordingly, the government believes the forfeiture money judgment will not be necessary to effectuate the forfeiture of the defendant's illegal proceeds or the return of the stolen assets to their rightful owners.

CONCLUSION

For the foregoing reasons, the information reflected in the PSR, and the record in this case, the United States respectfully requests that the defendant be sentenced to a period of 60 months of imprisonment to be followed by 3 years of supervised release, imposition of a restitution judgment

[3] While the Consent Preliminary Order of Forfeiture contains a provision crediting properties forfeited *to the United States* toward this money judgment, it does not provide a mechanism to credit properties returned to third parties through restitution or the third-party ancillary proceeding to the money judgment. *See* ECF No. 104, at 3-4.

described above, and entry of an Amended Preliminary Order of Forfeiture to be filed with the Court.

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
Special Assistant United States Attorney
Jolie F. Zimmerman, D.C. Bar No. 465110
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, DC 20530
(202) 353-0018 (Brown)
(202) 252-7220 (Zimmerman)
Christopher.Brown8@usdoj.gov
Jolie.Zimmerman@usdoj.gov

/s/ Jessica Peck

Jessica Peck, N.Y. Bar Number 5188248
C. Alden Pelker, Maryland Bar
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) 353-9455 (Peck)
(202) 616-5007 (Pelker)
Jessica.Peck@usdoj.gov
Catherine.Pelker@usdoj.gov