

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA :
 :
 v. : **CRIMINAL NO. 23-cr-239-2**
 :
HEATHER RHIANNON MORGAN, :
 :
 Defendant. :

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

The United States of America, by and through 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 18 months at offense level 14. 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, the defendant (Heather Rhiannon Morgan) was recruited into a money laundering conspiracy and a related conspiracy to defraud the government by her husband and co-defendant Ilya Lichtenstein (“Lichtenstein”), who, in August 2016 and without the defendant’s knowledge, hacked into a virtual currency exchange’s network and stole approximately 120,000 bitcoin (“BTC”). Sometime after the hack, but by no later than in or around early 2020, Lichtenstein told the defendant about the hack and theft. Acting under Lichtenstein’s

direction, the defendant assisted Lichtenstein in laundering proceeds from the hack and theft by, *inter alia*, allowing her personal and business accounts to be used to launder the stolen proceeds, making false statements to a virtual currency exchange about the origin of the funds, and purchasing gold coins with stolen funds and burying those gold coins at a secret location.

The defendant's conspiracies with Lichtenstein lasted from no later than in or around early 2020, through February 2022, when the defendant and Lichtenstein were arrested.

B. Factual Background

a. Overview of the Defendant's Criminal Conduct

In or around August 2016, Lichtenstein and the defendant were living together in San Francisco, California. At around that time, and unbeknownst to the defendant, Lichtenstein identified and compromised computer servers owned by Bitfinex, a large virtual currency exchange. Lichtenstein used his unauthorized access to Bitfinex's network to steal 119,754 BTC, valued at approximately \$71 million at the time of the hack.

Lichtenstein initially transferred the 119,754 BTC into a self-hosted virtual currency wallet under his control (the "Bitfinex Hack Wallet"). Over several years, Lichtenstein gradually withdrew funds totaling about 25,000 BTC from the Bitfinex Hack Wallet. He laundered those stolen funds using a variety of technologically sophisticated means, including laundering through complex transactions, non-compliant virtual currency exchanges, darknet markets, and mixers and tumblers, including Bitcoin Fog, Helix, and ChipMixer.

Following the hack, Lichtenstein enlisted the defendant's help in laundering the stolen funds. The defendant was initially unaware of the specific origin of Lichtenstein's proceeds, although she participated with Lichtenstein in efforts to conceal and obscure the source of the funds while knowing and understanding that the funds were the result of some unspecified

unlawful and fraudulent activity. Sometime after the hack, but by no later than in or around early 2020, Lichtenstein explicitly told the defendant that Lichtenstein was responsible for the 2016 hack of Bitfinex. The defendant joined the conspiracy with the intent of assisting Lichtenstein in laundering the stolen funds and later understood that in so doing she was conspiring to conceal his involvement in the previous hack of Bitfinex.

b. The Defendant's Involvement in the Money Laundering Conspiracies

The defendant and Lichtenstein took the following steps in furtherance of the money laundering scheme:

- i. Setting up numerous accounts at virtual currency exchanges and other U.S. financial institutions to stay below transaction thresholds that would require enhanced customer due diligence by financial institutions. The defendant, acting at Lichtenstein's direction, allowed her existing accounts to be used for the purpose of laundering the proceeds of the hack, and assisted Lichtenstein in creating new accounts for the purpose of laundering the proceeds of the hack;
- ii. Converting stolen funds into fiat currency through Russian and Ukrainian bank accounts and then withdrawing the laundered funds in the United States. At Lichtenstein's direction, the defendant withdrew the laundered proceeds at U.S.-based 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. During the course of the conspiracy, Lichtenstein notified the defendant regarding the existence of the digital wallet containing the laundered

Monero, and provided the defendant with the special code needed in case she had to access funds;

- 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 U.S. financial institutions opened under the defendant’s and Lichtenstein’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 the defendant 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 Virtual Currency Exchanges and Other U.S. Financial Institutions

During the period from in or around August 2016 through in or around February 2022, the defendant and Lichtenstein used false and fictitious identifying information to establish accounts, made false and fraudulent representations, and lied to and deceived virtual currency exchanges and other U.S. 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, Lichtenstein 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 Lichtenstein.
- ii. In or around February and March 2017, Lichtenstein 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”), Lichtenstein 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, Lichtenstein established an account at a U.S. financial institution (“USFI 5”) for the defendant and Lichtenstein’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 Lichtenstein 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”), Lichtenstein 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, the defendant falsely and fraudulently responded, “SalesFolk has some B2B customers that pay with cryptocurrency,” when in fact that was not the case. The defendant 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, the defendant 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 Defendant's Additional Relevant Conduct

In or around November 2021, the defendant and Lichtenstein learned that records related to an account held in Lichtenstein'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 Lichtenstein in violation of the court order. Upon receipt of the notice, the defendant and Lichtenstein took steps to further conceal their activity. For example, Lichtenstein deleted data from devices in the United States and abroad, and the defendant and Lichtenstein threw a computing device down a garbage chute, when said computing device contained relevant, inculpatory evidence related to this criminal scheme.

Additionally, on or about January 5, 2022, federal law enforcement agents from the Internal Revenue Service, Criminal Investigation ("IRS-CI"), the Federal Bureau of Investigation ("FBI"), and Homeland Security Investigation ("HSI") executed a search warrant at the defendant and Lichtenstein's home in New York, New York. While agents were executing this warrant, the defendant retrieved her cat, which was hiding under a bed. While kneeling next to the bed, the defendant grabbed her phone and began pushing the side button multiple times and swiped at the screen, in an apparent attempt to shut the phone off. A subsequent review of the phone by law enforcement indicated that the phone did not contain incriminating evidence that would have aided in the government's investigation or prosecution.

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 Lichtenstein 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 Lichtenstein's residence.

In late January and early February 2022, the case team uncovered evidence proving that Lichtenstein and the defendant 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 Lichtenstein 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 Lichtenstein 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. § 371 and § 1956(a)(1)(B)(i), and one count of Conspiracy To Defraud the United States, in violation of 18 U.S.C. § 371.

The defendant's sentencing is scheduled for November 15, 2024.

SENTENCING GUIDELINES

A. Statutory Maximums and Mandatory Minimums

Count Two: A violation of Money Laundering Conspiracy, in violation of 18 U.S.C. § 371 and § 1956(a)(1)(B)(i), carries a maximum sentence of 5 years of imprisonment; a fine of \$250,000 or twice the pecuniary gain or loss of the offense, pursuant to 18 U.S.C. § 3571(b)(2)-(3); 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.

Count Three: A violation of Conspiracy To Defraud the United States, in violation of 18 U.S.C. § 371, carries the same statutory penalties as above.

B. Sentencing Guidelines Calculation

a. The Government's Guidelines Calculation

The government agrees with the Final PSR (§ 71) that Counts Two and Three are grouped together pursuant to U.S.S.G. § 3D1.2(d) because the offense levels are determined largely on the basis of the total amount of harm or loss and the two relevant Guidelines provisions (§ 2C1.1 and § 2S1.1) are specifically listed under § 3D1.2(d).

Thus, the prevailing guideline is that for Count Two, Money Laundering Conspiracy, in violation of 18 U.S.C. § 371 and § 1956(a)(1)(B)(i). 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)	Substantial financial hardship to 1 victim	+2
§ 2B1.1(b)(10)	Sophisticated means	+2
§ 2X1.1(b)(2)	Incomplete conspiracy	-3
§ 3B1.2	Minor Role	-2
Total Offense Level:		29
§ 3E1.1	Acceptance of Responsibility	-3
Adjusted Offense Level:		26

The government agrees with the PSR (§ 84) that the defendant has no criminal history points and falls within Criminal History Category I.

Subsequent to the entry of the defendant's guilty plea on August 3, 2023, the U.S. Sentencing Commission amended the Guidelines, effective November 1, 2023, to create the new zero-point offender adjustment under § 4C1.1. If a defendant receives zero criminal history points and meets other eligibility criteria, she may be eligible for a 2-point reduction in offense level

under § 4C1.1. Although the defendant entered her plea prior to the amendment, the general rule is that the Court should apply the version of the Guidelines in effect at the time of sentencing. *United States v. Gary*, 291 F.3d 30, 36 (D.C. Cir. 2002); 18 U.S.C. § 3553(a)(4)(A). Accordingly, the government agrees with the PSR (¶ 80) that the defendant’s offense level should be reduced by an additional 2 points:¹

§§ 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)	Substantial financial hardship to 1 victim	+2
§ 2B1.1(b)(10)	Sophisticated means	+2
§ 2X1.1(b)(2)	Incomplete conspiracy	-3
§ 3B1.2	Minor Role	-2
	Total Offense Level:	29
§ 3E1.1	Acceptance of Responsibility	-3
§ 4C1.1	Zero-Point Offender	-2
	New Adjusted Offense Level:	24

At offense level 24 and Criminal History Category I, the defendant’s pre-departure Guidelines range would be **51-63 months of imprisonment**.

b. Areas of Disagreement with the PSR

The PSR diverges from the parties’ Guidelines calculation in several respects. These are addressed below:

Calculation of base offense level for money laundering: The parties calculated the base offense level for the defendant’s money laundering offense pursuant to the first prong of § 2S1.1,

¹ One of the criteria for the zero-point offender adjustment is that “the defendant did not personally cause substantial financial hardship,” U.S.S.G. § 4C1.1(a)(6). The government does not believe there is any contradiction between this provision and holding the defendant responsible, pursuant to § 2S1.1(a)(1) and § 1B1.1(b)(2)(A), for conduct that “resulted in substantial financial hardship to one or more victims.” The “substantial financial hardship” specific offense characteristic is applicable to the defendant through principles of relevant conduct, because she acted as an accessory after the fact to Lichtenstein’s wire fraud. However, she did not “*personally* cause” the substantial financial hardship within the meaning of § 4C1.1(a)(6) (emphasis added).

subsection (a)(1). Subsection (a)(1) directs the Court to calculate “[t]he offense level for the underlying offense from which the laundered funds were derived”—here, wire fraud, calculated pursuant to § 2B1.1. As a result, the parties’ Guidelines calculation includes the base offense level and specific offense characteristics (including violation amount, substantial financial hardship to at least one victim, and sophisticated means) for the underlying wire fraud offense representing the hack of Bitfinex.

Subsection (a)(1) usually applies to self-launderers or “direct launderers,” who both commit the underlying offense and launder the resulting illegal proceeds. However, subsection (a)(1) is not limited to those who personally commit the underlying offense. It also applies to any defendant who “would be accountable for the underlying offense” as relevant conduct. U.S.S.G. § 2S1.1(a)(1). Relevant conduct includes “all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused by the defendant.” U.S.S.G. § 1B1.3(a)(1)(A).

Here, the defendant did not commit or participate in the hack of Bitfinex in 2016. However, she fits comfortably within the definition of an accessory after the fact because she became aware that Lichtenstein committed the 2016 hack and then actively participated in the laundering activity for the purpose of protecting him from detection and arrest, *see* 18 U.S.C. § 3 (“Whoever, knowing that an offense against the United States has been committed, receives, relieves, comforts or assists the offender in order to hinder or prevent his apprehension, trial or punishment, is an accessory after the fact.”). Because she is an accessory after the fact, she is criminally responsible for the hacking activity under § 1B1.3. *See* Application Note 9 to U.S.S.G. § 1B1.3 (“In the case of . . . accessory after the fact, the conduct for which the defendant is accountable includes all conduct relevant to determining the offense level for the underlying offense that was known, or reasonably

should have been known, by the defendant.”). Therefore, the appropriate starting point in calculating the defendant’s base offense level is § 2S1.1(a)(1).

The PSR takes a different approach, arguing that the base offense level should be calculated pursuant to subsection (a)(2) of § 2S1.1. PSR at 43-44. Subsection (a)(2) is generally applicable to cases in which a defendant acts as a “third-party launderer” but was not involved in the specified unlawful activity that generated the illegal proceeds. *See United States v. Campbell*, 764 F.3d 874, 877 (8th Cir. 2014) (“[T]he Guidelines distinguish between direct money launderers in § 2S1.1(a)(1) and third-party launderers in § 2S1.1(a)(2). A direct launderer commits the crime that produces the illicit funds. A third-party launderer has no involvement in the underlying offense but only launders money that the underlying offense generated.”) (citations omitted).

The government agrees that the defendant did not personally *commit* the underlying wire fraud offense. But that is not the end of the analysis because subsection (a)(1) applies more broadly and includes, among others, defendants who are criminally responsible because they acted as an accessory after the fact. U.S.S.G. § 2S1.1(a)(1); Application Note 9 to U.S.S.G. § 1B1.3. While it is true the defendant did not participate in the original hack of Bitfinex, she was not a total stranger to the underlying offense: she participated in laundering the proceeds of the hack with the intent to protect her husband, Lichtenstein, from being arrested and prosecuted for it. She was therefore not acting as an arms-length, third-party launderer, but as one who assumed some responsibility for the hack by taking active measures to assist the perpetrator “in order to hinder or prevent his apprehension, trial or punishment,” 18 U.S.C. § 3. Accordingly, her base offense level is appropriately calculated pursuant to subsection (a)(1) of § 2S1.1.

Adjustment for obstruction of justice: 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, ¶ 64. 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’ actions² 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).

² 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, and to afford adequate deterrence to criminal conduct and protect the public from further crimes of the defendant; (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 defendant was recruited into two related conspiracies by her husband and co-defendant, Lichtenstein. The defendant and Lichtenstein’s criminal conduct was sophisticated,

involving what IRS agents described as the most complicated money laundering techniques they had seen to date. For example, Lichtenstein, at times with the defendant's assistance, (1) used accounts set up with fictitious identities, some of which were set up by the defendant at Lichtenstein's direction; (2) moved 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) utilized computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; (4) layered the stolen funds by depositing them into accounts at a variety of virtual currency exchanges and darknet markets and then withdrawing the funds, which obscures the trail of the transaction history by breaking up the fund flow; (5) converted the stolen BTC to other forms of virtual currency, including anonymity-enhanced virtual currency, in a practice known as "chain hopping"; and (6) used U.S.-based business accounts to legitimize activity.

As part of the conspiracies, the defendant and Lichtenstein laundered millions of dollars in proceeds from the Bitfinex hack. The planning involved was elaborate. Although the defendant was initially unaware of the specific origin of Lichtenstein's proceeds, she participated with Lichtenstein to conceal and obscure the source of the funds while knowing that the funds were the result of some unspecified unlawful and fraudulent activity. Then, no later than in or around early 2020, Lichtenstein explicitly told the defendant that Lichtenstein was responsible for the 2016 hack of Bitfinex. From there, the defendant made a conscious decision to engage in specific criminal activity, helping her husband launder millions in stolen funds for their personal gain. And it was not a momentary lapse or impulsive decision: the defendant consciously participated in the money laundering conspiracy and conspiracy to defraud over the course of years. The massive

scale, extraordinary sophistication, and continuous and deliberate nature of the defendants' criminal actions weigh in favor of a strong sentence.

That said, and without diminishing the seriousness of her offenses, the defendant did not act alone. Lichtenstein masterminded and orchestrated the Bitfinex hack without telling the defendant. He also initially solicited the defendant's assistance without explaining exactly what he was doing. The defendant was certainly a willing participant and bears full responsibility for her actions, but she was a lower-level participant.

Finally, while the defendant's actions contributed to significant financial harm and the defendant and her husband enjoyed a lifestyle fueled by millions of dollars in stolen funds, she herself spent a small fraction of the criminal profits.

b. The History and Characteristics of the Defendant

The defendant has no criminal history. She is a college graduate and has worked for most of her adult life, including as an entrepreneur and writer. She established and operated her own small business and presented as an intelligent, resourceful individual. Prior to and other than her involvement in her husband's scheme, she used her professional skillset for legitimate ends and had a record of being a productive member of society. Since her arrest, she has resumed working and maintains employment to support herself financially. This history makes it all the more troubling that the defendant so readily turned to criminal activity, but on balance, the defendant's history and characteristics weigh in favor of leniency.

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, and To Afford Adequate Deterrence to Criminal Conduct and Protect the Public from Further Crimes of the Defendant

The defendant's criminal conduct was serious, sophisticated, and deliberate. 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"). "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).

However, specific deterrence is not a significant factor here given the defendant's early acceptance of responsibility and her decision to cooperate with the government, her lack of any criminal history, and her continued efforts to maintain productive employment since her arrest. The defendant's recidivism risk is low. The defendant appeared to be a law-abiding and productive member of society prior to becoming involved in her husband's laundering scheme. The defendant was not involved in the original hack and theft and remained unaware of it during the initial years of her marriage. She was in some ways thrust into the middle of a serious criminal scheme without her initial consent, and undoubtedly felt compelled to support it out of a sense of loyalty to her husband and desire to preserve their life together. That does negate the seriousness of her conduct, as she did ultimately join her husband's conspiracy and use her own skillset to aid and enhance his criminal endeavors. However, it appears highly unlikely that the defendant would have sought out or otherwise become involved in criminal activity had it not been for her husband's actions. The defendant's criminal activity was thus the result of unique circumstances that are unlikely to re-materialize—and, even if they did, the defendant appears genuinely remorseful and appreciative of the serious consequences of her actions and those of her husband, such that the government believes that she would be unlikely to re-offend.

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 her husband. 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 her co-defendant husband 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. § 371 and § 1956(a)(1)(B)(i), and Conspiracy To Defraud the United States, in violation of 18 U.S.C. § 371. Both of these crimes 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, she 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. 101, 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's husband, Lichtenstein, 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 Robbers*, 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 Lichtenstein 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 her criminal conduct by pleading guilty, but she 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 her efforts into account.

B. Forfeiture

1. Forfeiture of Specific Properties

In her 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 Two. 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 anticipates filing a separate motion and proposed Amended Preliminary Order of Forfeiture addressing forfeiture for both defendants at the time it submits its sentencing memorandum for defendant Ilya Lichtenstein. *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.3d 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 18 months of imprisonment to be followed by 3 years of supervised release, imposition of a restitution judgment described above, and entry of an Amended Preliminary Order of Forfeiture to be filed with the Court.

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.

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