UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA **– v. –** **JAMES ZHONG,** **Defendant.**	**22 Cr. 606 (PGG)**

THE GOVERNMENT'S SENTENCING MEMORANDUM
REGARDING DEFENDANT JAMES ZHONG

DAMIAN WILLIAMS
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

David R. Felton
Assistant United States Attorney
- *Of Counsel* -

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA **– v. –** **JAMES ZHONG,** **Defendant.**	**22 Cr. 606 (PGG)**

GOVERNMENT'S SENTENCING MEMORANDUM
REGARDING DEFENDANT JAMES ZHONG

The Government respectfully submits this memorandum in advance of the sentencing of defendant James Zhong, currently scheduled for Friday, April 14, 2023, at 3:00 p.m. As set forth in the Presentence Investigation Report ("PSR") and in the parties' plea agreement, the defendant's stipulated Guidelines range is 27 to 33 months' imprisonment (the "Stipulated Guidelines Range"). The Probation Office recommends a below-Guidelines sentence of 24 months' imprisonment.

The Government agrees with defense counsel that there are significant mitigating factors here, including Zhong's youth and autism and, chief among them, his assistance to law enforcement in accessing what was then, in 2022, multiple billions of dollars of crime proceeds and, today, remains nearly $1.5 billion dollars of crime proceeds.[1] These factors—which counsel presented to the Government, and led the Government to exercise its discretion to allow Zhong to plead guilty to wire fraud, which has a Guidelines range of 27 to 33 months' imprisonment, as

[1] In total from the Zhong investigation, the Government has obtained final orders of forfeiture for approximately 51,680.32473733 Bitcoin, valued at over $3.4 billion at the time of seizure; Zhong's 80% interest in RE&D Investments, LLC, a Memphis-based company with substantial real estate holdings; $661,900 in cash seized from Zhong's home; and various metals also seized from Zhong's home. As of March 30, 2023, the Bitcoin alone is valued at $1.48 billion.

opposed to money laundering offenses with far steeper sentencing Guidelines—should be considered by the Court in fashioning a sentence. Thus, the Government agrees that a below-Guidelines sentence, and a sentence even below the 24 months recommended by Probation, would be appropriate. Nevertheless, the Government respectfully submits that an incarceratory sentence is necessary in this case, in light of the seriousness of Zhong's nearly decade-long conduct, the sophistication of his post-theft actions to conceal his identity and the source of the crime proceeds, and to avoid signaling to Zhong and others that such conduct presents little risk beyond simply being asked to pay back whatever remains of the crime proceeds. Indeed, in the 51 months before law enforcement's overt search of Zhong's residences, Zhong dissipated approximately $16 million of crime proceeds, spending lavishly on real estate investments, luxury products, travel, hotels, nightclubs, and other expenses. Based on the price of Bitcoin the day of the Search, Zhong's dissipated proceeds would have been valued at over $142 million. Based on the price of Bitcoin today, the dissipated proceeds would have been valued at over $61 million. Put simply, this conduct warrants imprisonment.

For these reasons, and the reasons explained below, the Government respectfully submits that a sentence of imprisonment, but below the Stipulated Guidelines Range and below Probation's recommended sentence of 24 months, would be sufficient but not greater than necessary to meet the goals of sentencing in this case.

I. BACKGROUND

A. Offense Conduct

Silk Road Background

Silk Road was an online "darknet" black market created and operated by Ross William Ulbricht. In operation from approximately 2011 until 2013, Silk Road was used by many drug dealers and other unlawful vendors to distribute massive quantities of illegal drugs and other illicit goods and services (such as illegal computer hacking services, forged identity documents, and murder-for-hire or "hitman" services, among other things) to buyers around the world, and to launder all funds passing through Silk Road. PSR ¶ 11.

Bitcoin was the only form of payment accepted on Silk Road. *Id.* ¶ 13. Silk Road's payment system essentially consisted of a Bitcoin "bank" internal to the marketplace, where every user had to hold an account in order to conduct transactions on Silk Road. Specifically, every Silk Road user had at least one Silk Road Bitcoin address associated with the user's Silk Road account. These addresses were stored on wallets maintained on servers controlled by Silk Road. *Id.* ¶ 14. In order to make purchases on the Silk Road marketplace, the user first had to obtain Bitcoin and send it to a Bitcoin address associated with the user's Silk Road account. *Id.* ¶ 15.

After funding the user's account, that user could then make purchases from Silk Road vendors. When the user purchased an item on Silk Road, the Bitcoin needed for the purchase was held in escrow by Silk Road pending completion of the transaction. *Id.* ¶ 16. The user's Bitcoin was then transferred to the Silk Road Bitcoin address of the vendor involved in the transaction. The vendor could then withdraw Bitcoin from the vendor's Silk Road Bitcoin address by requesting that Silk Road withdraw the Bitcoin to a different Bitcoin address, outside of Silk Road, such as the address of a Bitcoin exchange, which Silk Road would then process. That exchange could then, upon the vendor's request, exchange the Bitcoin for fiat currency or an alternative form of digital currency. *Id.* ¶ 17.

Silk Road charged a commission for every purchase conducted by its users. *Id.* ¶ 18. Ulbricht carefully conceived of Silk Road's business model to facilitate anonymous illegal transactions beyond the reach of law enforcement, including by hosting the site on the Tor network, which hides the identities of its users and their IP addresses, and by requiring vendors and customers to do business in Bitcoin. *Id.* ¶ 19. Further, during its operation, Silk Road made use of a so-called "tumbler" to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Bitcoin blockchain. As described in the Silk Road "wiki" page, Silk Road's tumbler sent "payments through a complex, semi-random series of dummy transactions . . . making it nearly impossible to link your payment with any coins leaving the site." By Ulbricht's design, this made it challenging to use the Bitcoin blockchain to follow the money trail involved in a given transaction, even where the buyer and vendor Bitcoin addresses were both known. *Id.* ¶ 20.

During the course of the Silk Road investigation, law enforcement located a number of computer servers associated with the operation of Silk Road (the "Silk Road Servers"). The Silk Road Servers include computer databases which contained records for transactions which occurred on Silk Road during the course of its operation. The transactional database included detailed information regarding each transaction, including the category of product that was sold, the purchase price, both in Bitcoin and in U.S. dollars, and the commission taken by Silk Road, also in both Bitcoin and U.S. dollars. *Id.* ¶ 21.

Between February 2, 2011, and October 2, 2013, approximately 1.5 million transactions occurred over Silk Road, involving approximately 9.9 million Bitcoin, which generated commissions of approximately 640,000 Bitcoin for Silk Road. The vast majority of transactions were for illegal narcotics. *Id.* ¶ 22. The data indicated a worldwide geographic scope of countries where vendors and buyers were located. *Id.* ¶ 23.

Following Ulbricht's trial conviction in this District, on May 29, 2015, he was sentenced principally to the recommended Guidelines range of life imprisonment. *See generally United States v. Ross Ulbricht*, S1 14 Cr. 68 (LGS), May 29, 2015 Sentencing Transcript ("Sentencing Tr."). With respect to forfeiture, at Ulbricht's 2015 sentencing, the district court concluded that "*all funds* passing through Silk Road's Bitcoin-based payment system were involved in the money laundering offense in Count Seven. The Bitcoin-based system promoted and facilitated illegal transactions on Silk Road and concealed the proceeds of those transactions. It also concealed the identities of and locations of users." Sentencing Tr. at 92:15-21 (emphasis added). Based on evidence that it described as "clear," the Court found, "by far more than a preponderance of the evidence," that Ulbricht was "liable for *all the funds* that passed through Silk Road *regardless of*

whether he personally retained them." *Id.* at 92:22-93:2 (emphasis added). Thus, as the district court found at sentencing, all of the approximately 9.9 million in Bitcoin that passed through Silk Road's Bitcoin-based payment system were directly forfeitable proceeds of Ulbricht's money laundering count of conviction. At the time, the exact whereabouts of many of these Bitcoin were unknown to the Government; they already had been withdrawn from Silk Road by Silk Road vendors and customers.

The Investigation Pre-Search

Background. In 2019, the Government and IRS-Criminal Investigation ("IRS-CI") began investigating the whereabouts of approximately 53,500 directly forfeitable Bitcoin that was involved in or is traceable to Ulbricht's crimes. Specifically, the Government began investigating a September 2012 scheme to defraud Silk Road of at least approximately 50,000 Bitcoin from Silk Road's Bitcoin-based payment system and subsequent efforts to launder this Silk Road Bitcoin. PSR ¶¶ 24, 25.

In reviewing images of the Silk Road Servers, IRS-CI analyzed computer databases which contained detailed Silk Road transaction records. The Silk Road Servers included the following information: accounting ledger of all user activity, deposits, and withdrawals; blockchain information about deposits and withdrawals, including which Silk Road addresses belong to which users; Bitcoin address information; Bitcoin transaction information; vendor/buyer disputes and resolutions; error log; gift codes; internal transfers; private messages between Silk Road users; shipping information; user account information, including account creation information; user feedback; transaction history, including user purchases; user favorites; vendor items for sale; and word filters. The Silk Road Servers transactional database included detailed information regarding

each transaction, including the category of product that was sold, the purchase price, both in Bitcoin and in U.S. dollars, and the commission taken by Silk Road, also in both Bitcoin and U.S. dollars. *Id.* ¶¶ 26, 27.

September 2012 Wire Fraud. During this review, IRS-CI learned that over a period of a few days in September 2012, Zhong created a number of user accounts (the "Fraud Accounts") on the Silk Road dark-web internet marketplace. Zhong then used these accounts to exploit a vulnerability in Silk Road's Bitcoin payment processing system. Some of these accounts, unlike the majority of the accounts, did not have a basic account profile or an identifiable username, such as Zhong's account with Silk Road UserID "2c0eed0345." Among the accounts created by Zhong with an identifiable username were: "thetormentor," "suxor," "dubba," "gribs," "s1lky," and "imsh." *Id.* ¶ 28.

Zhong created about nine user accounts, and in over 140 transactions occurring in a few days, Zhong transferred at least 50,000 Bitcoin from Silk Road's Bitcoin addresses into Zhong's own addresses, without ever providing any goods or services in return. Zhong thereafter moved these Bitcoin out of Silk Road, and, in a matter of days, consolidated them into two high-value amounts—one consisting of approximately 40,000 Bitcoin, and one consisting of approximately 10,000 Bitcoin. At the time of Zhong's fraud, all of these 50,000 Bitcoin had passed through Silk Road's Bitcoin-based payment system. *Id.* ¶ 29. During this period, Silk Road's servers were located in Iceland and Pennsylvania, while Zhong executed the scheme in Athens, Georgia. In contemporaneous posts on a Bitcoin message board from 2012, Zhong observed that Silk Road stored about 50,000 Bitcoin at a time, the very quantity that he unlawfully obtained during the course of his fraud scheme. *Id.* ¶ 42.

Zhong funded the Silk Road addresses associated with the Fraud Accounts with an initial deposit of between 200 and 2,000 Bitcoin per address. After Zhong made the initial deposit, Zhong then quickly executed a series of withdrawals. Due to a flaw in Silk Road's payment processing system, Zhong was able to exploit the withdrawal processing flaw and withdraw many times more Bitcoin out of Silk Road's addresses than Zhong had deposited in Zhong's own addresses in the first instance. *Id.* ¶ 30.

For example, on September 19, 2012, Zhong, using the Fraud Account associated with username "thetormentor," deposited 500 Bitcoin into one of that account's Silk Road Bitcoin addresses. Less than five seconds after making the initial deposit, "thetormentor" executed five withdrawals of 500 Bitcoin in rapid succession—*i.e.*, within the same second—resulting in a net gain of 2,000 Bitcoin. Within the next 24 minutes, "thetormentor" deposited another 500 Bitcoin into the account's Silk Road Bitcoin address. Within 19 minutes after making that deposit, "thetormentor" again executed three withdrawals of 500 Bitcoin—again, within the same second—which resulted in a net gain of 1,000 Bitcoin. In this manner, "thetormentor" successfully obtained 3,000 Bitcoin in total out of Silk Road on a single day. *Id.* ¶ 31.

As another example, on September 20, 2012, Zhong, using the account "gribs," made an initial deposit of 350 Bitcoin, and a few moments later, executed a series of three withdrawals of 350 Bitcoin each, resulting in a net gain of 700 Bitcoin. *Id.* ¶ 32. Thereafter, Zhong, using the account with Silk Road UserID "2c0eed0345," made an initial deposit of 2,000 Bitcoin, then executed a series of eight withdrawals of 2,000 Bitcoin each, all of which occurred in rapid succession, resulting in a net gain of 14,000 Bitcoin. *Id.* ¶ 33. On September 24, 2012, Zhong, using the account "dubba," made approximately one deposit as compared to over 50 Bitcoin

withdrawals from Silk Road, resulting in a net gain, before the account ceased its activity. In this fashion, Zhong using each of the Fraud Accounts, netted approximately 50,000 Bitcoin that he moved out of Silk Road in just a few days. *Id.* ¶ 34.

By September 24, 2012, Zhong had consolidated the funds outside of Silk Road into two sizeable amounts: a Bitcoin address containing approximately 40,000 Bitcoin, largely funded by the Silk Road exploits of Zhong's accounts "gribs" and "s1lky," and Zhong's account with UserID "2c0eed0345"; and a Bitcoin address containing approximately 10,000 Bitcoin, largely funded by the Silk Road exploits of Zhong's accounts "dubba" and "suxor." *Id.* ¶ 35.

While executing the September 2012 fraud, Zhong did not list any item or service for sale on the Silk Road, nor did Zhong purchase any item or service on Silk Road. In fact, with the sole exception of a single message sent by one of the Fraud Accounts (the content of which is unknown), the Fraud Accounts appear to have been used exclusively to deposit and withdraw Bitcoin from the Silk Road often in rapid succession. None of the Fraud Accounts were used or accessed after November 2012. Zhong registered the accounts by providing the bare minimum of information required by Silk Road to create the account: a username and a password. For instance, although a user registering an account with Silk Road was given the option of providing nationality or country location information, Zhong provided no such information for the Fraud Accounts. The Fraud Accounts were merely a conduit for Zhong to defraud Silk Road of Bitcoin. *Id.* ¶ 36.

Zhong's Years-Long Concealment of the September 2012 Wire Fraud. For several years after September 24, 2012, Zhong maintained the 50,000 Bitcoin that he transferred out of the Silk Road in the configuration described immediately above, that is, one address containing approximately 40,000 Bitcoin, and another address containing approximately 10,000 Bitcoin. In

the years that have followed the fraud, however, Zhong periodically transferred this Bitcoin in bulk to different Bitcoin addresses. In particular, Zhong transferred the approximately 40,000 Bitcoin described above to new addresses in or around, among other times, October 2013, March 2015, August 2017, and January 2018. *Id.* ¶ 37.

Zhong periodically transferred the approximately 10,000 Bitcoin described above in bulk to new addresses, among other times, February 2014, February 2015, August 2017, and November 2017. On May 1, 2019, Zhong transferred both the approximately 40,000 Bitcoin and the approximately 10,000 Bitcoin amounts to new addresses. *Id.* ¶ 38. With respect to the 10,000 Bitcoin configuration, on or around November 24, 2020, Zhong transferred the 10,000 Bitcoin unlawfully obtained from Silk Road to about 10 Bitcoin addresses containing approximately 1,000 Bitcoin each. *Id.* ¶ 39.

In August 2017, solely by virtue of Zhong's possession of the at least 50,000 Bitcoin that he unlawfully obtained from Silk Road, Zhong received a matching amount of a related cryptocurrency—at least approximately 50,000 Bitcoin Cash ("BCH Crime Proceeds")—on top of the 50,000 Bitcoin of Silk Road Bitcoin.[2] In order to conceal his ownership and the illegal source of the Silk Road Bitcoin and the BCH Crime Proceeds, Zhong thereafter exchanged through an overseas cryptocurrency exchange all of the BCH Crime Proceeds for additional Bitcoin, amounting to approximately 3,500 Bitcoin of additional crime proceeds that are traceable to

[2] In August 2017, in a hard fork coin split, Bitcoin split into two cryptocurrencies, traditional Bitcoin and Bitcoin Cash ("BCH"). When this split occurred, any Bitcoin address that had a Bitcoin balance (as Zhong's did) now had the exact same balance on *both* the Bitcoin blockchain *and* on the Bitcoin Cash blockchain. As of August 2017, Zhong thus possessed 50,000 BCH in addition to the 50,000 BTC that he unlawfully obtained from Silk Road, solely by virtue of his possession of that 50,000 BTC at the time of the August 2017 hard fork.

Ulbricht's laundering of criminal proceeds. *Id.* ¶ 40. Collectively, by the last quarter of 2017, Zhong thus possessed approximately 53,500 BTC (collectively, the "Silk Road Crime Proceeds") of directly traceable crime proceeds.

Within the calendar year before law enforcement's November 9, 2021 search of Zhong's residences, Zhong pushed approximately 750 Bitcoin of the Silk Road Crime Proceeds through a decentralized Bitcoin mixer. A common function served by decentralized Bitcoin mixers is to obfuscate one's control over and the source of Bitcoin. That is precisely what Zhong did here. *Id.* ¶ 41. In June 2021, months before law enforcement's search of his residences, Zhong was evasive and untruthful to a cryptocurrency exchange about where his holdings came from, misleadingly claiming that Silk Road Crime Proceeds were in fact trading profits or Bitcoin that he had mined.

Zhong repeatedly boasted, in various public message board posts, about his state-of-the-art computer setup and security measures deployed at his residences. IRS-CI's cyber team personally observed and confirmed the astounding technical sophistication of Zhong's home operations. Among other things, at his residences, Zhong maintained multiple computer servers, virtual private networks, cold wallets, virtual machines, numerous layers of encryption, and multiple Bitcoin nodes.[3] *Id.* ¶ 43.

As noted above, on or about November 24, 2020, Zhong transferred approximately 10,000 of Silk Road Crime Proceeds to approximately 10 Bitcoin addresses that he controlled containing

---

[3] The term "cold wallet" refers to the practice of storing Bitcoin offline, often in an encrypted, password-protected storage device known as a hardware wallet. Because Bitcoin is an entirely digital currency, it is vulnerable to theft and misappropriation by hackers if stored online; thus, offline storage in a cold wallet is used to protect the digital currency against online attack. A Bitcoin node is a program that validates Bitcoin transactions and stores a copy of all transactions that have ever occurred on the Bitcoin network in its local database.

approximately 1,000 BTC each. In detailed ledgers that Zhong maintained on his laptop, Zhong labeled one of these particular BTC addresses as "10K-IN," referring to Silk Road Crime Proceeds. *Id.* ¶ 45.

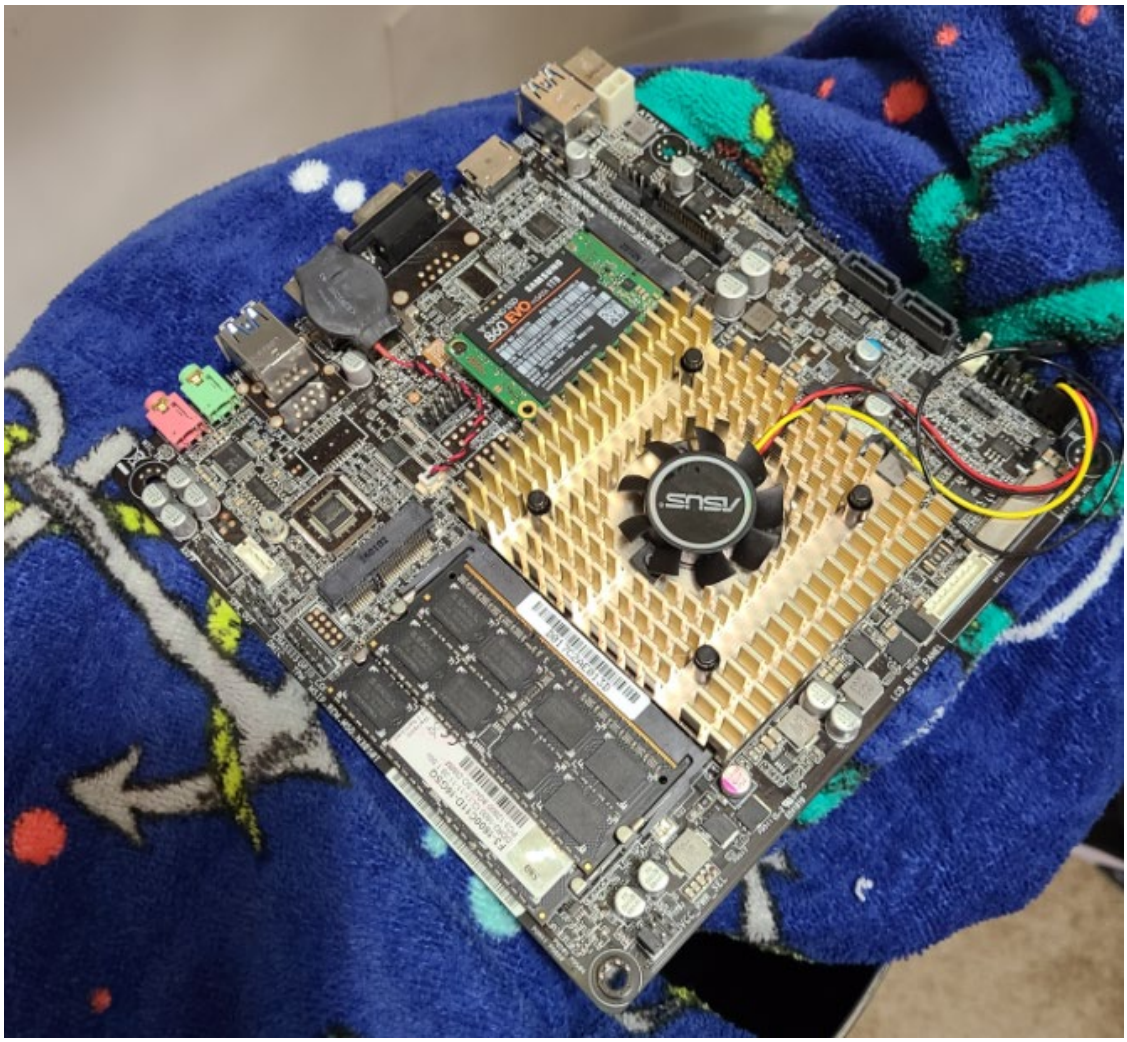
The Search

On November 9, 2021, law enforcement executed judicially authorized premises search warrants at two of Zhong's residences, one in the Northern District of Georgia and one in the Middle District of Georgia. During its execution of the search warrant at Zhong's Gainesville, Georgia lake house in the Northern District of Georgia (the "Search"), law enforcement recovered substantial portions of the Silk Road Crime Proceeds, as well as other valuable assets. *Id.* ¶ 46.

Law enforcement officers seized 50,491.06251844 Bitcoin of the approximately 53,500 Silk Road Crime Proceeds on devices in an underground floor safe, and on a single-board computer that was submerged under blankets in a popcorn tin stored in a bathroom closet. Additionally, law enforcement officers recovered property not traceable to Silk Road, including $661,900 in cash from the underground floor safe and a kitchen drawer, 25 Casascius coins (physical bitcoin) with an approximate value of 174 Bitcoin from the underground floor safe, and metal items from the underground floor safe.[4] Photographs of the popcorn tin, single-board computer, underground floor safe, and some of the seized items are included below:

[4] The metal items consisted of four one-ounce silver-colored bars, three one-ounce gold-colored bars, four 10-ounce silver-colored bars, and one gold-colored coin.


2 FAVORITES TOGETHER
2 FAVORITES TOGETHER
Cheetos
POPCORN
2
FLAVORS


ASUS


TRACKING
LIQUID

Furthermore, that day law enforcement also recovered 11.1160005300044 additional Bitcoin not traceable to Silk Road. *Id.* ¶ 47.

Using a conservative estimate of the lowest spot price of Bitcoin on November 9, 2021, the day of the Search, the value of the 50,491.06251844 Bitcoin of the Silk Road Crime Proceeds at the time of the Search was approximately $3.35 billion. The endpoint Bitcoin addresses where the seized Bitcoin was previously stored were visible in seized files and matched 11 of the applicable Bitcoin addresses which traced back to Zhong's transfers of the Silk Road Crime Proceeds in prior years. Additionally, the file name labels themselves revealed that 40,000 Bitcoin and 10,000 Bitcoin had been stored on the devices recovered during the Search. *Id.* ¶ 48.

During the Search, law enforcement officers also recovered from Zhong's living room a laptop containing detailed ledgers spelling out cryptocurrency transactions of assets configured in 40,000 and 10,000 blocks—the same configuration as the Bitcoin that Zhong had unlawfully obtained from Silk Road in September 2012—involving the Silk Road Crime Proceeds; these detailed ledgers further showed Zhong's control of the Silk Road Crime Proceeds. *Id.* ¶ 49. As noted above, in the ledgers, Zhong labeled one Bitcoin addresses as "10K-IN," referring to Silk Road Crime Proceeds, and labeled numerous transactions involving "BCH40K" and "BCH10K," referring to the BCH Crime Proceeds, showing Zhong's control of the Silk Road Bitcoin and BCH Crime Proceeds that Zhong exchanged for additional Bitcoin. *Id.* ¶ 50.

After the Search, because the Government seized substantial Bitcoin and computer equipment, Zhong no longer could control, at a minimum, the 50,491.06251844 Bitcoin traceable to the Silk Road seized during the Search. And, short of prevailing in litigation against the

Government, regardless of whether Zhong provided private keys and other technical assistance to the Government, Zhong never would be able to control that Bitcoin again.

Post-Search Conduct

After the Search, Zhong retained counsel. Following months of negotiations, and the Government's orally previewing with counsel the strength of some of its evidence, beginning in March 2022, counsel began surrendering to the Government passphrases and instructions for the Silk Road Crime Proceeds then in the Government's possession, as well as for additional Silk Road Crime Proceeds that Zhong had access to and had not dissipated. The passphrases and instructions provided by Zhong verified his prior control of the Silk Road Crime Proceeds.

On March 25, 2022, and May 25, 2022, Zhong's counsel voluntarily surrendered to the Government 825.38833159 Bitcoin and 35.4470080 Bitcoin, respectively, of additional Bitcoin that Zhong had unlawfully obtained from Silk Road in September 2012. Along with the 50,491.06251844 Bitcoin that law enforcement seized on November 9, 2021, this resulted in a total recovery of approximately 51,351.89785803 Bitcoin of the 53,500 Silk Road Crime Proceeds, *i.e.*, the subsequently located Silk Road Bitcoin. Using a conservative estimate of the lowest spot price of Bitcoin on the seizure dates, the total value of the Subsequently Located Silk Road Bitcoin is approximately $3.39 billion. *Id.* ¶ 51.

Furthermore, Zhong's counsel surrendered to the Government the following Bitcoin:

- 23.7112850 Bitcoin on April 27, 2022;
- 115.02532155 Bitcoin on April 28, 2022; and
- 4.57427222 Bitcoin on June 8, 2022. *Id.*

Using a conservative estimate of the lowest spot price of Bitcoin on the seizure dates, the total value of all Bitcoin seized for which the Government has obtained final orders of forfeiture is approximately $3.4 billion. The Bitcoin was seized on the dates specified in the chart below:

Date	**Quantity (BTC)**	**Lowest BTC Spot Price (USD)**	**Total USD Value at Time of Seizure**
November 9, 2021	50,491.06251844	$66,382.06	$3,351,700,741.56
November 9, 2021	11.1160005300044*	$66,382.06	$737,903.01
November 9, 2021	174*	$66,382.06	$11,550,478.40
March 25, 2022	825.38833159	$43,706.29	$36,074,661.78
April 27, 2022	23.7112850*	$37,997.31	$900,965.05
April 28, 2022	115.02532155*	$38,941.42	$4,479,249.37
May 25, 2022	35.4470080	$29,384.95	$1,041,608.56
June 8, 2022	4.57427222*	$29,944.40	$136,973.84
Total:	**51,680.32473733**		**$3,406,622,581.57**

*Not traceable to Silk Road.

B. Zhong's Guilty Plea, the Guidelines Calculation, Forfeiture, and the Presentence Investigation Report Recommendation

Guilty Plea and Guidelines

On November 4, 2022, Zhong waived indictment and pleaded guilty, pursuant to a plea agreement, to Count One of the Information, 22 Cr. 606 (PGG), which charged him with substantive wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2.

The plea agreement sets forth the following calculation of the offense level under the United States Sentencing Guidelines (the "Guidelines"):

(1) A base offense level of seven pursuant to U.S.S.G. § 2B1.1(a)(1);
(2) A 14-level increase, pursuant to U.S.S.G. § 2B1.1(b)(1)(H), because the loss amount was more than $550,000 but less than $1,500,000; and
(3) A three-level decrease, pursuant to U.S.S.G. § 3E1.1(a) and (b), for acceptance of responsibility.

In accordance with the foregoing, the applicable Guidelines offense level is 18. The parties agree that Zhong's Criminal History Category is I based on Zhong's 2014 DUI (alcohol) conviction in Athens, Georgia and his expunged cocaine possession deferred disposition also in Athens, Georgia, yielding a Stipulated Guidelines Range of 27 to 33 months' imprisonment. The PSR contains the same Stipulated Guidelines Range as that set forth in the plea agreement. PSR ¶¶ 64-80, p. 32.

Forfeiture and Government Sales of Seized Bitcoin

In connection with Zhong's guilty plea, on November 4, 2022, the Court entered a Consent Preliminary Order of Forfeiture as to Specific Property and Substitute Assets/Money Judgment forfeiting Zhong's interest in the following property:

- Zhong's 80% interest in RE&D Investments, LLC,[5] a Memphis-based company with substantial real estate holdings;
- $661,900 in United States currency seized from Zhong's home on November 9, 2021;
- Metal items, consisting of four one-ounce silver-colored bars, three one-ounce gold-colored bars, four 10-ounce silver-colored bars, and one gold-colored coin, all seized from Zhong's home on November 9, 2021;
- 11.1160005300044 Bitcoin seized from Zhong's home on November 9, 2021;
- 25 Casascius coins (physical Bitcoin) with an approximate value of 174 Bitcoin, collectively, seized from Zhong's home on November 9, 2021;
- 23.7112850 Bitcoin provided by Zhong on April 27, 2022;

[5] Zhong invested about $9.5 million of Silk Road Crime Proceeds in RE&D Investments, LLC ("RE&D"). RE&D is currently the debtor in Chapter 7 bankruptcy proceedings in the Western District of Tennessee. The Government has communicated with counsel to the Chapter 7 Trustee, and is optimistic that it will recover some value, and potentially significant value, from the debtor's estate, upon completion of the bankruptcy proceedings.

- 115.02532155 Bitcoin provided by Zhong on April 28, 2022; and
- 4.57427222 Bitcoin provided by Zhong on June 8, 2022.

Dkt. No. 7. The Court corrected a clerical error in the parties' order on December 6, 2022. On March 14, 2023, the Court entered a final order of forfeiture as to the above property, vesting all right, title, and interest in the above property in the United States. Dkt. No. 29.

On November 7, 2022, in *United States v. Ross Ulbricht*, S1 14 Cr. 68 (LGS), the Government filed a motion for entry of an Amended Preliminary Order of Forfeiture, seeking to forfeit approximately 51,351.89785803 Bitcoin traceable to Silk Road, valued at approximately $3,388,817,011.90 at the time of seizure, as follows:

- 50,491.06251844 Bitcoin seized from Zhong's home on November 9, 2021;
- 825.38833159 Bitcoin provided by Zhong on March 25, 2022; and
- 35.4470080 Bitcoin provided by Zhong on May 25, 2022.

14 Cr. 68 (LGS), Dkt. No. 394. Judge Schofield entered the Amended Preliminary Order of Forfeiture on December 5, 2022. Dkt. No. 395. On February 7, 2023, Judge Schofield entered a final order of forfeiture as to the above property, vesting all right, title, and interest in the above property in the United States. Dkt. No. 401.

With respect to the 51,351.89785803 Bitcoin forfeited in the *Ulbricht* case before Judge Schofield, the Government has begun liquidating (selling) it. On March 14, 2023, the Government sold 9,861.1707894 BTC (of the 51,351.89785803 BTC) for a total of $215,738,154.98. After $215,738.15 in transaction fees, the net proceeds to the Government were $215,522,416.83. Of the Bitcoin forfeited in the *Ulbricht* case, there remains approximately 41,490.72 BTC, which the Government understands is expected to be liquidated in four more batches over the course of this calendar year. The Government understands from IRS Criminal Investigation - Asset Recovery

& Investigative Services that the second round of liquidation will not be sold prior to Zhong's sentencing date.

Probation's Recommendation

The Probation Office recommends a variance sentence of 24 months' imprisonment. PSR at 32. It points out that Zhong "took advantage of the [Silk Road's] flaw by creating several user accounts to hide who he was and conducted multiple internet transactions in quick succession, which improperly caused the Silk Road bitcoin payment system to release about 50,000 coins to him that did not belong to him." *Id.* at 33. It continues,

> While the instant offense did not involve a crime of violence or drug trafficking, Zhong's conduct is still nevertheless serious. While engaging in one illegal activity, the purchasing of drugs, Zhong then began to steal from the source of which was providing him drugs. The defendant had in his possession multiple computer servers, virtual private networks, among other things, enabling him to commit the offense. He then managed to keep the Bitcoin protected, and his identity hidden for several years. His actions and him engaging in this crime of opportunity makes us question his risk of recidivism. Due to Zhong's conduct in the instant offense, we believe that a period of incarceration is warranted.

Id. at 34.

II. DISCUSSION

A. Applicable Law

As the Court is aware, the Guidelines still provide important guidance to the Court following *United States v. Booker*, 543 U.S. 220 (2005), and *United States v. Crosby*, 397 F.3d 103 (2d Cir. 2005). Indeed, although *Booker* held that the Guidelines are no longer mandatory, it also held that they remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. *Booker*, 543 U.S. at 264. As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable

Guidelines range," which "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007).

After that calculation, however, a sentencing judge must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) "the nature and circumstances of the offense and the history and characteristics of the defendant"; (2) the four legitimate purposes of sentencing, as set forth below; (3) "the kinds of sentences available"; (4) the Guidelines range itself; (5) any relevant policy statement by the Sentencing Commission; (6) "the need to avoid unwarranted sentence disparities among defendants"; and (7) "the need to provide restitution to any victims." 18 U.S.C. § 3553(a)(1)-(7); *see also Gall*, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
(B) to afford adequate deterrence to criminal conduct;
(C) to protect the public from further crimes of the defendant; and
(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

B. Discussion

The Government respectfully submits that a sentence of imprisonment, but below the Stipulated Guidelines Range and below Probation's recommended sentence of 24 months, would be sufficient, but not greater than necessary, to serve the purposes of sentencing. In particular, the seriousness and breadth of the offense, and the needs to promote respect for the law, provide just punishment for the offense, and afford adequate deterrence to criminal conduct, all justify such a sentence.

Offense conduct. A sentence of imprisonment is necessary to reflect the seriousness of the offense and to provide just punishment. Although the underlying 2012 wire fraud was not especially sophisticated in concept, it also was not simple, as Zhong created about nine user accounts to steal 50,000 Bitcoin from the Silk Road in over 140 transactions over a few days. This was not a one-click scheme to defraud, this required hours of work over several days. Additionally, although it is true that Zhong did not attempt to carry out the same scheme again in the ensuing weeks and months, it should be noted that Zhong attempted to and did obtain what he believed to be, based on his message board posts, the full amount of Bitcoin stored at a time by the Silk Road: 50,000 BTC.

More fundamentally, over the following nine-plus years, through countless transactions and deliberate choices, Zhong expertly obfuscated what he had done and how he obtained his fortune. Among other things, he used a decentralized Bitcoin mixer to frustrate law enforcement tracing efforts; used an overseas cryptocurrency exchange to convert the BCH to BTC; in June 2021, was evasive and untruthful to a cryptocurrency exchange about where his holdings came from, claiming that Silk Road Crime Proceeds were in fact trading profits or Bitcoin that he had mined; and used an impressive array of technological tools, all to, as Zhong himself concedes, attempt to keep his identity and control over the Silk Road Crime Proceeds a secret.[6]

Particularly with respect to the subsequent laundering, Zhong's actions were far from a

[6] As to whether, as Zhong attests, Ulbricht and Zhong messaged each other and Ulbricht sent Zhong additional Bitcoin, the Government has searched its images of the Silk Road Servers but not found any evidence of this. Nor has the Government received corroborating evidence of this from counsel. Thus, this "tacit after the fact approval by Ross Ulbricht of Jimmy's withdrawal of the Bitcoin from Silk Road," Def. Mem. at 38, should not be credited by the Court.

one-time mistake or a fleeting lapse in judgment. On a daily basis, over the course of many years, especially ratcheting up in August 2017 until the November 2021 Search, Zhong made a conscious and deliberate choice to continue to benefit from his crime. Zhong designed the original wire fraud, as well as the more sophisticated laundering conduct over the following nine-plus years, to evade detection. In this manner, he was able to extend his access to the crime proceeds, as the price of Bitcoin skyrocketed. The sophisticated nature of the laundering was intended in no small part to frustrate the efforts of law enforcement to identify Zhong as the Bitcoin's controller and trace its Silk Road origins.

Another aggravating factor is Zhong's dissipation of approximately 2,149 Bitcoin of the Silk Road Crime Proceeds. Based on the Government's tracing efforts to date, in the 51 months before the Search, Zhong spent over $16 million of money that was the Government's (not his) on real estate investments, private planes, boats, luxury products, travel, hotels, nightclubs, and other decadent items. Among other expenditures, Zhong dissipated Silk Road Crime Proceeds between August 2017 and November 2021 on the following items: $9.5 million in RE&D Investments, LLC, a Memphis-based company with substantial real estate holdings of which Zhong was the 80% owner; hundreds of thousands of dollars to luxury travel, yacht, and private jet companies; nearly $150,000 to Tesla; tens of thousands of dollars to boating companies; tens of thousands of dollars at the Plaza, Four Seasons, Ritz Carlton, Waldorf Astoria, and St. Regis hotels; tens of thousands of dollars at 21 Club, Tao, and various Florida and Georgia nightclubs; well over ten thousand dollars for tickets to sporting events; and well over ten thousand dollars for luxury brands such as Louis Vuitton, Gucci, and Jimmy Choo. And, of course, the portions of Zhong's high standard of living that he maintained even with untainted proceeds to buy two homes, multiple

Lamborghinis, a boat, multiple jet skis, and a motorcycle, were backstopped by the safety net of billions of dollars of Silk Road Crime Proceeds that he also possessed. Importantly, based on the price of Bitcoin the day of the Search, the 2,149 BTC of dissipated proceeds would have been valued at over $142 million. Based on the price of Bitcoin today, the dissipated proceeds would have been valued at over $61 million.

As for the defense argument that Ulbricht is an unsympathetic victim, while undoubtedly true that Ulbricht is less sympathetic than other victims, it does not change the following facts: Zhong committed a cyber-robbery of his drug dealer; spent over $16 million of these crime proceeds; deprived the Government of crime proceeds that it was entitled to that would have been valued at over $142 million at the time they would have been seized; and used his considerable technical skills to conceal and benefit from this crime for over nine years. It goes without saying that a drug dealer's crime proceeds, here Ulbricht's, do not exist in a lawless, grey area whereby they are free to be stolen, invested, and spent by criminals with no repercussions. Indeed, the Government regularly prosecutes robberies of drug dealers, notwithstanding that the victims of such crimes are, definitionally, engaged in criminal activity themselves.

Nor does Zhong deserve a sentence of time-served because his fraud proceeds appreciated in value. Again, a drug dealer's crime proceeds are not free to be stolen, invested, and spent by others with no risk of imprisonment. Rewarding Zhong for the appreciation of his crime proceeds by imposing a non-custodial sentence also "would encourage criminals to invest or gamble ill-gotten gains," *United States v. $465,789.31 Seized From Term Life Ins. Pol'y No. PJ 108 002 588 in Name of Lee at AXA Equitable Life Ins. Co., New York, New York*, No. 3:15-CV-1353 (JAM), 2018 WL 4568408, at *5 (D. Conn. Sept. 24, 2018), in hopes that they would benefit with a lighter,

non-custodial sentence if their investments or gambling efforts panned out. The Government, and future victims, should not have to bear the burden of future defendants' choice of investments of crime proceeds.

As for Zhong's assistance in accessing the Silk Road Crime Proceeds, the Government of course gives Zhong considerable credit for this assistance. Indeed, it is because of this aid that the Government exercised its discretion to allow Zhong to plead guilty to wire fraud, and not money laundering (with a potential Guidelines range over ten times as long as the Stipulated Guidelines Range that the parties agree applies), and his decision to help the Government access the Bitcoin is the primary basis of the instant below-Guidelines recommendation.

That said, it bears mentioning that Zhong did not voluntarily turn the Silk Road Bitcoin over to law enforcement. Rather, law enforcement seized it pursuant to search warrants. The day of the search, Zhong provided zero assistance as the case agents recovered the Silk Road Bitcoin that Zhong had meticulously hidden in an underground floor safe and a bathroom closet, realizing that his nearly decade-long crime had been discovered. For at least four months, the Government sought from Zhong information so that Zhong could permanently relinquish the Silk Road BTC, billions of dollars of crime proceeds that Zhong would almost certainly never again possess regardless of whether Zhong provided the Government technical assistance. After the Government voluntarily proffered to counsel the strength of its evidence, and after Zhong understood that the Government knew that Zhong had dissipated millions of dollars of crime proceeds, Zhong eventually surrendered the information in March and April 2022. In short, of course Zhong deserves credit for sharing the information that he did with the Government, but the above context is necessary to complete the picture. By the time Zhong gave up the information, he did so

knowing that, at least with respect to the 50,491.06251844 Bitcoin seized the day of the Search, he almost certainly would never be able to access it again.

Zhong also rightly points to his difficult family background, autism spectrum disorder, age, and supportive letters from friends as additional mitigating factors. Just as the Government took these factors into account when offering Zhong a wire fraud plea and is taking these factors into account in its sentencing recommendation, so too should the Court at sentencing. On Zhong's family background, the Government respectfully observes that, though worthy of consideration, it is sadly true that defendants with comparable and, candidly, far more difficult backgrounds, are regularly sentenced to lengthy terms of imprisonment in this District. As for Zhong's autism spectrum disorder, nobody disputes that Zhong is able to discern from right and wrong, took affirmative steps evincing consciousness of guilt and to conceal his conduct from law enforcement, is highly functional and intelligent, and had considerable lawfully obtained means to live on during the period he dissipated millions of dollars of Silk Road Crime Proceeds.

Although Zhong was, as counsel observes, young at the time of the fraud, as he grew older he did not take steps to rectify his earlier crime; instead, he continued to live off of and spend the crime proceeds. In fact, Zhong's spending escalated over time up until the Search. As for the character letters, as counsel points out, several of the writers are indebted to Zhong, having each received millions of dollars of gifts from Zhong, albeit perhaps unknowingly (to them), in the form of Silk Road Crime Proceeds. Def. Mem. at 20 n.14. Specifically, three of the writers, Alexa Pisczak, Julian Pisczak, and Christina Ross each received 50 Bitcoin of Silk Road Crime Proceeds, valued at about $3.3 million at the time of the Search, and $1.4 million today.

Moreover, one of Zhong's purported explanations for not preserving or returning the Silk

Road Crime Proceeds, that it would "have been unlawful for Jimmy to return it to Ulbricht even if he had wanted to," *id.* at 7 n.2, is entitled to little weight. Zhong displayed ample awareness that what he did was against the law in the years following his 2012 crime. It strains credulity to think that he behaved the way he did because he thought that it would have been unlawful for him to return the Silk Road Crime Proceeds. At a minimum, he could have retained counsel to communicate with federal law enforcement, particularly after Ulbricht's arrest, prosecution, and conviction.

Finally, Zhong's reliance on a readily distinguishable, civil forfeiture action in the Northern District of California is of little help to him. *Id.* at 33-34, 37. The Government has conferred with one of the agents on that case and reviewed the civil forfeiture complaint. To start, unlike Zhong, Individual X surrendered the Bitcoin in that case far earlier, and in a wholly different posture, than did Zhong. Again, Zhong only provided the Government his private keys and technical assistance *after* a judicially authorized search warrant was executed on his homes, after the Government had seized 50,491.06251844 Bitcoin of Silk Road Crime Proceeds and significant substitute assets, and after it became clear to Zhong, following the Government's voluntary proffer of certain irrefutable evidence, that he almost certainly would never be able to access it again. In contrast, there was no judicially authorized premises search warrant for Individual X, and law enforcement had not already seized Individual X's Bitcoin prior to Individual X's provision of information and the Bitcoin to law enforcement.

Unlike Zhong, who, as discussed above, engaged in years of sophisticated, state-of-the-art, and highly successful efforts to mask what he had done and conceal his crimes, Individual X left virtually all of the Bitcoin untouched in the same address for seven-and-a-half years from April

2013 until Individual X surrendered it to law enforcement in November 2020. Further, unlike Zhong, who dissipated over $16 million of Silk Road Crime Proceeds, spending opulently in the process, Individual X did not have anything close to such spending habits, and only dissipated Bitcoin that was far less valuable, estimated to be less than $100,00 at the time of dissipation, as compared to Zhong's $16 million. In sum, Individual X's case is significantly different from Zhong's, and does not militate in favor of a non-custodial sentence.

Specific deterrence. Specific deterrence and the need to promote respect for the law also counsel in favor of a custodial sentence. As noted above, for over nine years, Zhong tried to conceal what he had done and, over the final four of those years, spent over $16 million of money that was not his on real estate investments, luxury products, travel, hotels, nightclubs, and other self-indulgent items.

During this time, and prior to the Search, despite his technical brilliance and eminently employable skills, Zhong had zero employment history except for installing alarms during the Summer of 2009 and, he reports, Bitcoin mining, also in 2009, 12 years before the Search. PSR ¶¶ 109-10. Instead, Zhong chose, day in and day out, to fund his opulent lifestyle in substantial part with the Silk Road Crime Proceeds. Although Zhong took great measures to conceal his connection to the crime, that did not stop him from boasting about his opulent lifestyle—an indicator that he felt no shame about or remorse for living on criminal proceeds. For example, on August 10, 2020, about 11 years since Zhong had worked lawfully, and after he had spent over $10 million of crime proceeds on private jets, nightclubs, luxury goods, and five-star hotels, Zhong posted a photo of his dog in a Lamborghini, while also referencing an additional Lamborghini of his that was "still in the shop." When a user responded to the photo, "American Dream right

there!" Zhong posted: "Exactly why I'll never have any sympathy for these free shit people. I grew up broke as hell, taught myself software development and electronics design in high [] school, college classes were a joke, then FPGA & ASIC development in my free time in college. You have the internet, any skill in the world is there for you to learn for free. Learned automotive repair, welding, CAD design, CNC machining, 3D printing too. GET A JOB." In light of the severity, length, and breadth of his conduct, specific deterrence and the need to promote respect for the law also weigh in favor of sentence of incarceration.

General deterrence. The need for general deterrence is also acute in this case, given how lucrative cyber frauds are and how difficult they are to detect and prosecute. One of the paramount factors that the Court must consider in imposing sentence under Section 3553(a) is the need for the sentence to "afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). Courts have generally recognized that "white collar crime . . . requires heavy sentences to deter because it is potentially very lucrative." *United States v. Hauptman*, 111 F.3d 48, 52 (7th Cir. 1997); *see also Harmelin v. Michigan*, 501 U.S. 957, 988 (1991) (noting that "since deterrent effect depends not only upon the amount of the penalty but upon its certainty, crimes that are less grave but significantly more difficult to detect may warrant substantially higher penalties"). "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 quotation omitted). "Defendants in white collar crimes often calculate the financial gain and risk of loss, and white collar crime therefore can be affected and reduced with serious punishment." *Id.*; *see also United States v. Goffer*, 721 F.3d 113, 132 (2d Cir. 2013) (noting district court's comments during an insider trading sentencing

that defendant made a "deliberate decision, weighing the risks, that insider trading 'was a game worth playing'" and characterizing "district court's assertion that insider trading requires high sentences to alter that calculus" as "a Congressionally-approved example of giving meaning to the 18 U.S.C. § 3553(a) factors"); *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) ("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 expected benefits of a crime and hence the punishment required to deter it."); Drago Francesco, Roberto Galbiati & Pietro Vertova, *The Deterrent Effects of Prison: Evidence From a Natural Experiment*, 117 J. of Political Econ. 257, 278 (2009) ("Our findings provide credible evidence that a one-month increase in expected punishment lowers the probability of committing a crime. This corroborates the theory of general deterrence.").

This is particularly so in the case of profitable cyber fraud schemes like the fraud here. These types of frauds result in substantial gains to their perpetrators and yet are inherently difficult for law enforcement to detect and stop. It took IRS-CI considerable resources and years to uncover Zhong's crime and trace the Silk Road Crime Proceeds. It has, unfortunately, become too easy for advanced, computer-savvy individuals like Zhong to target and victimize holders of cryptocurrency from behind computer screens, and to hide their crimes through a web of concealment-focused transactions, mixers, and offshore cryptocurrency exchanges. This Court's sentence of Zhong should send a strong and clear message to others that cryptocurrency thefts and frauds, no matter the victim, run the risk of incarceration.

III. CONCLUSION

On these unique facts, a sentence of imprisonment, but below the Stipulated Guidelines Range and below Probation's recommended sentence of 24 months, would be appropriate and just. Such a sentence would appropriately credit Zhong for surrendering to the Government access to his substantial crime proceeds and recognize the other mitigating factors discussed above. At the same time, the requested period of incarceration would also avoid minimizing the seriousness of Zhong's long-running conduct and would send a message to would-be cyber criminals that time

in prison—and not merely being asked to give up whatever is left of their ill-gotten gains—is the likely consequence of criminal conduct.[7]

Dated: New York, New York
March 31, 2023

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

By: /s/ David R. Felton
David Felton
Assistant United States Attorney
(212) 637-2299

cc: Michael F. Bachner, Esq.
John A. Garland, Esq.
Donald F. Samuel, Esq.
Amanda R. Clark Palmer, Esq.
(by ECF)

[7] The Government is not seeking a fine in light of the sworn financial information provided by Zhong's counsel, and counsel's representations about Zhong's forthcoming tax liabilities.