

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

UNITED STATES OF AMERICA :
 :
 v. : **CRIMINAL NO. 19-cr-395 (BAH)**
 :
LARRY DEAN HARMON, :
 :
 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 96 months at offense level 29. 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, from 2014 to 2017, Larry Harmon (“the defendant”) ran Helix, a darknet mixer that laundered customers’ bitcoin. Helix was connected to Grams, a darknet search engine also run by the defendant. Helix was one of the most popular mixing services on the darknet and was highly sought after by online drug dealers who needed to launder their illicit proceeds. Helix processed at least approximately 354,468 bitcoin—the equivalent of approximately \$311,145,854 in U.S. dollars at the time of the transactions—on

behalf of its customers, including customers in the District of Columbia. Much of those funds were coming from or going to darknet drug markets. The defendant retained a percentage of these transactions as his commissions and fees for operating Helix. The defendant began to shut down operations for Grams and Helix in or about December 2017.

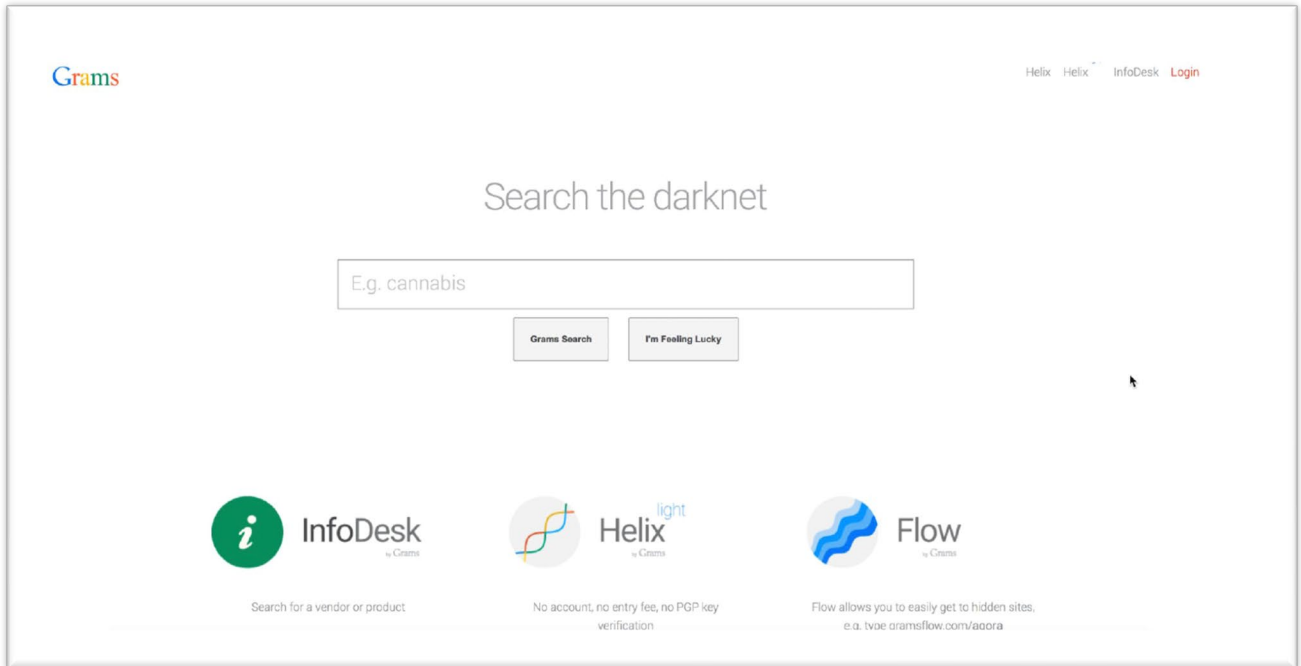
B. Factual Background

a. Grams: The Origin of the Defendant's Darknet Platform

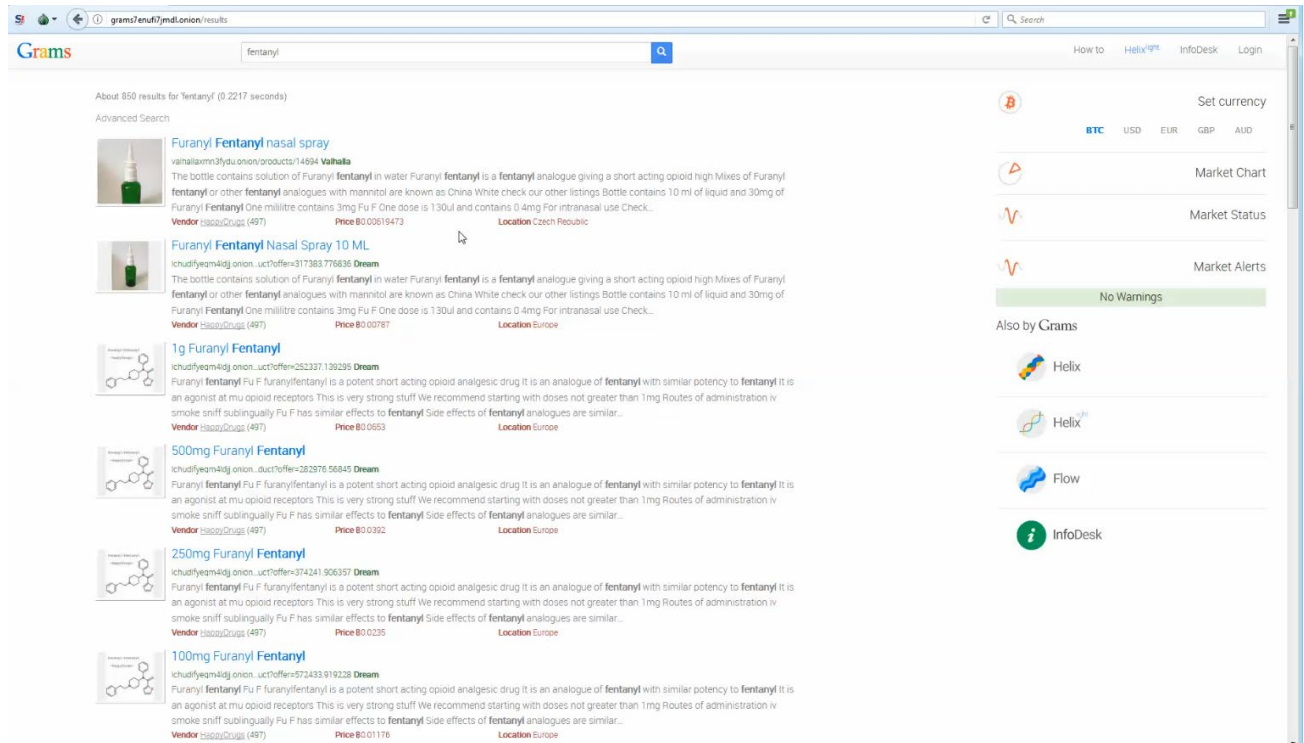
In or around 2014, the defendant launched Grams, a service designed to make it easier for people to find and buy items on darknet markets. At the time, darknet drug markets were rising in popularity. In the aftermath of the 2013 takedown of the first major online darknet drug market, Silk Road, numerous other markets emerged and competed for prominence. The sites were similar on their faces, offering a wide variety of illegal goods for sale. The available products included stolen credit card information, compromised account credentials, hacking tools, and stolen or forged identity documents, but by far the most prevalent items sold on the sites were illegal narcotics. Drug vendors from all over the globe found an expanded customer base and were now able to distribute their wares to anyone with a shipping address. The darknet markets plainly displayed and advertised drugs on their homepages, allowing site visitors to filter for opiates, stimulants, psychedelics, and other categories of drugs. As the defendant himself observed in an online post, “Right now the Darknet is 90% drugs and illegal items for sale.” In order to avoid law enforcement disruption, the sites operated exclusively on Tor, an anonymizing network that concealed users’ locations by routing Internet traffic through a series of relay nodes across the globe.

While Tor provided needed anonymity to the criminals operating on the darknet markets, it also made the marketplaces harder to find for a casual drug user—which in turn limited the sites’

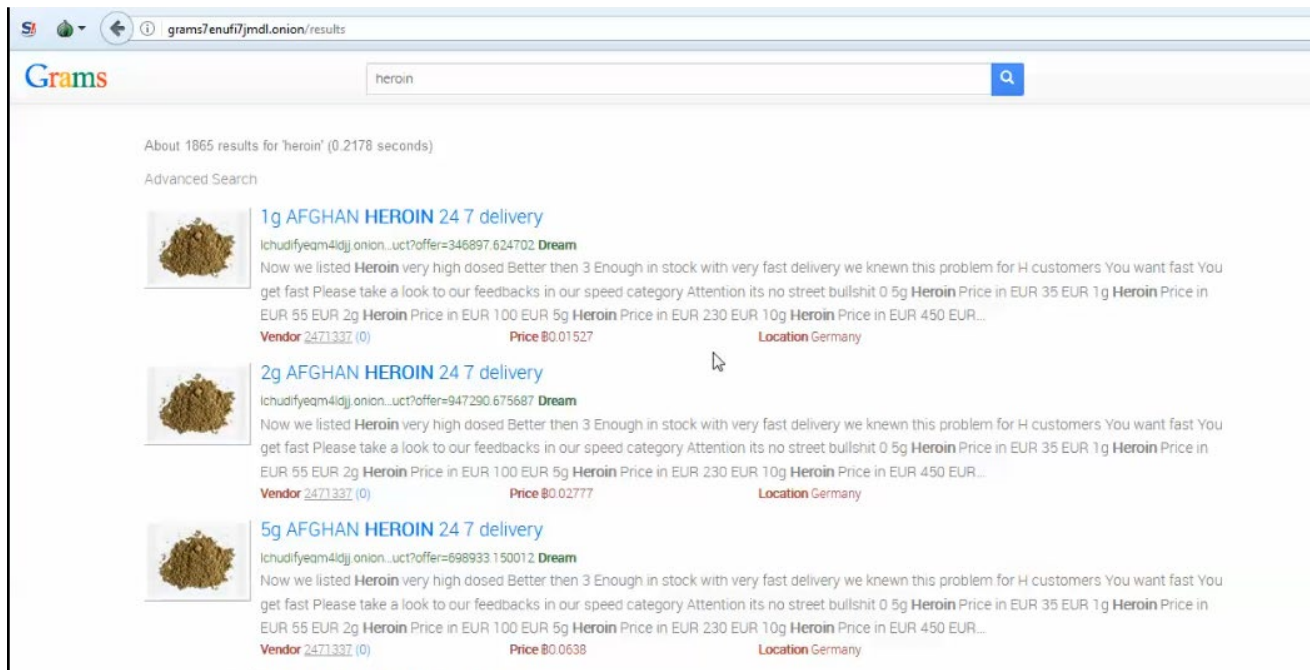
profitability. The defendant recognized this as a business opportunity. The defendant launched Grams, the self-proclaimed Google of the darknet. Grams was designed to allow users to easily find the various darknet markets, and to search across them.



The Grams homepage, displayed above, offered a clean user interface that mimicked Google. Users could easily search multiple markets for whatever item they were seeking and could compare listings within the Grams search results. For example, a search for “fentanyl,” displayed below based on an undercover screenshot captured during the investigation, returned numerous listings of fentanyl for sale:



A user could look through the Grams search results and find links directly to the listings selling the item. For example, the below screenshot reflects an undercover's search on the defendant's site for heroin, which yielded over 1,800 results:



A Grams user could click on any of the links and navigate directly to the product listing. For example, the top search results for “heroin” above featured multiple listings from a vendor on Dream Market, a prominent darknet market at the time. A user could click on the link in the Grams search results and navigate directly to the order page, where they could place their order for heroin:

Dream Market
Ichudifeqm4ldj.onion
 Established 2013

Shop Messages: 0 Account: B0 [REDACTED]

0 Logout

Browse by category

- Drugs 53964
 - Opioids 4850
 - Buprenorphine 238
 - Codeine 218
 - Dihydrocodeine 31
 - Fentanyl 463
 - Heroin 1185**
 - Hydrocodone 196
 - Hydromorphone 53
 - Morphine 115
 - Opium 177
 - Other 142
 - Oxycodone 700
 - Digital Goods 41896
 - Drugs 53964
 - Drugs Paraphernalia 411
 - Services 3179
 - Other 2478

Onion mirrors

Ichudifeqm4ldj.onion
 jd9huwcvhw94.onion
 13e8y3u0ifkzow2.onion
 7ep7acrhunzdcw3l.onion

5g Heroin Pure Uncut #3


Vendor [REDACTED] (190) (4.89★) (7, 5/5) (216/4/0) (35/1/1)

Price B0.0449 (€160)

Ships to Worldwide, Worldwide

Ships from France

Escrow Yes



Product description

★★★★★ Heroin Pure Uncut #3 ★★★★★

Very strong heroin #3 is for opiate-users with higher tolerance. Direct off the brick & 100% uncut! For smoking and IV.

Imported from Afghanistan.

Terms and conditions of [REDACTED]

How to buy ?

Fill in this informations correctly :

Name :
 Address :
 City :
 Zip Code :

Links

- Forum
- Help
- Conferences
- Vendor application
- Earn money

Exchange

BTC	1.0
mBTC	1000.0
USD	4248.9
EUR	3562.6
GBP	3284.7
CAD	5283.3
AUD	5336.7
SEK	33809.0
NOK	32900.6
DKK	26498.6
TRY	14581.7
CNH	28117.1
HKD	33110.8
RUB	248298.9
INR	271106.7
JPY	462215.2

News

- Deposit delays 27/10/2016
- Forum under maintenance 12/08/2016
- Earn money by finding bugs 14/01/2016
- Forum Relaunched 29/03/2016
- Invite friends and earn money 07/03/2016

Hint. Javascript enabled

b. Helix – Early Development

The defendant did not stop with his development of the Grams search tool. He set out to be a one-stop-shop for all of the needs of darknet market vendors, administrators, and everyday users. He took steps to develop a full suite of tools that would enable people to buy and sell more drugs faster and easier. The most significant and successful add-on service to Grams was Helix, the defendant's darknet mixer.

In mid-2014, within several months of launching Grams, the defendant announced Helix. Helix was a direct response to a significant need among darknet users. Darknet markets accepted payment in bitcoin, a cryptocurrency that allowed anyone with an Internet connection to send funds peer-to-peer, without the involvement of intermediaries such as banks or payment processors. This

lack of intermediaries was essential to darknet markets, who otherwise would have had their funds seized and accounts shut down due to the openly illicit nature of their transactions. However, bitcoin relied on a public transaction ledger, known as the blockchain, which meant that transactions could be traced from one bitcoin address—the cryptocurrency equivalent of an account number—to another. Furthermore, when the bitcoin was converted to U.S. dollars or another more widely accepted currency, law enforcement could often obtain records from the exchange conducting the transaction to identify the person responsible. Savvy drug vendors thus wanted to make their transactions more difficult to trace on the blockchain. While many experimented with DIY self-laundering processes—such as sending transactions through a series of hops or layers, or breaking the transactions into smaller sub-pieces and then coalescing them after a long chain of transactions—demand grew for professional services that could launder dirty funds in a way that would make it nearly impossible to connect a stash of bitcoin to its illicit origins.

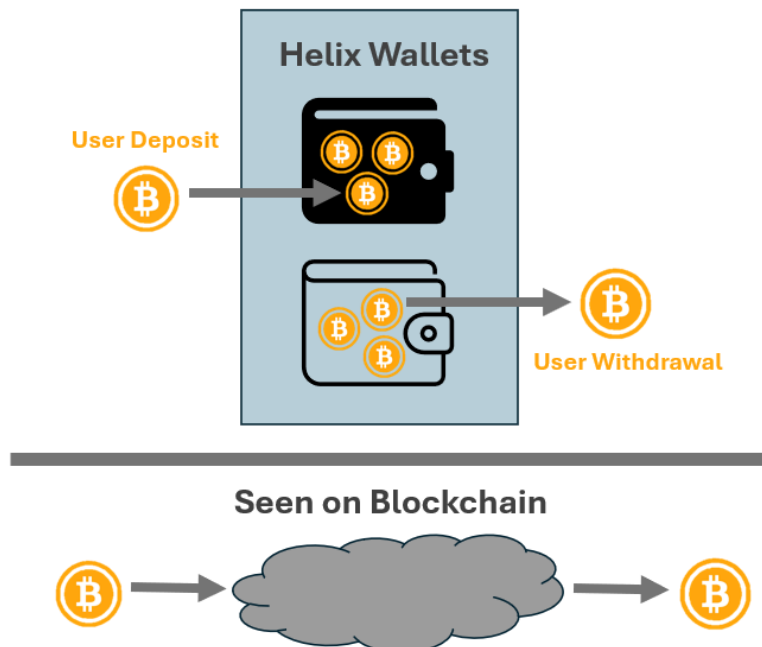
In laundering his own funds from his early operation of Grams, the defendant used Bitcoin Fog, the largest and longest-running bitcoin mixer at the time. Bitcoin Fog was popular and widely used by members of the darknet drug community, the very group that the defendant was attracting to Grams. As the defendant recalled in his February 2024 testimony at the trial of the Bitcoin Fog administrator, Roman Sterlingov, Mr. Harmon thought that the Bitcoin Fog user interface was clunky and that the service would benefit from more user-friendly improvements. The defendant thus set out to launch his own Bitcoin mixer, intended to improve upon Bitcoin Fog’s features and provide a more seamless experience for Grams users.

The defendant espoused the benefits of using a professional service like Helix: “Using a tumbler to tumble your coins is like paying a mechanic to change your oil. You can change your

oil yourself and save some money but you will have to get dirty and it will take a lot of your time. If you use a mechanic you pay more than doing it yourself, but you know it gets done right and quickly without you having to spend any of your time.” ECF No. 39, Ex. A.

c. Helix Operation

Helix enabled customers, for a fee, to send bitcoin to designated recipient addresses in a manner which was designed to conceal and obfuscate the source or owner of the bitcoin. A Helix customer began the mixing process by sending their bitcoin to a bitcoin wallet controlled by Helix. Helix then transmitted bitcoin located in other wallets controlled by Helix—which Helix advertised were not linked to darknet activity—to a receiving address designated by the customer. In practice, this allowed customers to transmit bitcoin to other bitcoin addresses without leaving a direct trail of transactions on the public blockchain. A highly simplified conceptual diagram is displayed below:



The defendant offered two versions of Helix: Helix, which required a customer to have a Grams account, and Helix Lite, which did not require a Grams account. For the original version of Helix, users were able to log into Helix and deposit their bitcoin. While logged in, they could indicate the withdrawal address they wanted the bitcoin sent to. The defendant's system would automatically process that withdrawal—less a 2.5% fee—with a time delay based on the confirmations required in bitcoin transaction processing. This was an improvement on the main competitor mixer at the time, Bitcoin Fog, which required users to log in multiple times in order to process the funds.

The defendant subsequently developed Helix Light, a version of Helix that did not require any log-in. Helix Light users could input into the Helix Light interface the bitcoin address to which they wanted their funds sent, without having to first log in. Helix Light provided unique, session-specific bitcoin address for users to deposit their funds. Helix Light functionality is displayed in the graphic below, which was featured on the defendant's site:



Helix offered customer support functionality, through which the defendant spent many hours communicating with Helix users and assisting them with their laundering. He

troubleshooted transactions and explained fundamental concepts related to the darknet and cryptocurrency. Helix also asserted that it deleted customer information after seven days, or allowed customers to delete their logs manually after a withdrawal.

The defendant touted Helix's superiority compared to other mixers by claiming that the bitcoin distributed to his customers were "new" bitcoin that had not been used on the darknet. The defendant partially accomplished this by funneling Helix bitcoin through accounts at an overseas, noncompliant bitcoin exchange—depositing "dirty" Helix funds received from customers and withdrawing new, "clean" fund from the exchange. While Helix was designed to appear straightforward from a user perspective, behind the scenes the defendant managed a sophisticated set-up of hundreds of thousands of bitcoin addresses and servers across the globe. In total, the defendant controlled over 800,000 bitcoin addresses, and Helix conducted hundreds of thousands of individual transactions.

d. Defendant Targeted Darknet Market Users

The defendant designed Helix to enable users on the darknet to make untraceable transactions online and evade law enforcement, and he explicitly advertised Helix to customers as a way to conceal transactions on the darknet from law enforcement. The defendant posted frequently on the online forum Reddit using a pseudonymous moniker "GramsAdmin," which identified him as the administrator of Grams. In a posting written on or about June 2014, shortly before launching Helix, the defendant explained that Helix was designed to be a "bitcoin tumbler" that "cleans" bitcoins by providing customers with new bitcoins "which have never been to the darknet before."

Harmon explained, "I created grams because 90% of the darknet was behind blackmarket sites which required a login to view. This made it unsearchable by normal search engines. . . . I

wanted to make it easier for users to use the darknet.” ECF No. 16, Ex. C. Harmon understood that he was providing an essential service to darknet users who would otherwise be arrested by law enforcement. He encouraged drug dealers and buyers specifically to use Helix, noting, “No one has ever been arrested just through bitcoin taint, but it is possible and do you want to be the first? If you get a controlled delivery and you deny ordering the package the bitcoin taint will be the evidence they need to prove you ordered it. It is better to be safe than sorry no matter which tumbler or tumbling method you use.” ECF No. 16, Ex. E.

e. Symbiotic Partnership with Darknet Markets

The defendant worked to ensure Grams and Helix connected to or otherwise supported all of the major darknet markets at the time. The defendant developed an Application Program Interface (API) to allow darknet markets to integrate Helix directly into their bitcoin withdrawal systems. The defendant also customized features of Helix to ensure compatibility with significant markets.

As one example, in 2014, the defendant engaged in a conversation with a member of the administrative team of Evolution, a prominent darknet market at the time. The defendant explained his challenges getting the API working to allow Grams users to search Evolution’s listings. In the discussion, the defendant stated his desire for Grams and “evo” (a common shorthand for Evolution) to “work together more,” suggesting, “if grams pushed evo by integrat[ing] certain features and evo pushed grams as the best [sic] place for reviews and tumbling we would both shoot to the top.” (The reference to “reviews” pertains to the Grams search results, while “tumbling” is a reference to the Helix service.) The defendant further observed that such a symbiotic arrangement “worked well for agora and bitcoinfog,” referring to Agora, another popular darknet marketplace, and Bitcoin Fog. Shortly after this conversation, the defendant added

functionality to Helix to make it specifically compatible with Evolution, and the Evolution team member sent a message to the defendant indicating that he would post on two popular message boards that it was “safe” and “a great method” to use Helix in conjunction with Evolution.

The defendant understood the value of cultivating relationships with the administrators of various darknet markets to partner with his services. He explained at the time:

I have been talking to outlaw, silkroad2, cloud nine. They all said they want on grams and are either going to use my api [*i.e.*, Application Program Interface] or give me some of their own. I consider them with agora which is already on there to be the majors. . . . if there is a strong demand for a market and they are not on there I will make sure we add them.

ECF No. 16, Ex. F. Outlaw, Silkroad2, Cloud Nine, and Agora were all darknet drug trafficking markets.

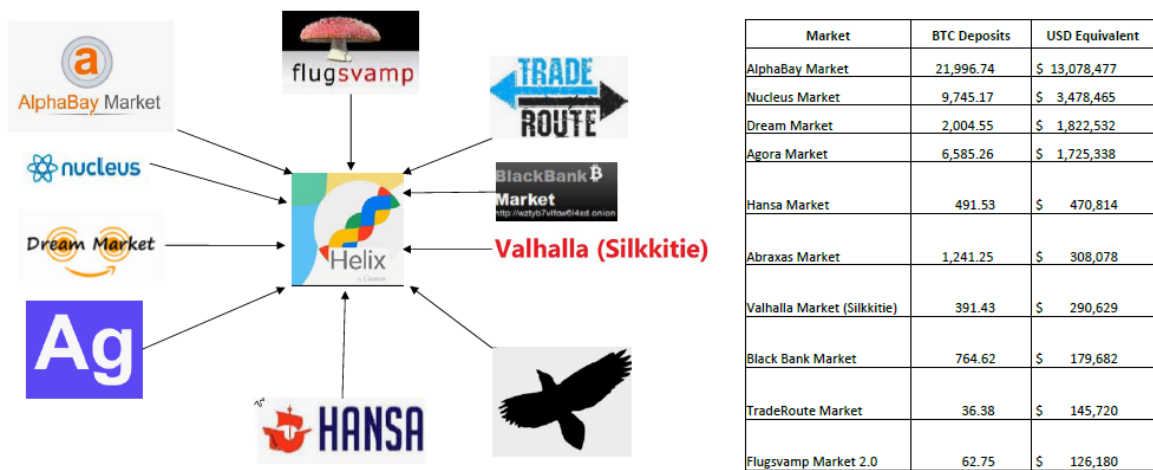
One of Helix’s most significant transaction counterparties was AlphaBay, whose customers frequently used Helix to launder their funds. AlphaBay was a darknet market which ran from in or about December 2014 through in or about July 2017, when the site was seized by law enforcement. At the time of the seizure, AlphaBay was the largest darknet marketplace in operation, offering a platform for customers to purchase a variety of illegal drugs, guns, and other illicit goods. In or about November 2016, the AlphaBay website recommended to its customers that they use a bitcoin tumbler service to “erase any trace of [their] coins coming from AlphaBay,” and provided an embedded link to the Tor address for Grams/Helix.

On or about November 8, 2016, a Federal Bureau of Investigation (FBI) employee acting in an undercover capacity from a location in the District of Columbia transferred bitcoin from an AlphaBay bitcoin wallet to Helix. Helix then exchanged the bitcoin for an equivalent amount of bitcoin, less a 2.5 percent fee, which was not directly traceable to AlphaBay.

The largest identifiable customers sending bitcoin to Helix were darknet markets selling

illegal goods and services, including AlphaBay, Agora Market, Nucleus, and Dream Market, and other Darknet markets. The figures for the funds sent *directly* from these and other darknet markets is significant. Investigators traced 43,319.68 bitcoin, valued at over \$21 million at the time of the transactions, straight from wallets on darknet marketplaces into Helix deposit addresses. Det. H'rg Ex. 5; 2/11/20 Tr. at 25:19-26:13. The top darknet deposit sources are displayed in the chart below:

Top 10 Depositors for Helix Were Darknet Markets



These figures capture only the *direct* transfers, on the Helix deposit side. When looking at indirect transfers, Helix received over \$73 million worth of bitcoin from darknet markets. The indirect transfers more comprehensively illustrate user activity. Commonly, darknet users will include one or more addresses between a darknet market withdrawal and a service deposit. For example, if a cocaine vendor on AlphaBay withdrew funds from AlphaBay to his own personal wallet on his computer, then sent the funds on to Helix several hours later, that transaction would not be included in the above figures of *direct* deposits. Rather, it would be considered an *indirect* transfer. Consideration of the volume of indirect transfers even further illuminates the scope of Helix’s money laundering operation.

The transfers from darknet markets to Helix largely equate to darknet drug vendors who are withdrawing their proceeds from the markets and sending it through Helix to clean the funds before they are cashed out at an exchange or otherwise spent. Darknet buyers would also use Helix to clean their funds before making a purchase on a darknet market. These transactions appear as deposits into Helix from—directly and indirectly—virtual currency exchanges. The funds would then be withdrawn from Helix and sent to darknet markets. The same blockchain analysis used to substantiate the deposit figures above indicates that of the money withdrawn from Helix, just under \$50 million was sent to a darknet market, including approximately \$18.9 million sent directly from Helix to the market with no intermediary addresses.

The defendant promoted the use of Helix as an intervening service for transfers between mainstream bitcoin exchanges and darknet markets. For example:

- In a Reddit comment first posted on March 23, 2015, and re-posted approximately a dozen times through 2017, the defendant instructed users how to check the “taint” on their bitcoin to ensure that their transactions on a bitcoin exchange could not be linked to their darknet market activity. The defendant provided an example in which “a user buys bitcoins on coinbase send to a tumbler and tells the tumbler to send to a market address Coinbase(wallet A) -> Tumbler (wallet B) -> Market (wallet C).” ECF No. 39, Ex. A (Reddit Comments by GramsAdmin-Excerpts). Coinbase is a popular cryptocurrency exchange.
- The defendant instructed a Reddit user: “You should send bitcoins like this coinbase->Tumber(Helix)->market. That is the fastest way and works.” ECF No. 39, Ex. A.
- The defendant instructed another Reddit user how to send funds from a Coinbase account to a darknet market through Helix: “You would enter the market address, then

you will be given an address to send the coins to. Send the coins from coinbase to the address you are given.” ECF No. 39, Ex. A.

f. The Defendant’s Deliberate Efforts To Evade Law Enforcement

The defendant frequently assured customers that he was taking extensive measures to protect them from law enforcement. As the defendant explained on Reddit, “we have no hot wallet, that is how they track the others. We have thousands of wallets, used only once. Every 2 weeks we delete and remove all the old wallets from the server, so if the server ever got seized they could not connect old wallets to helix.” Reddit, GramsAdmin, date : 2015-01-21 23:44:43 UTC. “Helix uses new addresses for each transaction so there is no way LE would [be] able to tell which addresses are helix addresses.” Det. Hr’g Ex. 14. The defendant further boasted, “if my site got seized They would not get me or the bitcoins” (referring to potential seizure by law enforcement) (date : 2014-11-07 00:01:57 UTC), indicating that he physically and virtually segregated the storage of his bitcoin private keys.

The defendant took great care to avoid detection and disruption by law enforcement. In Reddit comments, Harmon expressed concerns about his organization being infiltrated by a “UC,” or undercover law enforcement officer: “I don’t want any UC working for me. . . I really like the one guy. Can you guys think of any ways I could make him prove he wasn’t a UC? I would really like to keep him but I need to be sure.” Det. Hr’g Ex. 14.

The defendant used servers located overseas—including in China—to conceal his activity from law enforcement. He used fake names and changed servers repeatedly to avoid detection. The defendant assured users on Reddit that he used “hosting in non-us friendly countries” (referring to countries that are not friendly to U.S. law enforcement) that “don’t give your data to LE.” Reddit, GramsAdmin, date : 2015-01-14 06:50:04 UTC.

g. Related Services on Grams

While individual darknet markets had search functions, Grams allowed users to search for products across multiple darknet markets, without needing to know the Tor address of or create accounts on all of the different markets. To develop this functionality, the defendant had to visit the various marketplaces and write code and application programming interfaces (APIs) customized to each in order to enable this search platform. The illicit nature of these marketplaces was immediately apparent to visitors. The sites prominently displayed the narcotics being distributed. Furthermore, the operation of Grams' search engine often necessitated discussions with the administrators of the darknet marketplaces.

The defendant also ran a service through Grams called TorAds, through which he allowed vendors and others to purchase advertising placement on Grams. Another related service, GramsWords, functioned similarly to Google AdWords, allowing vendors to pay to have their advertisements or listings prominently displayed when Grams users searched for certain terms. For example, a cocaine vendor could pay to ensure that a Grams user searching for "cocaine" would see that vendor's listings displayed at the top of the search results. The advertising vendors dealt primarily in illegal narcotics.

C. The Defendant's Additional Relevant Conduct

Between 2014 and his arrest in 2020, the defendant engaged in a sophisticated series of money laundering and fraud sub-schemes to conceal the proceeds he earned from operating Grams/Helix. The defendant's primary source of income for the period of time covered by the indictment was the illicit proceeds earned from the operation of Helix. In order to spend these proceeds, originally obtained in the form of bitcoin, the defendant needed to further launder and legitimize them. This required a multifaceted scheme by the defendant that involved making

fraudulent misrepresentations to financial institutions, forging documents and submitting false documentation, and operating additional unlicensed money transmitting businesses to convert his bitcoin proceeds. The defendant also submitted false tax returns to conceal his proceeds from Helix and show legitimate income where none existed.

After shutting down Grams/Helix, the defendant overtly controlled other companies including Harmon Web Innovations (“HWI”), Coin Ninja, and an associated bitcoin payment app called DropBit. After Helix closed in 2017, the defendant launched a new business, “Coin Ninja,” in order to continue to launder his proceeds from Helix. Coin Ninja initially offered a bitcoin mixing service which purported to operate similarly to Helix but functioned on the clearnet and was not specifically tied to darknet markets. The frequently asked questions section of the Coin Ninja website, CoinNinja.io, described how the mixer worked and closely matched the process used by Helix. Coin Ninja never attracted a significant user base, and the defendant’s initial efforts to use the Coin Ninja brand to legitimize his Helix income was unsuccessful. At least two bitcoin exchanges flagged the defendant’s transactions as suspicious during the exchanges’ Know Your Customer (KYC) due diligence process. These exchanges questioned the defendant’s source of bitcoin. In response, the defendant indicated that the proceeds—which were in fact sourced from Helix – were earned through the defendant’s operation of Coin Ninja. After the defendant provided a description of Coin Ninja as a mixing service, both exchanges closed the defendant’s accounts.

Shortly thereafter, the defendant appeared to pivot Coin Ninja’s business model and publicly focus instead on the development of DropBit, a mobile application which purported to simplify the transfer of bitcoin from one person to another. The DropBit app was accessible through CoinNinja.com, rather than the CoinNinja.io that was used by the mixing service. By the time of the defendant’s arrest, Coin Ninja had multiple full-time employees who were

working in earnest to build and grow the DropBit platform. However, Coin Ninja still was not profitable; instead, the defendant continued to use Coin Ninja as a front to launder proceeds from the Grams/Helix activity.

The defendant also used his purported web development company, Harmon Web Innovations (HWI), as a front company to disguise the fiat currency proceeds resulting from the sale of bitcoin he obtained through the operation of Grams/Helix. The defendant advertised HWI publicly as a web development company involved in computer programming and web design work. In reality, the defendant used HWI as a front to conceal the fiat currency proceeds of bitcoin generated from Helix. The government determined that over 90% of the deposits into the defendant's HWI business bank accounts were sourced from the sale of bitcoin, which the defendant obtained from his operation of Grams/Helix. The defendant then transferred funds from the HWI accounts to fund his Coin Ninja business, described further below; pay himself a salary; and purchase assets, including real estate and cars.

The defendant provided false invoices to at least one financial institution portraying his repeated transactions with a bitcoin dealer as related to computer programming services, in order to legitimize the income. The defendant also included false information on his tax returns to legitimize the ill-gotten gains earned from the operation of Helix.

Ultimately, the defendant converted a portion of his Helix proceeds by operating his own small-scale virtual currency exchange business, offering exchanges through advertisements on LocalBitcoins, a popular peer-to-peer exchange platform, and through face-to-face transactions for cash. The defendant was not licensed for this activity. On numerous occasions, the defendant enlisted third parties to assist in his bitcoin sales. The defendant would arrange bitcoin sales through LocalBitcoins and then send other individuals as straw sellers to meet the buyers face-to-

face and sell the bitcoin in exchange for cash. The defendant provided specific instructions regarding how to transfer the cash as part of his money laundering scheme. The straw sellers would then provide the fiat proceeds to the defendant, either by giving the cash to the defendant in person, mailing cash to the defendant, sending the defendant funds via a financial transfer platform such as MoneyGram, or providing cash to a third party who would hold the cash at the defendant's direction.

D. Procedural History

On or about December 3, 2019, the defendant was charged by Indictment with violations of 18 U.S.C. § 1956(h) (Money Laundering Conspiracy), 18 U.S.C. § 1960(a) (Operating an Unlicensed Money Transmitting Business), and D.C. Code § 26-1023(c) (money transmission without a license). The defendant was arrested on or about February 6, 2020. Trial was set for September 13, 2021. The court held hearings on several pretrial motions, and a pretrial conference was held on July 30, 2021. On or about August 18, 2021, the defendant pleaded guilty to one count of Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h).

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

SENTENCING GUIDELINES

A. Statutory Maximums and Mandatory Minimums

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

18 U.S.C. § 3663A; and an obligation to pay any applicable interest or penalties on fines and restitution not timely made.

B. Sentencing Guidelines Calculation

As calculated in the Plea Agreement, and consistent with Probation's calculations, the offense level is as follows:

§ 2S1.1(a)(2)	Base offense level	8
§ 2B1.1(b)(1)(O)	More than \$250 million	+28
§ 2B1.1(b)(1)(i)	Knew funds were proceeds of or intended to promote drug offenses	+6
§ 2S1.1(b)(2)(C)	Defendant in business of laundering	+4
	Total Offense Level:	46
§ 3E1.1	Acceptance of Responsibility	-3
	Adjusted Offense Level:	43

At offense level 43 and Criminal History Category I, the defendant's pre-departure Guidelines range would be life imprisonment. The statutory maximum for money laundering conspiracy is 20 years.

C. Criminal History and Zero-Point Offender Status

Subsequent to the entry of the defendant's guilty plea on August 18, 2021, 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, he may be eligible for a 2-point reduction in offense level under § 4C1.1. Although the defendant entered his 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). If the defendant were

awarded the reduction, his adjusted offense level would be reduced to a level 41, which, with a Criminal History Category 1, results in a guidelines range of 324-405 months imprisonment.

However, the defendant has two prior convictions that were noted in the PSR—a 2009 conviction for operating a vehicle under the influence of alcohol or drugs, and a 2017 conviction for disorderly conduct. PSR (¶ 56-57). While this would not historically have impacted the defendant’s sentencing exposure, as he still falls within Criminal History Category I, it does make him ineligible for the zero-point offender reduction. The defense in its objections to the PSR argues that the defendant nonetheless meets the criteria at USSG § 4C1.1, and that the reduction would have been awarded but for Commentary 5 to USSG § 4A1.2. ECF No. 143 at 2-3. Commentary 5 states that “convictions for driving while intoxicated or under the influence ... are always counted without regard to how the offense is classified.” U.S.S.G. § 4A1.2, App. N. 5. Commentary 5 reflects a deliberate decision by the Commission to consider the gravity of convictions for driving while intoxicated or under the influence. The government thus agrees with Probation that the defendant is not eligible for a reduction as a zero-point offender. However, since the defendant’s guidelines range with or without the zero-point offender reduction still exceeds the 20-year statutory maximum for money laundering conspiracy, the potential reduction does not meaningfully impact the government’s sentencing recommendation.

SENTENCING RECOMMENDATION

A. Sentencing Factors

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

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

a. The Nature and Circumstances of the Offense

The nature and circumstances of the defendant's offense are gravely serious. The details are set forth at length above. Online drug trafficking on the darknet remains a significant societal threat and concern. Darknet drug markets connect drug dealers with new audiences across the globe. In addition to fueling the trade of illegal substances, they may create added risk of harm to novice drug users. With the click of a button, a user can find any drug imaginable, at exceptional potencies. In at least some cases, this has contributed to young teens experimenting with hard drugs, at times with devastating consequences. One of law enforcement's most effective measures in identifying darknet market operators and online drug dealers is by tracing their cryptocurrency payments. Mixing services like the defendant's prevent law enforcement from tracing those funds, and thus facilitate and perpetuate the online drug trade. They also frustrate efforts by law-abiding virtual currency exchanges which seek to identify, report, and/or reject payments tied to drug trafficking and other criminal activities. Hundreds of drug dealers were able to operate for years with greater impunity as a result of the defendant's actions. The defendant personally facilitated hundreds of millions of dollars of illicit fund movement, much of which was tied to the online drug trade. And the defendant developed his service with exacting attention to detail and the utmost concern for operational security, so that he and his criminal customers would not be caught. The massive scale, extraordinary sophistication, and continuous and deliberate nature of the defendants' criminal actions weigh in favor of a strong sentence.

These actions caused significant harm. As the D.C. Circuit and other courts have recognized, the laundering of illegal proceeds represents a distinct injury to society—concealing and facilitating the underlying crimes and frustrating law enforcement's ability to detect illicit abuse of the financial system. *See United States v. Braxtonbrown-Smith*, 278 F.3d 1348, 1355

(D.C. Cir. 2002) (“Section 2S1.1 measures the harm to society that the money laundering causes to law enforcement’s efforts to detect the use and production of ill-gotten gains”) (quoting *United States v. Allen*, 76 F.3d 1348, 1369 (5th Cir. 1996)); *United States v. Martin*, 320 F.3d 1223, 1227 (11th Cir. 2003) (“Unlike the 1998 Sentencing Guidelines for theft or fraud, which compute the offense level according to the ‘loss’ incurred by the victim, see U.S.S.G. §§ 2B1.1(b)(1), 2F1.1(b)(1), the 1998 Sentencing Guidelines for money laundering compute the base offense level according to the ‘value of the funds,’ U.S.S.G. § 2S1.1(b)(2). This is so because the harm from such a transaction does not generally fall upon an individual, but falls upon society in general. Each unlawful monetary transaction harms society by impeding law enforcement’s efforts to track ill-gotten gains.”) (cleaned up).

b. The History and Characteristics of the Defendant

The defendant does not have a significant criminal history apart from the Helix conspiracy. He is a skilled computer programmer and website developer, possessing marketable skills that make his decision to pursue a criminal livelihood all the more troubling. That said, given the defendant’s remorse and acceptance of responsibility, his technical skills and abilities will position him well to obtain lawful employment and make a successful reintegration into society following his sentence.

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

1. Seriousness of Offense

As described further above, the defendant’s criminal conduct was serious and extensive. A significant period of incarceration is warranted to reflect the gravity of the offense.

2. General Deterrence

General deterrence should be an important consideration for the Court when sentencing the defendant. Mixers are one of the most significant challenges facing law enforcement working in the cryptocurrency space today. Over the past several years, the U.S. government and other countries have taken public action against over a half dozen criminal cryptocurrency mixing platforms, such as Helix, Bitcoin Fog, BestMixer, Sinbad, Tornado Cash, and Samourai Wallet. Many of those actions have involved well-publicized arrests and criminal prosecutions. Yet criminals continue to set up mixing services, and illicit actors—including hackers, ransomware actors, darknet market operators, investment fraudsters, child sexual abuse material producers, and North Korea’s lucrative crypto heist perpetrators—continue to flock to these services. Mixers and related services have grown more sophisticated, taking advantage of anonymity-enhanced cryptocurrencies with non-transparent blockchains, as well as using decentralized finance platforms and smart contracts, to move funds. This makes it increasingly difficult for law enforcement to investigate criminal activity involving cryptocurrency, identify those responsible, shut down the criminal enterprises, return stolen funds, and protect future victims.

Many criminals believe that they can outsmart law enforcement and get away with their crimes; that belief is particularly pernicious in the area of cyber and cryptocurrency-related crimes. Criminals engaging in a wide array of underlying illicit activity turn to cryptocurrency to help them profit from their crimes while concealing their involvement in the criminal activity. For years, the defendant was able to conceal his activity; his technical abilities and laundering skills made it extremely difficult to tie anything back to him. Law enforcement was able to identify the defendant only through significant effort by skilled personnel. Such investigations are lengthy and resource-intensive, and the government lacks the personnel and resources needed to successfully

investigate every complex scheme. A sentence of incarceration in this matter will send a needed message to other crypto criminals who might otherwise believe they can commit crimes with impunity.

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

While general deterrence weighs in favor of a sentence of significant incarceration, it is also important to take into account the defendant’s decision to cooperate and provide substantial assistance to the government’s law enforcement efforts. The defendant took full responsibility for his actions. As discussed in the accompanying sealed filing, the defendant’s assistance has benefitted numerous investigations. The Court, in fashioning an appropriate sentence, should

weigh both the need to provide general deterrence to other would-be crypto money launderers, as well as the need to encourage other defendants to cooperate as this defendant has done.

3. Specific Deterrence and Need To Protect the Public

The defendant's acceptance of responsibility, sincere remorse, and substantial assistance to the government suggest that his risk of recidivism is low. Over a decade has passed since the defendant launched Grams in 2014. Law enforcement agents and undersigned counsel have spent time with the defendant related to his debriefing and cooperation and have observed a stark contrast between the online messages from GramsAdmin quoted above and the defendant's current demeanor, tone, and approaches to issues.

The sentence in this case should serve as a reminder that a return to crime carries the risk of a serious punishment. If the defendant were to take what he has learned from this prosecution and incorporate it into a future money laundering scheme, he would be even better-equipped to conceal his activity while monetizing his crimes. However, the government believes that the defendant will be able to use his considerable skills for legitimate ends, and hopes that he will make positive contributions to the tech and anti-money laundering industries following his sentence.

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).

A closely analogous case is *United States v. Sterlingov*, D.D.C. No. 21-cr-395 (RDM), involving a defendant who operated another darknet cryptocurrency mixer, Bitcoin Fog, which laundered approximately \$400 million in largely illicit darknet transactions. Sterlingov was convicted at trial of Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h); “Sting” Money Laundering, in violation of 18 U.S.C. § 1956(a)(3)(A); Operating an Unlicensed Money Transmitting Business, in violation of 18 U.S.C. §§ 1960(a) & 2; and Operating an Unlicensed Money Transmitting Business, in violation of D.C. Code § 26-1023(c). Sterlingov is scheduled for sentencing before Judge Randolph Moss on November 8, 2024; his actual sentence is not yet known but should be available prior to Mr. Harmon’s sentencing hearing. Based on strikingly similar offense conduct—as well as certain aggravating factors, including Sterlingov’s lack of remorse and his perjury at trial—the government is recommending that he be sentenced to a term of imprisonment of 30 years. 21-cr-395, ECF No. 314.

While Sterlingov’s offense conduct is comparable to that in this case, he and Mr. Harmon are not similarly situated for the purposes of sentencing. Mr. Harmon took full responsibility for his actions, pleaded guilty, expressed genuine remorse, and cooperated extensively with the government—including by testifying as a government witness in the *Sterlingov* trial and by assisting in other matters, as further detailed in the government’s sealed addendum.

e. Consideration of Time in Home Confinement

The defendant is not eligible for formal time served credit for the time he has spent on home confinement since March 2020. Courts have consistently rejected efforts by defendants to

claim credit for time spent in pretrial home confinement. *See, e.g., Brown v. Warden Fort Dix FCI*, 789 Fed. App'x 291 (3d Cir. 2020) (affirming denial of relief under § 2241 where petitioner sought sentence credit for home confinement); *Cook v. Wilson*, 2020 U.S. Dist. LEXIS 131976, 2020 WL 4284583, at *3 (N.D. Tex. Jul. 24, 2020) (holding that petitioner was not entitled to sentence credit for home confinement “no matter how restrictive the conditions”); *Purcell v. Joseph*, 2022 U.S. Dist. LEXIS 58894, 2022 WL 958388 (N.D. Fla. Feb. 23, 2022) (holding that petitioner was not entitled to credit for time spent released on bond to home confinement); *Mays v. Hudson*, No. 22-3142-JWL, 2022 U.S. Dist. LEXIS 169016, at *5 (D. Kan. Sep. 19, 2022) (“Under *Koray* and subsequent case law, it is clear that petitioner is not entitled to the sentence credit for time spent in home confinement.”).

However, it is significant that the defendant has spent 56 months on home confinement and has exhibited exemplary behavior on pretrial release during that time. This lengthy period of compliance with home confinement gives the government confidence that the defendant poses a low risk of recidivism, and it is factored into the government’s recommendation for a below-guidelines period of additional incarceration.

f. Additional Considerations Surrounding the Defendant’s Cooperation

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

g. Restitution and Fines

The government is not seeking restitution. While Helix caused enormous harm—in particular by facilitating drug transactions—it is not the kind of harm that is readily quantifiable through restitution.

The government agrees with Probation that the defendant is unable to pay a fine. PSR ¶ 131.

B. Forfeiture

a. Property Subject to Forfeiture

Under Count One of the Indictment—money laundering conspiracy encompassing the entire scope of Helix’s operations—the defendant is required to forfeit “any property, real or personal, involved in such offense, or any property traceable to such property.” 18 U.S.C. § 982(a)(1). Property “involved in” a money laundering offense includes “the money or other property being laundered (the corpus), any commissions or fees paid to the launderer, and any property used to facilitate the laundering offense.” *United States v. Puche*, 350 F.3d 1137, 1153 (D.C. Cir. 2003) (internal citation omitted). As the D.C. Circuit has observed, “[t]he statute sweeps broadly because ‘money laundering largely depends upon the use of legitimate monies to advance or facilitate the scheme.’” *United States v. Bikundi*, 926 F.3d 761, 793 (D.C. Cir. 2019) (quoting *Puche*, 350 F.3d at 1153).

Property “involved in” a Bitcoin mixer such as Helix includes all of the funds that flowed through it. To be sure, Helix was designed, operated, and marketed to darknet drug traffickers, and the largest identifiable share of its transactions are traceable to known darknet markets. But as this Court has previously explained:

Where, as here, the conspiracy takes the form of a business, all funds flowing through the business that “bankroll” or otherwise facilitate the alleged conspiracy

are “involved in” it. Thus, any untainted funds used as “seed” money to start Helix or to run Grams, Helix’s companion service, were used to further Helix’s core business, which was cleaning bitcoins used in Darknet drug purchases. Finally, to the extent some of Helix’s business came from transactions unrelated to drug activity, the fees from those transactions remain forfeitable because the evidence suggests that “the business as a whole was overwhelmingly devoted to” transactions from Darknet markets, which, in turn, overwhelmingly deal in drugs.

United States v. Harmon, 474 F. Supp. 3d 76, 85 n.5 (D.D.C. 2020) (internal citations omitted); *cf. United States v. Braxtonbrown-Smith*, 278 F.3d 1348, 1353 (D.C. Cir. 2002) (“[M]oney need not be derived from crime to be ‘involved’ in it; perhaps a particular sum is used as the bankroll facilitating the fraud.”) (quoting *United States v. \$448,342.85*, 969 F.2d 474, 476 (7th Cir. 1992)).

This broad understanding of property “involved in” a money laundering business is particularly apt in the case of a Bitcoin mixer, where the pool of Bitcoin deposits quite literally facilitates the laundering process. For just this reason, in the *Sterlingov* case, Judge Moss found that property “involved in” the operation of Bitcoin Fog, another Bitcoin mixer, included the total amount of funds deposited into the mixer:

[T]he very essence of Bitcoin Fog’s service was commingling—that is, mixing—funds. Dkt. 106-1 at 2 (“[U]sing our service you mix up your bitcoins in our own pool, with other users’ bitcoins, and get paid back to other accounts from our mixed pool, which, if properly done by you can eliminate any chance of finding your payments and mak[e] it impossible to prove any connection between a deposit and a withdraw[al] inside our service.”). It anonymized bitcoins by combining them with other bitcoins, and, importantly, without a sufficiently large pool of bitcoins to mix, it would not have worked. *Id.* Each deposit of funds into Bitcoin Fog therefore contributed to its efficacy and facilitated its activities—both lawful and unlawful.

United States v. Sterlingov, 2023 WL 2387759, at *7 (D.D.C. Mar. 6, 2023). Thus, “even if the funds at issue were first obtained through legal means, *Sterlingov* would have known that by combining them with the rest of the funds in Bitcoin Fog’s pool, he was facilitating Bitcoin Fog’s criminal activities.” *Id.* The same logic applies to Helix. Helix was overwhelmingly devoted to facilitating Darknet drug transactions, but even supposedly “clean” deposits still facilitated the

money laundering conspiracy by providing a pool of Bitcoin to bankroll and facilitate Helix's mixing operations.

b. Forfeiture Money Judgment

The government is seeking entry of the attached Amended Preliminary Order of Forfeiture. Consistent with the defendant's plea agreement and the Preliminary Order of Forfeiture entered at sentencing, the government is seeking a forfeiture money judgment in the amount of \$311,145,854, representing the dollar equivalent of "laundering transactions totaling at least 354,468 bitcoins (BTC)" for which the defendant has acknowledged responsibility, ECF No. 122 (Plea Agreement), at 2-3. *See United States v. Roberts*, 660 F.3d 149, 166 (2d Cir. 2011) ("[T]he law does not demand mathematical exactitude in calculating the proceeds subject to forfeiture . . . because the purpose of forfeiture is punitive rather than restitutive, district courts are not required to conduct an investigative audit to ensure that a defendant 'is not deprived of a single farthing more than his criminal acts produced.'") (quoting *United States v. Lizza Indus., Inc.*, 775 F.2d 492, 498 (2d Cir.1985)); *United States v. Del Giudice*, 594 F. Supp. 3d 998, 1006 (N.D. Ill. 2022) (explaining that the calculation of the "total money judgment for [the] forfeiture allegation . . . must be reasonable but not exact").

c. Specific Properties Subject to Forfeiture

In addition to a forfeiture money judgment, the government is seeking forfeiture of specific properties that were derived from the defendant's fees and proceeds from operating Helix and are therefore considered property "involved in" Count One. At the time of the defendant's plea agreement, he consented to entry of the Consent Preliminary Order of Forfeiture, ECF No. 125.

The government is now seeking an Amended Preliminary Order of Forfeiture in order to update the list of specific properties subject to forfeiture and to adjust the crediting mechanism, as

described in further detail below. The government's proposed order now includes an Amended Attachment A listing each of the specific properties subject to forfeiture. This list includes the addition of \$345,000.00, representing the defendant's former interest in Airfill Hodling AB ("Airfill"), which he acquired using Helix proceeds and voluntarily liquidated pursuant to the Plea Agreement, *see* ECF No. 122 (Plea Agreement), at 11; it includes additional cryptocurrency assets traceable to Helix which were seized from the possession of the defendant's brother, Gary Harmon, but which were not forfeited in *United States v. Gary James Harmon*, 21-cr-433 (BAH); and it makes certain minor clerical adjustments. The Amended Preliminary Order of Forfeiture is consistent with the Plea Agreement and well-supported by the record.

d. Crediting of Specific Properties Toward the Forfeiture Money Judgment

Finally, the Amended Preliminary Order of Forfeiture provides that the net value of the forfeited specific properties will be credited toward the defendant's forfeiture money judgment. *See United States v. Ponzo*, 2014 WL 3893790, at *5 (D. Mass. Aug. 6, 2014) ("The Court is also mindful of the fact that, under Fed. R. Crim. P. 32.2(e), the value of the specific assets found forfeitable by the jury will be applied to the money judgment as will any assets that are located and identified after the entry of this Order."); *Bikundi*, 926 F.3d at 792 (affirming forfeiture order that "ordered [two co-defendants] to forfeit specific pieces of property, including cash, vehicles, jewelry, and real property, with the values of the forfeited properties to be credited on a fifty-fifty basis toward each of their forfeiture money judgments"). "This eliminates any concern" that the total value of the forfeited property will exceed the money judgment amount and subject the

defendant to a “double forfeiture.” *United States v. Tardon*, 56 F. Supp. 3d 1309, 1320 (S.D. Fla. 2014).

The government notes that the defendant’s brother, Gary Harmon, fraudulently stole approximately 712.6003 BTC from wallets originally seized in this case. Those wallets belonged to the defendant and contained funds derived from the defendant’s fees and proceeds from operating Helix. *See United States v. Gary James Harmon*, 21-cr-433 (BAH), ECF No. 46 (Statement of Offense and Related Conduct), ¶¶ 10, 15, 19-24. As a result of the plea and sentencing in Gary Harmon’s case, the government was able to recover cryptocurrencies and other properties valued (at the time of sentencing) at more than \$20 million. *See id.*, ECF No. 49 (Consent Preliminary Order of Forfeiture). Because those properties were ultimately derived from property “involved in” the Helix money laundering conspiracy, the Amended Preliminary Order of Forfeiture provides that the government’s net proceeds obtained from the forfeitures in the *Gary Harmon* case should also be credited toward the money judgment in this case.

Due to the increase in the market value of Bitcoin and other cryptocurrencies since the conduct giving rise to forfeiture occurred, the government anticipates that the net value of the specific properties seized in this case will exceed the defendant’s forfeiture money judgment.

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 96 months of imprisonment to be followed by 3 years of supervised release, imposition of a money judgment described above, and entry of an Amended Preliminary Order of Forfeiture to be filed with the Court.

Respectfully submitted,
MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar No. 481052

BY: /s/ Christopher B. Brown
Christopher B. Brown, D.C. Bar No. 1008763
Special Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, DC 20530
(202) 353-0018
Christopher.Brown8@usdoj.gov

/s/ Catherine Alden Pelker
C. Alden Pelker, Maryland Bar
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007
Catherine.Pelker@usdoj.gov