UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

– v. –

SHAKEEB AHMED,

Defendant.

S1 23 Cr. 340 (VM)

THE GOVERNMENT'S SENTENCING MEMORANDUM REGARDING DEFENDANT SHAKEEB AHMED

DAMIAN WILLIAMS
United States Attorney
Southern District of New York
26 Federal Plaza
New York, New York 10278

David R. Felton
Kevin Mead
Assistant United States Attorneys
- *Of Counsel* -

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA **– v. –** **SHAKEEB AHMED,** **Defendant.**	**S1 23 Cr. 340 (VM)**

GOVERNMENT'S SENTENCING MEMORANDUM REGARDING DEFENDANT SHAKEEB AHMED

The Government respectfully submits this memorandum in advance of the sentencing of defendant Shakeeb Ahmed, currently scheduled for Friday, April 12, 2024, at 10:00 a.m. As set forth in the Presentence Investigation Report ("PSR") and in the parties' plea agreement, the defendant's applicable sentencing range would otherwise be 70 to 87 months' imprisonment but, pursuant to U.S.S.G. § 5G1.1(a), because the statutory maximum sentence is 60 months, the Guidelines sentence is 60 months (the "Stipulated Guidelines Sentence"). For the reasons explained below, the Government submits that, after balancing Ahmed's acceptance of responsibility in admitting to both of his hacks and surrendering his crime proceeds, against, among other factors, the seriousness of his offense conduct, the significant damage that he inflicted on his victims, and the critical need to achieve general deterrence in this precedential, first-of-its-kind conviction for the hack of a smart contract, a slightly below Guidelines variance sentence of 48 months would be sufficient but not greater than necessary to meet the goals of sentencing.

I. BACKGROUND

A. **Offense Conduct**

Crypto Exchange Attack Overview

In July 2022, Ahmed, who was residing in Manhattan, orchestrated and executed a scheme to fraudulently obtain approximately $9 million worth of cryptocurrency (the "Attack") from victim [redacted],[1] a decentralized cryptocurrency exchange (the "Crypto Exchange"), including cryptocurrency deposited by the Crypto Exchange's users. Ahmed conducted the Attack by exploiting a vulnerability in the Crypto Exchange and inserting fake pricing data to fraudulently generate millions of dollars' worth of inflated fees that Ahmed did not in fact earn, but which Ahmed was able to withdraw from the Crypto Exchange in the form of cryptocurrency, thereby defrauding the Crypto Exchange and its users, whose cryptocurrency Ahmed had fraudulently obtained. At the time of the Attack, Ahmed was employed as a senior security engineer at a leading international technology company unrelated to the Crypto Exchange. His resume reflected skills in, among other things, reverse engineering smart contracts and blockchain audits, which are some of the specialized skills Ahmed used to execute the Attack. (PSR ¶ 7).

After the Attack, Ahmed laundered the stolen cryptocurrency through a series of transactions designed to conceal the source and owner of the funds, including through: (a) conducting token-swap transactions; (b) "bridging" fraud proceeds from the Solana blockchain over to the Ethereum blockchain; (c) exchanging fraud proceeds into Monero, an anonymized and particularly difficult cryptocurrency to trace; and (d) using overseas cryptocurrency exchanges.

[1] [redacted]

(PSR ¶ 8). After the Attack, Ahmed also searched online for information about, among other things, the Attack, his own criminal liability for the Attack, criminal defense attorneys with expertise in similar cases, law enforcement's ability to successfully investigate the Attack, and fleeing the United States to avoid criminal charges. (PSR ¶ 9).

After the Attack and once in possession of the stolen fees in cryptocurrency, Ahmed decided to return a substantial portion of the fraud proceeds to the Crypto Exchange, and to provide information to the Crypto Exchange about how he accomplished the Attack, if the Crypto Exchange refrained from referring his fraudulent scheme to law enforcement. Ahmed ultimately kept approximately $1.5 million worth of fraudulently obtained cryptocurrency from the Crypto Exchange. (PSR ¶ 10).

Background on the Crypto Exchange

The Crypto Exchange was incorporated in the Asia-Pacific region and operates on the Solana blockchain. At all relevant times, the Crypto Exchange was a decentralized exchange that allowed users to deposit and exchange different kinds of cryptocurrencies. A decentralized exchange does not rely on any sort of entity or company to act as an intermediary between buyers and sellers. Instead, it relies on "smart contracts" associated with "liquidity pools," analogous to pots of money, in order to serve as an "automated market maker." A "smart contract" is a computer program that runs on a blockchain. An "automated market maker" controls a "liquidity pool" of different types of cryptocurrencies, and uses a smart contract to buy and sell the cryptocurrencies in that liquidity pool. (PSR ¶ 11).

Specifically, the Crypto Exchange was a concentrated liquidity market maker, meaning that it allowed individuals or entities depositing cryptocurrency into its liquidity pools—referred to as "liquidity providers"—to set the price ranges—referred to as "ticks"—at which the individuals' cryptocurrency in the liquidity pool would be traded. For example, an individual who deposits 100 Ether into the concentrated liquidity market maker's liquidity pool can control the range at which the 100 Ether is offered for liquidity, so the individual might, for example, provide the 100 Ether subject to the limitation that it only be traded when the price is between 0.9 and 1.1 Bitcoin. In this example, the liquidity provider would profit by receiving a percentage of the transaction fees generated if the specified price range was triggered. In this example, 0.9 Bitcoin would be the lower tick, and 1.1 Bitcoin would be the upper tick. (PSR ¶ 12).

At all relevant times, the Crypto Exchange paid fees to liquidity providers who deposited cryptocurrency into a liquidity pool. Those fees were calculated by a smart contract that took into account, among other things, the total amount of cryptocurrency the liquidity provider deposited and the actual amount of liquidity that was provided based on the price ranges selected by the liquidity provider. In essence, the greater the amount of cryptocurrency and liquidity provided, the higher the fee the liquidity provider could earn. More broadly, larger cryptocurrency deposits on the Crypto Exchange limit price volatility and increase liquidity. (PSR ¶ 13).

One of the inputs into the smart contract that calculated those fees was referred to as a "tick account." The tick accounts were owned and controlled by the Crypto Exchange—in other words, the blockchain showed that the owner of the tick accounts was the Crypto Exchange, and not any user or other third party. The tick accounts contained data about, among other things, how much liquidity all liquidity providers had provided for a particular price range, or tick. Users could not create or own tick accounts. (PSR ¶ 14).

Another input into the smart contract that calculated the fees was referred to as a "position account." Position accounts kept track of a user's share in a liquidity pool. In contrast to a tick account, which users could not create, the Crypto Exchange was set up to allow any user to create a "position account." Position accounts and tick accounts contained different types of data, but the general format of the two accounts was similar. As structured by the Crypto Exchange, both tick accounts and position accounts were listed as owned by the Crypto Exchange on the blockchain, even though position accounts could be created by a user. Ahmed exploited this vulnerability during the Attack. (PSR ¶ 15).

The Attack on the Crypto Exchange

To carry out the Attack, Ahmed, among other things: (a) the day before the Attack, conducted a series of test transactions of nominal value with the Crypto Exchange to obtain tick data and locate system vulnerabilities; (b) created at least two accounts that were *not* tick accounts; (c) supplied one of these non-tick accounts with fake price-tick data; and (d) carefully structured and designed these non-tick accounts to nonetheless falsely appear as authentic tick accounts. In other words, Ahmed used at least two non-tick accounts that he intentionally created and designed to masquerade as tick accounts (the "Fake Tick Accounts") to fraudulently cause the Crypto Exchange's smart contract to accept them as legitimate tick accounts. As described below, Ahmed used one such Fake Tick Account (the "First Fake Tick Account") to generate millions of dollars of inflated fees based on the fake price-tick data he supplied, and the other Fake Tick Account (the "Second Fake Tick Account") to withdraw millions of dollars' worth of cryptocurrency. (PSR ¶ 16).

On July 2, 2022, Ahmed created the First Fake Tick Account and fraudulently caused the Crypto Exchange's smart contract to accept it as authentic. Ahmed entered fake price-tick data into the First Fake Tick Account in order to fraudulently cause the Crypto Exchange's smart contract to calculate that Ahmed had provided more liquidity to the pool than he had actually contributed, which generated large fees for Ahmed that he had not legitimately earned. In other words, the Crypto Exchange's users legitimately earn fees based on how much cryptocurrency they provide to the liquidity pool in relation to pool-wide data. By entering fake price-tick data into the First Fake Tick Account, Ahmed used fake data to make it falsely appear to the Crypto Exchange that Ahmed had provided more liquidity to the pool than he actually had, and thus, Ahmed was able to fraudulently generate fees for himself to which he was not entitled. In so doing, Ahmed defrauded both the Crypto Exchange and its users. (PSR ¶ 17).

To further the Attack, Ahmed took out a series of cryptocurrency "flash loans" worth tens of millions of dollars from a cryptocurrency lending platform (the "Crypto Lender"). A "flash loan" is an uncollateralized cryptocurrency loan without borrowing limits that is taken out and repaid in a single transaction, and can be used in situations where an individual sees an opportunity to immediately profit on the blockchain. (PSR ¶ 18).

Over a period of several hours on July 2 and 3, 2022, Ahmed deposited the funds from the flash loans into the Crypto Exchange's liquidity pools, withdrew the funds, claimed a falsely inflated percentage of the flash loans as fees from the Crypto Exchange through his deceptive use of the First Fake Tick Account, and then repaid the flash loans to the Crypto Lender. In total, as part of the Attack, Ahmed took out at least 21 flash loans from the Crypto Lender and used to them to generate falsely inflated fees from five separate liquidity pools controlled by the Crypto Exchange. (PSR ¶ 19).

As part of the Attack, Ahmed also needed to withdraw the flash loan money that he had deposited into the liquidity pool—the principal—and return it to the Crypto Lender. In order to process a withdrawal of the principal, the Crypto Exchange's smart contract required a tick account that was listed as owned by the Crypto Exchange on the blockchain, and that contained data matching the tick data from the fee-claiming process. To satisfy this requirement, Ahmed created the Second Fake Tick Account, a position account—listed as owned by the Crypto Exchange—and manipulated its data to closely resemble a tick account. Specifically, Ahmed made a series of cryptocurrency deposits in specific amounts and in a specific order, in order to manipulate the data in the Second Fake Tick Account so that it contained data that matched certain of the data in the First Fake Tick Account. By doing this, Ahmed was able to fraudulently cause the Crypto Exchange's smart contract to treat Ahmed's position account—the Second Fake Tick Account—as a legitimate tick account. Ahmed then used the Second Fake Tick Account to withdraw the principal he owed and returned it to the Crypto Lender. (PSR ¶ 20).

An example of how Ahmed used the Fake Tick Accounts and one of the flash loans to defraud the Crypto Exchange is described below. Because each flash loan must be taken out and repaid as part of a single transaction on the blockchain, each of the following events together occurred as a single transaction conducted by Ahmed:

a. On July 2, 2022, Ahmed took out a flash loan from the Crypto Lender of approximately 840,000 PAI (Parrot) ("PAI"). PAI is a digital stablecoin worth approximately one dollar.

b. Ahmed deposited the approximately 840,000 PAI into a liquidity pool ("Pool-1") controlled by the Crypto Exchange that covered exchanges between PAI and a second cryptocurrency: USDC (USD Coin) ("USDC"). Like PAI, USDC is a digital stablecoin worth approximately one dollar.

c. Ahmed used the First Fake Tick Account, which contained fake price-tick data supplied by Ahmed, to claim inflated fees of approximately 1,133.93 PAI and 120.14 USDC.

d. Ahmed then used the Second Fake Tick Account to withdraw his principal of 840,000 PAI.

e. Ahmed repeated the cycle four more times with the same flash loan. Each time, he redeposited the 840,000 PAI into Pool-1, claimed inflated fees of approximately 1,133.93 PAI and 120.14 USDC through his use of the First Fake Tick Account, and withdrew his principal of 840,000 PAI through his use of the Second Fake Tick Account.

f. After five cycles, Ahmed returned the principal of 840,000 PAI to the Crypto Lender, plus a small fee to the Crypto Lender, and kept falsely inflated fees from the Crypto Exchange totaling approximately 5,669.65 PAI and 600.7 USDC. (PSR ¶ 21).

Based on approximate U.S. dollar conversions of the cryptocurrency valuations at the time (around July 2, 2022), Ahmed ultimately claimed approximately $9 million in cryptocurrency as falsely inflated fees from 21 flash loans based on the falsified data in the First and Second Fake Tick Accounts. (PSR ¶ 22). After the Attack, the Crypto Exchange initiated a plan to compensate the users Ahmed had victimized. (PSR ¶ 23).

Ahmed's Post-Attack Laundering of Stolen Fees

After Ahmed fraudulently obtained inflated cryptocurrency fees in the Attack, he laundered the fraud proceeds through a series of transactions in order to conceal the nature, location, source, and his control of the stolen funds. Ahmed engaged in the following laundering transactions, among others:

a. In July 2022, after the Attack, Ahmed conducted dozens of transactions exchanging one cryptocurrency token for another.

b. In July 2022, after the Attack, Ahmed "bridged" fraud proceeds across one blockchain over to another. A bridge contract is a mechanism to transfer cryptocurrency from one blockchain to another.

c. In July 2022, after the Attack, Ahmed laundered fraud proceeds through a swap aggregator to other wallets on the Solana blockchain. Swap aggregators aggregate liquidity from across different decentralized exchanges to work out more favorable crypto prices for decentralized exchange traders.

d. On November 5, 2022, Ahmed exchanged fraud proceeds into the cryptocurrency Monero, an anonymized and particularly difficult cryptocurrency to trace.

e. In May 2023, Ahmed laundered fraud proceeds through overseas cryptocurrency exchanges. (PSR ¶ 24).

Post-Attack Communications With the Crypto Exchange

On July 3, 2022, almost immediately after the Attack, the Crypto Exchange initiated public communications on the blockchain with the unidentified "hacker" of the Crypto Exchange (in actuality, Ahmed) in order to seek the return of the stolen funds. In these public statements on the blockchain, the Crypto Exchange indicated, among other things, that it would refer the Attack to law enforcement if the stolen funds were not returned and offered to pay the then-unidentified hacker $800,000 for the return of all the stolen funds. (PSR ¶ 25).

On July 6, 2022, a few days after the Attack, Ahmed, using an encrypted email service based overseas, contacted the Crypto Exchange and stated that he would return a portion of the stolen funds if the Crypto Exchange agreed not to refer the Attack to law enforcement for investigation. At the time, Ahmed was in possession of approximately $9 million in stolen funds. Specifically, Ahmed told the Crypto Exchange that it was in a "tough spot" and stated that he would keep approximately $2.5 million of stolen cryptocurrency, noting that he would return of the remainder of the stolen funds to the Crypto Exchange on the condition that it not refer his conduct to law enforcement. (PSR ¶ 26).

In response, also on July 6, 2022, the Crypto Exchange restated its original figure of $800,000, noting that it was "starting to apply for legal support and in that case it wouldn't take long to find you" and "[o]therwise, you may face prosecution and likely lose everything." (PSR ¶ 27).

On July 7, 2022, Ahmed indicated that he intended to keep $1.8 million of the stolen cryptocurrency and stated, for the first time, that he would provide, in substance and in part, details on two purported vulnerabilities in the Crypto Exchange's platform and how to improve the Crypto Exchange's code. In doing so, Ahmed told the Crypto Exchange that its post-Attack predicament was a "nightmare scenario." Later that same day, Ahmed returned all but approximately $1.5 million of the fraudulently obtained cryptocurrency to the Crypto Exchange. The next day, on

July 8, 2022, Ahmed provided information about the Crypto Exchange's technical vulnerabilities. (PSR ¶ 28).

Ahmed's Post-Attack Internet History

On July 5, 2022, just two days after the Attack and before he had communicated with the Crypto Exchange, Ahmed visited or searched for information about the Attack itself on the internet. For example:

a. Ahmed searched for the term "defi hack."

b. Ahmed visited a news article with the title, "[Crypto Exchange] Vulnerability Causes DeFi Clients to Lose Millions."

c. Ahmed visited a news article with the title, "Why Expensive Crypto Hacks Are The Cost of Doing Business in DeFi."

d. Ahmed also visited several pages on the Crypto Exchange's website. (PSR ¶ 29).

On July 5, 2022, still before he had communicated with the Crypto Exchange, Ahmed visited a news article describing a $10 million bounty that a cryptocurrency bridging platform had paid. That same day, Ahmed visited or searched for information about white-collar criminal defense attorneys with expertise in cryptocurrency. (PSR ¶ 30).

Ahmed used a particular virtual private network ("VPN-1") to conceal his Internet Protocol address while he executed the Attack. On July 27, 2022, and continuing into August 2022, Ahmed visited or searched for information in an attempt to confirm that VPN-1 could not be traced back to him. From July 2022 through December 2022, Ahmed visited or searched for information about whether he was likely to be prosecuted for the Attack. In particular:

a. On July 5, 2022, still before he had communicated with the Crypto Exchange, Ahmed searched for the term "embezzled."

b. On August 6, 2022, Ahmed searched for the term "defi hacks fbi."

c. On August 8, 2022, Ahmed searched for the term "defi hacks prosecution."

d. On August 16, 2022, Ahmed searched for "wire fraud," which is one of the charges in this Indictment.

e. On August 16, 2022, Ahmed searched for the term "how to prove malicious intent."

f. On August 20, 2022, Ahmed searched for the term "evidence laundering." (PSR ¶ 31).

From August 2022 through December 2022, Ahmed visited or searched for information about his ability to flee the United States, avoid extradition, and keep his stolen cryptocurrency. For example:

a. On August 22, 2022, Ahmed searched for the term, "can I cross border with crypto."

b. On September 7, 2022, Ahmed searched for the terms, "how to stop federal government from seizing assets" and "how to stop fed govt from seizing assets."

c. On October 27, 2022, Ahmed searched for the term, "buying citizenship" and visited related websites including: "16 Countries Where Your Investments Can Buy Citizenship . . . ." (PSR ¶ 32).

Ahmed's Attack on Nirvana Finance, a Second Crypto Exchange

While negotiating a guilty plea to his hack of the Crypto Exchange, Ahmed voluntarily disclosed to the Government and accepted responsibility for a second significant hack he had committed.

In July 2022, Ahmed, facilitating a similar *modus operandi* that exploited the Crypto Exchange, defrauded Nirvana Finance ("Nirvana"), a decentralized exchange incorporated in the Caribbean region that trades its own digital cryptocurrency, ANA, which operates on the Solana blockchain. At all relevant times, Nirvana allowed users to deposit and exchange ANA and other kinds of cryptocurrencies. Nirvana was designed so that when a user purchased a substantial quantity of ANA, the price of ANA increased, and when a user sold a substantial quantity of ANA, the price of ANA decreased. (PSR ¶ 33).

On July 28, 2022, Ahmed schemed to defraud Nirvana by executing a hack in which he used a flash loan of approximately $10 million to access Nirvana's liquidity pools. Ahmed exploited a vulnerability in Nirvana's platform and used smart contracts to purchase ANA at its initial, low price, rather than at a higher price that Nirvana had designed to charge a user like Ahmed, who was acquiring a large amount of ANA. After the price of ANA was updated to reflect Ahmed's acquisition, he resold his ANA at a new, higher price, resulting in a profit of approximately $3,600,000 in cryptocurrency. Afterwards, Ahmed paid-off the flash loan. (PSR ¶ 34).

Following the attack on Nirvana, Nirvana offered a "bug bounty" of up to $600,000 for the return of the fraudulently acquired cryptocurrency. Ahmed demanded a "bug bounty" of $1,400,000, to which Nirvana declined. Instead, Ahmed kept all the stolen funds. Following the

July 28, 2022 attack on Nirvana, Ahmed engaged in a sophisticated series of cryptocurrency transactions to launder his stolen funds derived from Nirvana, including through cryptocurrency mixers such as Samourai Whirlpool. (PSR ¶ 35).

The approximately $3,600,000 worth of stolen cryptocurrency derived from the July 28, 2022 attack on Nirvana represented nearly all of the funds possessed by Nirvana. As a result, Nirvana shut down all operations shortly after Ahmed's attack on the exchange. (PSR ¶ 36).

B. Ahmed's Indictment, Guilty Plea, the Guidelines Calculation, and the PSR

On July 10, 2023, a grand jury sitting in this District returned a two-count indictment charging Ahmed with wire fraud and money laundering in connection with his hack of the Crypto Exchange. While negotiating a guilty plea to his hack of the Crypto Exchange, Ahmed, through counsel, voluntarily disclosed to the Government and accepted responsibility for a second significant hack he had committed, the Nirvana hack.

On December 14, 2023, Ahmed pleaded guilty, pursuant to a plea agreement, to Count One of the S1 Superseding Information, S1 23 Cr. 340 (VM), which charged him with accessing a protected computer without authorization in furtherance of fraud, in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), and 2. The next day, the Court accepted the guilty plea. (Dkt. 30). As part of the plea agreement, Ahmed agreed to forfeit to the United States all right, title, and interest in his crime proceeds—the stolen cryptocurrency he had fraudulently obtained from his hack of the Crypto Exchange and Nirvana— namely, (a) cryptocurrencies in the amounts of approximately 2,604,731 DAI, 5,513.838 XMR, 23.663 BTC, 15.912 Wrapped BTC, 300,192 USDC, 6.221425 ETH, and 8.8452 SOL; and (b) cryptocurrencies in the amount of 40.26 XMR, which were seized by the Government on or about July 11, 2023.

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 six pursuant to U.S.S.G. § 2B1.1(a)(2);
(2) A 20-level increase, pursuant to U.S.S.G. § 2B1.1(b)(1)(K), because the loss amount was more than $9,500,000 but less than $25,000,000;
(3) A two-level increase, pursuant to U.S.S.G. § 2B1.1(b)(2)(A)(iii), because the offense resulted in substantial financial hardship to one or more victims;
(4) A two-level increase, pursuant to U.S.S.G. § 2B1.1(b)(10)(C), because the offense involved sophisticated means and Ahmed intentionally engaged in or caused the conduct constituting sophisticated means; and
(5) A three-level decrease, pursuant to U.S.S.G. § 3E1.1(a) and (b), for acceptance of responsibility.

Thus, the applicable Guidelines offense level is 27 and the Criminal History Category is I. Ahmed's sentencing range would otherwise be 70 to 87 months' imprisonment but, pursuant to U.S.S.G. § 5G1.1(a), because the statutory maximum sentence is 60 months, the Stipulated Guidelines Sentence is 60 months. The PSR contains the same Guidelines calculation as that set forth in the plea agreement. (PSR ¶¶ 52-68, p. 34). [2]

The Probation Office, which did not have the benefit of the Crypto Exchange's victim impact statement, (PSR ¶ 48), recommends a downward variance sentence of 24 months' imprisonment. PSR at 34.

[2] The Government is not seeking a fine in light of the sworn financial information provided by Ahmed. The Court previously entered a consent preliminary order of forfeiture against Ahmed. (Dkt. 34). Consistent with the parties' plea agreement and the PSR, the Government will submit a proposed restitution order for $5,071,074.23, with $1,500,000 paid to the Crypto Exchange and $3,571,074.23 paid to Nirvana, around the time of sentencing. (PSR ¶ 40).

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. A Slightly Below Guidelines Variance Sentence of 48 Months Would Be Just and Appropriate

The Government respectfully submits that a sentence of 48 months would be sufficient, but not greater than necessary, to serve the purposes of sentencing. In particular, the nature and circumstances of Ahmed's offense and the need to provide just punishment, achieve specific and especially general deterrence, and account for the devastating, ongoing harm to his victims, all justify such a sentence.

Offense conduct. A sentence of 48 months is necessary to reflect the nature and circumstances of the offense and to provide just punishment, particularly given the sophistication of Ahmed's multiple hacks and the devastation that he caused to his victims. Such a sentence also would consider Ahmed's full acceptance of responsibility in admitting to both of his hacks (including affirmatively raising the Nirvana hack, with which he had not been charged, to the Government) and surrendering the cryptocurrency he had converted his crime proceeds into. Indeed, it is because of these factors that the Government exercised its discretion to allow Ahmed to plead guilty to computer fraud, and not wire fraud or money laundering (with a higher statutory maximum and potential Guidelines range than the statutory maximum and Stipulated Guidelines Sentence that the parties agree applies), and makes the instant below-Guidelines recommendation.

Still, it bears noting that the offense conduct is serious. Ahmed's Attack on the Crypto Exchange is not something he simply stumbled into. To the contrary, it required detailed planning, as seen by his use of VPN-1 to conceal his Internet Protocol address while he executed the Attack and the series of test transactions with the Crypto Exchange that he conducted in the lead-up to the Attack to obtain tick data and locate system vulnerabilities. It also required technical expertise, which Ahmed undoubtedly possessed. And it required Ahmed's willingness to commit outright fraud, as Ahmed supplied one of the Crypto Exchange's accounts with fake price-tick data and carefully structured and designed these non-tick accounts to nonetheless falsely appear as authentic tick accounts. Moreover, Ahmed threatened the Crypto Exchange during his post-hack communications, when he told the Crypto Exchange that its post-Attack predicament was a "nightmare scenario" and sought to extract a seven-figure payment from the Crypto Exchange.

Ahmed's actions in carrying out the Attack on the Crypto Exchange were far from a one-time mistake or a fleeting lapse in judgment. After he fraudulently obtained inflated cryptocurrency fees in the Attack, he laundered the fraud proceeds through a series of complicated transactions to conceal the nature, location, source, and his control of the stolen funds. Ahmed designed the scheme to evade detection and frustrate the efforts of victims and law enforcement to identify him and trace proceeds. In this regard, after the Attack, Ahmed conducted dozens of transactions exchanging one cryptocurrency token for another, "bridged" fraud proceeds across one blockchain over to another, and laundered fraud proceeds through a swap aggregator to other wallets on the Solana blockchain. Further, four months after the Attack, Ahmed kept going when he exchanged fraud proceeds into the cryptocurrency Monero, an anonymized and particularly difficult cryptocurrency to trace. In the months after the attack, Ahmed visited or searched for information about his ability to flee the United States, avoid extradition, and keep his stolen cryptocurrency. Even after that he continued the offense conduct: ten months after the Attack, Ahmed laundered fraud proceeds through overseas cryptocurrency exchanges. Over and over, until he was arrested about a year after the Attack, Ahmed made a conscious and deliberate choice to continue to perpetuate his crimes.

And of course, he committed a second crime by defrauding Nirvana of approximately $3,600,000 worth of stolen cryptocurrency, which represented nearly all of the funds possessed by Nirvana. But this time, after Nirvana rejected Ahmed's "bug bounty" offer of $1,400,000, Ahmed instead kept all of the stolen funds. Again, as with the Attack on the Crypto Exchange, he engaged in a sophisticated series of cryptocurrency transactions to launder his stolen funds, including through cryptocurrency mixers such as Samourai Whirlpool. As a result, Nirvana shut down all operations shortly after Ahmed's attack on the exchange.

Victim Impact. Among the most serious aspects of Ahmed's conduct is the harm he caused to his victims, who have not been truly made whole by Ahmed's restitution payments. Not even close. Ahmed's victims have incurred financial, reputational, and incalculable emotional trauma that continues to this day. Users of the Crypto Exchange and Nirvana lost their deposited cryptocurrency when Ahmed hacked the exchanges and, while some have received and others will receive cryptocurrency as restitution, many users lost their right to control their assets as they saw fit as they still await, over a-year-and-a-half later, the return of significant portions of their cryptocurrency.

The operators of the Crypto Exchange and Nirvana have also been falsely accused of having committed the crimes themselves as alleged in-house perpetrators. As part of sentencing, they have given statements recounting this and additional harms that Ahmed caused them, which statements are attached to this submission as Exhibits A through C. Together, the victim statements provide the Court with powerful evidence of the serious and lasting harm of Ahmed's crimes and the need to justly punish him. The Government highlights portions of the victim statements below.

As the Crypto Exchange notes in its victim impact statement, which the U.S. Probation Office did not have the benefit of reviewing before finalizing the PSR, "[a]part from direct losses" incurred by the Crypto Exchange, "there are many other losses and impacts that we suffered. Many of them are hard to be evaluated quantitatively." (Ex. A). "Firstly, in order to remediate the effect, we developed a series of follow-up smart contracts to ensure the remaining liquidity can be safely claimed back by our users. The audit cost for these new smart contracts is $84,000." (*Id.*). Additionally, "[t]he labor cost of new version development and maintenance is hard to calculate already but is definitely no less than $200,000." (*Id.*).

The Crypto Exchange also points to the profound, nearly existential drop in its "total value locked" or "TVL," which is the reduction in assets staked on the Crypto Exchange's blockchain network. As it writes,

> Secondly, the TVL on [the Crypto Exchange] dropped by more than 95% since the incident, which is an approximately $10M value escape. The price of our governance token has been dropping continually after the incident. The token price before the incident was around $0.12 but now it is about $0.003 and also lacks enough liquidity. This has caused huge losses to both our investors and our team. All these are inevitable and are devastating to our project.

(*Id.*).

The Crypto Exchange also invokes the damaging reputational and privacy impact of Ahmed's crime on its team members, noting that

> this incident has also had a huge negative impact on the reputation of our team and the privacy rights of our team members. We are also facing increasing difficulty communicating with venture capitals and other investors in this industry. These things may affect our career and life for a very long time. The losses and harm it brought to us are immeasurable.

(*Id.*).

As for the direct losses of Ahmed's Attack on the Crypto Exchange, it should be noted that, after the Attack, the Crypto Exchange initiated a plan to compensate the users Ahmed had victimized whereby the Crypto Exchange bore the bulk of the loses caused by the Attack and paid users back "84% of their original funds." (*Id.*). As for the remaining 16%, because Ahmed, to conceal his crime and launder the stolen cryptocurrency, conducted a series of token-swap transactions exchanging the original stolen cryptocurrency for other types of cryptocurrency, the cryptocurrency Ahmed ultimately surrendered to the Government, which the Government in turn will provide to the Crypto Exchange to compensate the users' outstanding losses, is less valuable today than the original cryptocurrency Ahmed stole from the Crypto Exchange would have been today, had he not conducted his laundering token-swap transactions.

The Crypto Exchange concludes its letter by writing,

> Although this project has been in a state of continuous losses since the incident, our team has been insisting on maintaining its services till today, because we want to wait and strive for a proper result for all our users. We are extremely pleased that this case is coming to a judgement soon.

(*Id.*).

As for Nirvana, it has submitted a detailed victim impact statement of its own, detailing the various harms its team members have suffered as a result of Ahmed's crimes. (Ex. B). It is set forth in full below:

> As a representative of Nirvana Finance, I am writing to articulate the profound harm inflicted upon our users and team by [Ahmed's] criminal actions. [Ahmed's] exploitation of our platform in July 2022 through a calculated and sophisticated attack led to the unauthorized extraction of approximately $3.6 million. Due to our platform's internal leverage mechanisms, this theft represented a staggering loss of around $15 million in value to our community.
>
> This theft not only stripped our users of significant financial resources but also shattered their trust in both our platform and the broader decentralized finance ecosystem. Our community was built on principles of transparency, security, and mutual respect; [Ahmed's] actions grievously undermined these core principles, casting a long shadow of distrust and insecurity.

> In addition to the financial damages to Nirvana's user base, the personal and financial toll on our team has been considerable during this time. The aftermath of the theft saw us grappling with the immediate financial repercussions of losing our livelihoods overnight, coupled with the daunting task of restoring our platform's integrity and user confidence. In addition, in this industry, a team's reputation is extremely important. Until [Ahmed's] guilty plea proved we were not responsible, our team endured significant reputational damage.
>
> The strain of these efforts has taken a significant emotional and psychological toll on every member of our team, compounding the financial damage with a profound personal and professional impact.
>
> [Ahmed's] decision to plead guilty and forfeit over $12.3 million, while a step towards restitution, does not alleviate the ongoing challenges faced by our users and team. The complete breach of trust and the destruction of our platform can never be rectified. The funds stolen and laundered through sophisticated means reflect a blatant disregard for the law and the principles upon which decentralized finance stands.
>
> We implore the court to recognize the severity of [Ahmed's] actions and their far-reaching consequences on innocent individuals who placed their trust in Nirvana Finance. We feel that the sentencing should reflect the gravity of the harm inflicted upon our community and serve as a deterrent to prevent similar attacks on the integrity of digital finance.

(*Id.*).

Nirvana expressed similar sentiments in an email to the Government the day after Ahmed's guilty plea when it wrote, "I know this is a landmark case since you're really setting a precedent here. It's been a very rough 16 months for the team since the hack as we've been repeatedly accused and threatened so this was a huge weight off of our shoulders." (Ex. C).

In light of the harms experienced by Ahmed's victims—including the collapse of their businesses, financial losses, loss of trust, false accusations of in-house theft, shattered reputations, damaged psyches, and derailed careers—a sentence of 48 months is necessary to reflect the seriousness of the offense and to provide just punishment.

Specific deterrence. Specific deterrence and the need to promote respect for the law also militate in favor of a sentence of 48 months. As noted above, Ahmed committed not one but two distinct, significant, and ruinous hacks. And far from a one-click, one-time fraud, for about a year until he was caught, Ahmed tried to conceal the two widely publicized and scrutinized hacks he had carried out. Again, both hacks required detailed planning, technical expertise, a willingness to defraud, and coercive communications with his victims trying to survive and prevent a run on their businesses.

Nor was there any need or justification for Ahmed to turn to fraud. At the time of his crimes, Ahmed was a well-educated and well-compensated senior security engineer in a committed relationship. (PSR ¶¶ 76, 90-108). At the time of his over $12.3 million crimes, Ahmed was earning over $400,000 per year as a senior security engineer at Amazon. (PSR ¶¶ 92, 93). For tax years 2020, 2021, and 2022, he earned total income, respectively, of $486,619, $489,413, and $388,325. (PSR ¶ 107). His crimes thus appear to have been motivated by greed and perhaps misguided confidence that he would not get caught. While the Court should of course consider Ahmed's mental health and familial struggles discussed in the PSR, it is sadly true that defendants with comparable and seemingly far more difficult backgrounds, are regularly sentenced to lengthy terms of imprisonment in this District. In short, there was absolutely no need or justification for Ahmed to turn to crime.

In light of the severity, duration, and breadth of his conduct, coupled with the lack of any need or justification for Ahmed's crimes, specific deterrence and the need to promote respect for the law also weigh in favor of a substantial incarceratory sentence.

General deterrence. The need for general deterrence is quite acute in this case, given how prevalent and lucrative cyber frauds—and especially cryptocurrency and DeFi hacks—are and how difficult they are to detect and prosecute. With respect to prevalence of DeFi hacks, public reporting indicates that DeFi exploits caused a staggering $53.5 billion in losses in 2022 and over $1.3 billion in losses in 2023.[3]

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

[3] *See, e.g.*, Jeff Owens, *DeFi Has a Risk Problem and It's Time to Solve It*, CoinDesk, Dec. 20, 2023, https://www.coindesk.com/consensus-magazine/2023/12/20/defi-has-a-risk-problem-and-its-time-to-solve-it/; Bessie Liu, *The 5 biggest DeFi hacks of 2023*, Blockworks, Dec. 22, 2023, https://blockworks.co/news/biggest-defi-hacks-2023; *see also* Zeke Faux, *Number Go Up* 102 (2023) (estimating that in 2021 a total of $3.2 billion in cryptocurrency was stolen from exchanges and decentralized finance apps).

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.").

This is particularly so in the case of sophisticated, profitable cryptocurrency thefts like the DeFi hacks here. These types of crimes are pernicious and lucrative: they are extremely enriching to their perpetrators and yet inherently difficult for law enforcement to detect and stop. As the enormous numbers above reveal, it has, unfortunately, become far too easy for cyber-criminals like Ahmed to target and victimize DeFi exchanges 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 Ahmed—the first-ever sentencing for the hack of a smart contract, which appears likely to be closely monitored by participants in the DeFi ecosystem—should send a strong and clear message to others that sophisticated hacks, particularly ones as crushing to victims as were Ahmed's crimes, will be met with serious consequences.

Unwarranted sentencing disparities. Finally, a sentence of 48 months is appropriate to avoid creating an unwarranted sentencing disparity. As the Second Circuit has explained, "we have repeatedly made clear that 'section 3553(a)(6) requires a district court to consider nationwide sentence disparities, but does not require a district court to consider disparities between co-defendants.'" *United States v. Ghailani*, 733 F.3d 29, 55 (2d Cir. 2013) (quoting *United States v. Frias*, 521 F.3d 229, 236 (2d Cir. 2008)). Here, the PSR's summary of the U.S. Sentencing

Commission's Judiciary Sentencing Information data, which analyzed the sentences imposed on the 164 defendants with the same final offense level, 27, and Criminal History Category, I, as Ahmed over the last five fiscal years (FY2018-2022), indicates that the average sentence imposed was 51 months and the median sentence imposed was 48 months. (PSR 30-31). Accordingly, based on Ahmed's conduct and the sentences imposed over the last five fiscal years on the 164 defendants with the same final offense level and Criminal History Category as Ahmed, to sentence Ahmed below 48 months would risk creating an unwarranted sentencing disparity.

III. CONCLUSION

On the facts here, a slightly downward variance sentence of 48 months would be appropriate and just. Such a sentence would appropriately credit Ahmed for surrendering to the Government access to his crime proceeds and recognize his acceptance of responsibility. At the same time, the requested period of incarceration would recognize the lasting harm he has inflicted and continues to inflict on his victims, avoid minimizing the seriousness of Ahmed's multiple, sophisticated crimes, and send a message to would-be cyber criminals that meaningful time in prison—and not merely being asked to part with their ill-gotten gains—is the likely consequence of such aggravated criminal conduct.

Dated: New York, New York
April 1, 2024

Respectfully submitted,

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

By: /s/____________________________
David R. Felton
Kevin Mead
Assistant United States Attorneys
(212) 637-2299 / -2211

cc: Defense counsel (by ECF and email)