UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -x

UNITED STATES OF AMERICA	**:**	
- v. -	**:**	**21 CR. 714 (KPF)**
NICKOLAS SHARP,	**:**	
Defendant.	**:**	

- -x

GOVERNMENT'S SENTENCING MEMORANDUM
REGARDING DEFENDANT NICKOLAS SHARP

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

VLADISLAV VAINBERG
ANDREW K. CHAN
Assistant United States Attorneys
- Of Counsel -

Table of Contents

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -x

UNITED STATES OF AMERICA	:	
- v. -	:	**21 CR. 714 (KPF)**
NICKOLAS SHARP	:	
Defendant.	:	

- -x

GOVERNMENT'S SENTENCING MEMORANDUM
REGARDING DEFENDANT NICKOLAS SHARP

The Government respectfully submits this memorandum for the Court's consideration in connection with the sentencing of defendant Nickolas Sharp ("Sharp" or "the defendant"), which is scheduled for May 10, 2023, at 3:00 p.m.[1]

In late 2020, Sharp secretly stole gigabytes of confidential files from a public New York-based technology company where he was employed ("Company-1"). During the course of this cybersecurity attack (the "Cyber Attack"), Sharp caused damage to Company-1's computer systems by altering log retention policies and other files, to conceal his unauthorized activity on the network and even implicate other co-workers. While working on a team remediating the effects of the Cyber Attack, Sharp sent a ransom note to Company-1, posing as an anonymous attacker who claimed to have obtained unauthorized access to Company-1's computer networks. The ransom note sought the equivalent of approximately $1.9 million in Bitcoin cryptocurrency in exchange for the return of the stolen data and the identification of an existing "backdoor," or vulnerability, to Company-1's computer systems. After Company-1 refused the demand, Sharp published a portion of the stolen files on a publicly accessible online platform. When Federal

[1] The Probation Office's final presentence report dated April 25, 2023 is referenced as the "PSR". The defendant's sentencing submission filed April 26, 2023, is referenced as "Def. Mem."

Bureau of Investigation ("FBI") agents executed a search warrant on his home in March 2021, Sharp lied to law enforcement about his non-involvement in the attack and the means of the attack. Afterwards, Sharp re-victimized his employer by planting false media stories as a purported whistleblower to malign Company-1's response and disclosures related to the Cyber Attack, while concealing his own role, causing Company-1 (and in turn its shareholders) to lose over four billion of dollars in market capitalization value.

In December 2021, Sharp was arrested on a four-count Indictment. On February 2, 2023, pursuant to a plea agreement, Sharp pled guilty to Count One, Three, and Four of the Indictment, which charged him with intentionally damaging protected computers, in violation of 18 U.S.C. § 1030(a)(5)(A), wire fraud, in violation of 18 U.S.C. § 1343, and making false statements to the Federal Bureau of Investigation in violation of 18 U.S.C. § 1001.

As discussed below, the applicable Sentencing Guidelines range in this case is 97 to 121 months' imprisonment. The Government respectfully submits that aggravated nature of the scheme and magnitude of harm caused by the defendant not captured in the Guidelines calculations amply warrants a sentence within the stipulated Guidelines range. A lower sentence would fail to serve the essential sentencing goals of providing just punishment, affording general and specific deterrence, and promoting respect for the law.

I. Factual Background

A. Background on Company-1

Company-1 is a technology company headquartered in New York, New York, which manufactures and sells wireless communications products. Company-1's shares are traded on the New York Stock Exchange. As of March 29, 2021, Company-1's market capitalization was over $23 billion. PSR ¶ 1. From August 2018 up to and including on or about April 1, 2021, Sharp

worked as a senior software engineer and Cloud Lead at Company-1, responsible for software development and cloud infrastructure security, among other things. PSR ¶ 2.

At all relevant times, Company-1 used multiple third-party providers to host its data and facilitate its product development. Company-1 maintained an account with Amazon Web Services ("AWS"), which was used to host server infrastructure and manage development of Company-1's new applications and products. PSR ¶ 12. The AWS infrastructure included servers that ran a portion of Company-1's operations and hosted certain of Company-1's system, code, and credentials. *Id.* Company-1 also subscribed to services from a third-party company named GitHub, Inc. ("GitHub"), which is a provider of internet hosting for software development, developer collaboration, and version control. PSR ¶ 13. Through GitHub, Company-1 stored certain development files, as well as the history of changes to those files, in data structures called repositories. *Id.* Developers employed by Company-1 had individualized accounts on GitHub that provided them with varying levels of access to various repositories hosting Company-1's code and development projects. *Id.* Company-1 also maintained a high-level access account shared among a group of developers ("GitHub Account-1"), which provided access to all or nearly all of Company-1's repositories on GitHub. *Id.* User activity on GitHub is logged. *Id.*

B. Sharp Plans the Attack and an Exit from Company-1

At all relevant times, Sharp resided at a residence in Portland, Oregon (the "Sharp Residence"). The internet connection from the Sharp Residence was associated with a specific Internet Protocol address at certain relevant times (the "Sharp IP").

Sharp was employed by Company-1 from in or about August 2018 up to and including on or about April 1, 2021, including throughout committing the Cyber Attack in or about December 2020, and sending a ransom demand in January 2021. PSR ¶¶ 18-37. Sharp was a senior developer who had access to credentials for Company-1's GitHub and AWS servers. PSR ¶ 18.

On or about July 7, 2020, Sharp used his personal Paypal, Inc. account to purchase a 27-month subscription to a Virtual Private Network (or "VPN") service[2] provided by a company called Surfshark.[3] PSR ¶ 19. Sharp downloaded Surfshark VPN on multiple devices, including his cell phone and laptop, and used the VPN service prior to the Cyber Attack. *Id.*

On or about December 9, 2020, Sharp applied for a position at a technology company based in California ("Company-2"). PSR ¶ 21. Over the course of the ensuing weeks and months, Sharp successfully interviewed and obtained that position. A day after applying to Company-2, Sharp began the Cyber Attack and extortion scheme to which he has pleaded guilty.

C. Sharp Conducts Reconnaissance and Begins the Cyber Attack

On or about December 10, 2020, at approximately 2:55 a.m. UTC,[4] and again at 3:16 a.m., Sharp used his own Company-1 credentials to access a particular key (the "Key") on Company-1's infrastructure through AWS servers. PSR ¶ 22. The connection was made through the Sharp IP from Sharp's home. *Id.* The Key accessed by Sharp permitted the user to, among other things, obtain access to other credentials within Company-1's infrastructure and to run searches through that infrastructure. *Id.* Through this log-in, Sharp was conducting reconnaissance on how to use the credentials to launch the subsequent anonymous attack. *Id.*

---

[2] A Virtual Private Network ("VPN") is an internet connection method used to add security and privacy to network connections. When a user connects to a VPN, it creates an encrypted tunnel between the user and a remote server operated by a VPN service. All of the user's internet traffic is encrypted and routed through this tunnel to the ultimate internet or web resource being accessed by the user. Because internet traffic exits the VPN server, the user's computer appears to have the IP address of said server, masking the IP address of the user's computer, and thus his identity and location. PSR ¶ 15.

[3] Surfshark is a company headquartered in the British Virgin Islands that sells a commercial VPN service (the "Surfshark VPN") to the public, which, as described above, can effectively anonymize their users by replacing their personal IP addresses with IP addresses operated by Surfshark through its servers. PSR ¶ 16.

[4] For consistency, unless otherwise noted, all times are in the UTC time zone.

Approximately two minutes later, on December 10, 2020, at approximately 3:18 a.m., Sharp re-connected to Company-1's AWS infrastructure using a masked IP provided by the Surfshark VPN. PSR ¶ 23. Sharp, now acting as the anonymous attacker, used the same Key he accessed on his work account two minutes earlier to connect to AWS and to run a command "getcalleridentity." *Id.* That command returns the username and account information for the AWS account for which it is run and can validate that the credential is usable. *Id.*

On December 21, 2020, at approximately 9:58 p.m., Sharp logged into Company-1's GitHub infrastructure via a web browser, using his own Company-1 work credentials. PSR ¶ 24. Sharp logged in through his Sharp IP address, and viewed the names of certain repositories of data. *Id.* Approximately one minute later, on December 21, 2020, at approximately 9:59 p.m., Sharp used the Surfshark VPN that masked his true IP address to connect into GitHub through SSH by using Company-1's high-level Github Account-1. PSR ¶ 25. Sharp used the SSH connection to execute a series of commands to copy Company-1's repositories of data to Sharp's computer. *Id.*

D. The Slip-Up

Throughout the Cyber Attack, Sharp generally masked his true IP address through the Surfshark VPN successfully. But in one fleeting instance during the exfiltration of data, the Sharp IP address was logged making an SSH connection to use Github Account-1 to copy a repository. PSR ¶ 26. This slip-up was caused by an internet outage at Sharp's home that appeared to temporarily disable his VPN.

Specifically, between December 21, 2020 at approximately 11:47 p.m. and December 22, 2020 at 2:16 a.m., Sharp used the Surfshark VPN to mask his connection while cloning Company-1's Github repositories. PSR ¶ 27. On December 22, 2020 at approximately 2:16 a.m., Sharp's exfiltration commands stopped. PSR ¶ 28. At around the same time, the internet service at the Sharp Residence went down. *Id.* A video camera inside Sharp's home captured him speaking on

the phone to a representative of his internet service provider at approximately 2:21 a.m. and subsequently stating "The internet is down." *Id.* Then, at approximately 2:54 a.m., Sharp can be seen and heard saying, "Okay. Yeah. The internet should be working now." *Id.*

At approximately 2:54 a.m., the Internet service at the Sharp Residence was reenabled, and approximately one minute later, the Sharp IP was logged, unmasked by any VPN, using GitHub Account-1 to continue sending clone commands to steal Company-1's data. PSR ¶ 29. Then the VPN kicked in again. Over the next several hours, on December 22, 2020 between approximately 3:04 to 5:31 a.m., Sharp cloned approximately 155 data repositories from Company-1 through Github Account-1, using the Surfshark VPN to once again mask his IP address. PSR ¶ 30.

E. Sharp Researches How To Monetize His Attack

On December 23, 2020, in the middle of Sharp's Cyber Attack, Sharp messaged a senior cybersecurity employee of Company-1 ("Employee-1") to ask whether an employee of Company-1 such as himself would be eligible for a financial payout under Company-1's HackerOne bug bounty program for discovering vulnerabilities or lost credentials. PSR ¶ 31. HackerOne is a vulnerability coordination and bug bounty platform that connects businesses with penetration testers and cybersecurity researchers. PSR ¶ 32. Company-1 had a HackerOne program to pay outside parties to report vulnerabilities. *Id.* Employee-1 told Sharp that Company-1 pays for reports of "found credentials," but regarded these messages from Sharp as suspicious and preserved them. *Id.*

F. Sharp Destroys Existing Cybersecurity Logs and Attempts to Implicate Other Coworkers While Covering His Tracks

Sharp continued to access Company-1's GitHub or AWS data using the Surfshark VPN through at least on or about December 26, 2020. PSR ¶ 33. He used sophisticated means to cover his tracks and delete logs that would help reconstruct the means of the attack. *Id.* Among other

things, Sharp applied one-day lifecycle retention policies to certain logs on AWS which would have the effect of deleting certain evidence of the intruder's activity within one day. *Id.*

Sharp also modified forensic artifacts to make it appear as if other Company-1 employees were using the Key actually used by Sharp during particular sessions in the attack. PSR ¶ 34. Between December 22 and December 26, 2020, Sharp manually renamed at least 18 AWS sessions that he opened to conduct the attack to make it appear as if one of five other Company-1 DevOps team members was using the Key. *Id.* In so doing, Sharp sought to obfuscate his role in the attack and divert suspicion onto innocent co-workers. *Id.*

G. Sharp Lies to Company-1 During Its Remediation of the Attack

The Cyber Attack was discovered by other employees of Company-1 on or about December 28, 2020. PSR ¶ 35. At that time, Sharp joined a team working to assess the scope and damage caused by the Cyber Attack and remediate its effects, all while concealing his role in committing the Cyber Attack. *Id.* Sharp made numerous false statements to Company-1's employees, forensic investigators, and other representatives to evade detection. *Id.* For example, upon the team's identification of Surfshark VPN as the tool used by the attacker, Sharp pretended to have never used Surfshark VPN himself. *Id.*

H. Sharp Extorts Company-1 And Publishes Proprietary Data

On or about January 7, 2021, at approximately 4:01 a.m., senior employees at Company-1, including an employee located in Manhattan, received a ransom email (the "Ransom Email") from the perpetrator of the Cyber Attack, secretly sent by Sharp. PSR ¶ 36. The email was sent through an IP address associated with the Surfshark VPN. *Id.* The Ransom Email offered, in substance, to return the stolen data and not to publish or use it, in exchange for the payment of 25 Bitcoin, a cryptocurrency. *Id.* The Ransom Email also offered to identify a purportedly still unblocked "backdoor" used by the attacker for the sum of another 25 Bitcoin. *Id.* The total amount requested

for ransom was equivalent to close to $1.9 million, based on the prevailing exchange rate between Bitcoin and U.S. dollars at the close of January 7, 2021. *Id.* The Ransom Email also referenced a chat communication on Keybase[5], sent by the attacker to Employee-1, a senior cybersecurity employee. *Id.* That Keybase communication contained a copy of the Ransom Email text as well as uploaded examples of Company-1's stolen data. *Id.*

Company-1 did not pay the ransom prior to the ransom deadline set forth the Ransom Email. PSR ¶ 37. On or about January 9, 2021, at approximately 11:57 p.m., three minutes before the ransom deadline was to expire, Sharp (as the anonymous perpetrator) sent Employee-1 a message on Keybase. *Id.* The message read "No BTC. No talk. We done here." *Id.* The message contained a link to a public Keybase folder on which Sharp uploaded certain of Company-1's stolen proprietary data for public access. *Id.* Company-1 promptly caused Keybase to remove the folder. *Id.*

I. Sharp Destroys Evidence and Lies to the FBI

Sharp knew that Company-1 referred the matter for investigation to the FBI in January 2021. PSR ¶ 40. Around the same time, after Sharp's home IP was discovered to be involved in the attack, Sharp was also asked to relinquish his company-provided router, video cameras, and work computer to a forensic company hired by Company-1. *Id.* This evidence was also analyzed by the FBI. Forensic analysis on the router showed that during key times of the attack in December 2020, a different MacBook laptop, which Sharp did not relinquish to Company-1, had connected to Sharp's home router during the Cyber Attack, and transferred data in corresponding amounts to what was being stolen. *Id.* This laptop was identified with the host name Admins

[5] Keybase is an encrypted social networking service that permits users to, among other things, send private messages and files directly to other Keybase users and also to upload files that would be publicly available to any Keybase user. PSR ¶ 14. Less than an hour prior to using Keybase to send the ransom note to Company-1, Sharp conducted internet searches related to the extent to which data from Keybase would be discoverable through subpoena. PSR ¶ 39.

MBP and a unique Mac address.[6] *Id.* On or about January 29, 2021, while knowing that the FBI was investigating the Cyber Attack, Sharp wiped and reset the Admins MBP laptop he used to perpetrate the Cyber Attack, but kept the laptop in his home. PSR ¶ 41.

On or about March 24, 2021, FBI agents executed a search warrant on the Sharp Residence and seized certain electronic devices belonging to Sharp, including the Admins MBP laptop he used for the attack. PSR ¶ 42. During the execution of that search, Sharp made numerous false statements to FBI agents, including among other things, in substance, that he was not the perpetrator of the Cyber Attack and that he had not used Surfshark VPN prior to the discovery of the Cyber Attack. *Id.* When confronted with records demonstrating that Sharp bought the Surfshark VPN service in July 2020, approximately six months prior to the Cyber Attack, Sharp falsely stated, in part and substance, that someone else must have used his PayPal account to make the purchase. *Id.*

J. Sharp Spreads False Whistleblower Stories to Revictimize Company-1

Several days after the FBI executed the search warrant, Sharp reached out to a journalist posing as a Company-1 whistleblower. PSR ¶ 43. Sharp caused false or misleading news stories to be published about the Cyber Attack and Company-1's original public disclosures and response to the Cyber Attack. *Id.* In a lead article, titled "Whistleblower: Company-1 Breach 'Catastrophic,'" published on March 30, 2021, Sharp identified himself as an anonymous source within Company-1 who had worked on remediating the Cyber Attack. *Id.* Sharp asserted, in part, that Company-1 had intentionally deceived customers by "massively downplay[ing]" the impact of a "catastrophic" data breach. *Id.* Sharp pretended that Company-1 had been hacked by unidentified perpetrators who maliciously acquired root administrator access to Company-1's

[6] A media access control address (or "MAC") is a unique physical 12-digit identifier associated with the network interface controller on a computer or other device that connects to the internet.

AWS accounts. *Id.* In fact, as Sharp well knew, Sharp had taken Company-1's data using credentials to which he had access in his role as Company-1's AWS cloud administrator, and Sharp had used that data in a failed attempt to extort Company-1 for millions of dollars. *Id.*

At the time of Sharp's actions, Company-1 had a market capitalization over $23 billion and earned revenue from manufacturing and selling network and other products for retail customers and commercial enterprises, who relied on such products being secure. Following the publication of articles reporting on Sharp's false allegations and discussing the hackers' potential access to Company-1's products in customers' homes, between Tuesday, March 30, 2021 and Wednesday March 31, 2021, Company-1's stock price fell approximately 20%, losing over four billion dollars in market capitalization. PSR ¶ 44.

In an effort to further victimize Company-1, Sharp separately contacted various U.S. and foreign regulators to furnish false allegations about the data breach and Company-1's disclosures as a purported whistleblower, without revealing that he was in fact the perpetrator of the attack. PSR ¶ 45.

II. Guidelines Calculation

The Probation Office has calculated the United States Sentencing Guidelines (the "Guidelines") applicable to this offense consistently with what the parties stipulated in their plea agreement. PSR ¶¶ 8, 54-67.

Sharp's total offense level under the Guidelines is 30, based on the following:

- Count One, Three, and Four are grouped, and have a base offense level of 7 pursuant to § 2B1.1(a)(1);
- A 16-level increase is warranted pursuant to § 2B1.1(b)(1)(I) because the loss caused by the defendant's criminal conduct exceeded $1,500,000 but was below $3,500,000;[7]

[7] For purposes of the Guidelines, the parties stipulated to a loss amount and restitution of $1,590,487 based solely on the cost of forensic remediation incurred by Company-1 in the immediate aftermath of Sharp's attack. *See* U.S.S.G. § 2B1.1, Application Note 3(A)(v)(III). This figure does not include

- A 2-level increase is warranted pursuant to §2B1.1(b)(10)(C) because the offense involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means;
- A 4-level increase is warranted pursuant to §2B1.1(b)(19)(A)(ii) because the defendant was convicted under 18 U.S.C. § 1030(a)(5)(A);
- A 2-level increase is warranted pursuant to § 3B1.3 because the defendant abused a position of private trust or used a special skill in a manner that significantly facilitated the commission or concealment of the offense;
- A 2-level increase is warranted pursuant to § 3C1.1 because the defendant willfully obstructed justice with respect to the investigation of the offense; and
- A 3-level decrease is warranted pursuant to § 3E1.1(a) and (b) because the defendant demonstrated acceptance of responsibility for the offense by timely entering a guilty plea.

PSR ¶¶ 54-67.

Sharp's criminal history category is I. PSR ¶ 71. Based on an offense level of 30 and a criminal history category of I, the applicable Guidelines range is 97 to 121 months' imprisonment. PSR ¶ 121.[8]

III. Sentencing Legal Principles

The Guidelines are no longer mandatory, but they 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). "[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). The Guidelines range is thus "the lodestar" that "anchor[s]" the district court's discretion. *Molina-Martinez* v. *United States*, 136 S. Ct. 1338, 1345-46 (2016) (quoting *Peugh* v. *United States*, 133 S. Ct. 2072, 2087 (2013)) (internal quotation marks omitted).

---

additional harm caused to the Company-1 and its shareholders through Sharp's subsequent misconduct leading to a market drop of billions of dollars of Company-1's shareholder value.

[8] The Presentence Report recommends a sentence of 42 months imprisonment. PSR p. 33.

After making the initial Guidelines calculation, a sentencing judge must consider the factors outlined in Title 18, United States Code, Section 3553(a), and "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, 18 U.S.C. § 3553(a), which are: "a) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for that offense; b) the need to afford adequate deterrence to criminal conduct; c) the need to protect the public from further crimes by the defendant; and d) the need for rehabilitation." *United States* v. *Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)).

Under Section 3553(a), "in determining the particular sentence to impose," the Court must consider: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense. *See* 18 U.S.C. § 3553(a).

In light of *Booker*, the Second Circuit has instructed that district courts should engage in a three-step sentencing procedure. *See Crosby*, 397 F.3d at 103. First, the Court must determine the applicable Sentencing Guidelines range, and in so doing, "the sentencing judge will be entitled to find all of the facts that the Guidelines make relevant to the determination of a Guidelines sentence and all of the facts relevant to the determination of a non-Guidelines sentence." *Id*. at 112; *see also United States* v. *Corsey,* 723 F.3d 366, 375 (2d Cir. 2013) ("Even in cases where courts depart or impose a non-Guidelines sentence, the Guidelines range sets an important benchmark against which to measure an appropriate sentence."). Second, the Court must consider whether a departure from that Guidelines range is appropriate. *Crosby*, 397 F.3d at 112. Third, the Court must consider the Guidelines range, "along with all of the factors listed in section 3553(a)," and

determine the sentence to impose. *Id.* In so doing, it is entirely proper for a judge to take into consideration his or her own sense of what is a fair and just sentence under all the circumstances. *United States* v. *Jones*, 460 F.3d 191, 195 (2d Cir. 2006).

IV. Section 3553(a) Analysis

The Government respectfully submits that a sentence within the Guidelines range of 97 to 121 months' imprisonment is necessary to reflect the seriousness and aggravated nature of Sharp's crimes, provide just punishment, afford general and specific deterrence, and promote respect for the law.

A. The Nature and Circumstances of the Offense

The offense is very serious and should be punished accordingly. The callousness and sophistication of Sharp's scheme, as well as its impact on his victimized former employer, coworkers, and the public, warrant a sentence within the Guidelines range of 97 to 121 months.

The theft itself is breathtaking enough. In mid and late December, day after day, Sharp secretly logged into Company-1's networks using credentials entrusted to him and other high-level developers to steal tens of gigabytes of highly sensitive files belonging to a billion-dollar technology company. Sharp stole dozens of so-called secrets files from Company-1's AWS Secrets Manager, a cloud password management tool. Sharp also stole over 1,400 AWS task definitions files, and over 1,100 GitHub code repositories where Company-1 stored its development files and proprietary code. Sharp's theft took this confidential and valuable protected data from Company-1's secured network and copied it onto a laptop on Sharp's home. This, in and of itself, was an extremely serious cyberattack that required well over $1.5 million dollars and hundreds of hours of employee and consultant time to fully identify and remediate.

But Sharp did not stop there. To cover his tracks, he deleted and tampered with various AWS logs that Company-1 had set up as part of its cybersecurity measures that would help detect

breaches. The deletion of those logs made it more difficult to identify the scope and pattern of the attack. In addition to deleting logs and masking his own identity with a VPN, Sharp also attempted to implicate his coworkers in the attack. Between December 22 and 26, 2020, Sharp manually renamed at least 18 AWS sessions that he opened to conduct the attack with the naming convention associated with five other Company-1 DevOps team members. Put another way, Sharp made it seem like five of his fellow coworkers on the DevOps team—whom he knew and worked with—actually conducted various malicious Surfshark-masked sessions, rather than himself. On December 22, 2020 alone, Sharp stole over 1,000 GitHub repositories and also renamed eight malicious AWS sessions conducted through Surfshark VPN to make it appear as if they were conducted by three different co-workers. Sharp's willingness to manufacture evidence implicating innocent coworkers for an extremely serious hack, notwithstanding the possible consequences to them, shows an extreme ruthlessness that is utterly deserving of the Guidelines range.

Nor did Sharp cease his criminal conduct when the breach was discovered by other employees at Company-1. He swung into action as a tireless investigator and team player, spending hours supposedly remediating the attack and brainstorming its causes, while secretly impeding the discovery of its true manner and means. And Sharp did not stop there. Acting on pure greed and desire to further harm Company-1, he extorted it—as the anonymous attacker— for close to two million dollars to return the stolen data and identify purported backdoors. Sharp's decision to pursue the extortion plan and send the ransom note *ten days* after the discovery of the breach evidences his extreme confidence that he successfully covered his tracks and could now stand to reap his rewards.

When Company-1 did not pay the reward in the time allotted, Sharp was not content to let the scheme go. He wanted to continue to hurt Company-1. And so, Sharp published stolen secrets and task definitions on a public online folder—which Company-1 was able to quickly take down.

This attempted disclosure of highly sensitive proprietary data that Sharp stole further aggravates his offense and requires serious punishment.

Sharp knew that the FBI was investigating this offense from his days on the remediation team. He obstructed that investigation in multiple serious ways. After the FBI's involvement was known to him, Sharp wiped the laptop he used to steal company data. And when the FBI arrived at his home to execute a search warrant, he lied, repeatedly and explicitly, about his non-involvement in the attack and the means by which the attack was carried out. Sharp offered multiple theories for how the true attacker could have committed the crime, even as he knew that the FBI had found and seized the laptop Sharp used to commit this offense. At every turn, Sharp acted consistent with the unwavering belief that his sophistication and cunning were sufficient to deceive others and conceal his crime.

And then, undeterred by the FBI's confrontation and the fact that a federal judge had already found probable cause that his own home contained evidence of this crime, Sharp set out to revictimize Company-1. He callously pretended to be an anonymous whistleblower, falsely accusing Company-1 of misrepresenting to its customers the scope of the attack he perpetrated. This spiteful attack carried dramatic consequences for Company-1 and anyone who owned stock in Company-1. In a single day after Sharp caused a false article to be published, billions of dollars of value were lost. The defendant knew the consequences of his actions and ran at least seven internet searches for Company-1's stock price on that day. Even that was not enough for Sharp. He then tried to incite investigations by U.S. and foreign regulators into Company-1 based on the same lies.

The applicable Guidelines section, Section 2B1.1, appropriately focuses on the financial harm caused by the defendant's actions. The defendant, having made a conscious decision to abuse the authority placed in him by a major technology company – an institution housing troves of

proprietary confidential data – is rightly responsible for the many steps taken and associated costs incurred by Company-1 in investigating the compromise, rooting out the intruder, and engaging in appropriate remediation. *See* U.S.S.G. § 2B1.1, Application Note 3(A)(v)(III) (defendants convicted of 18 U.S.C. § 1030 responsible for "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service," even where "such pecuniary harm was not reasonable foreseeable"); *see also United States* v. *Musacchio*, 590 F. App'x 359, 365 (5th Cir. 2014) ("Note 3(A)(v)(III) was designed to more fully account for specific factors relevant to computer offenses") (internal quotations omitted, emphasis in original).

Insofar as financial remediation loss largely drives the offense level under Section 2B1.1, however, the Guidelines in this case do not capture the more pernicious harm caused by the defendant's conduct aimed at destroying Company-1's reputation with its customers, shareholders, regulators, and the public market at large, which resulted in literally billions of dollars in losses. That harm is plainly extensive and deserving of substantial punishment.

B. History and Characteristics of the Defendant

The Government respectfully submits that there is nothing in the defendant's personal history and characteristics to meaningfully differentiate him from the heartland of cyber offenders in support of a downward variance. To the contrary, unlike many defendants who appear before this Court, Sharp had a good childhood and grew up in a supportive, stable, nuclear family. PSR ¶ 78. One of four children to his parents, who work as a nuclear engineer and a teacher, Sharp recalled being well taken care of growing up. PSR ¶ 79. He has been married for over 15 years, with five children, has no medical, mental heath or substance abuse concerns, and enjoys a strong family support system. PSR p. 32.

Sharp has been working in the software field since approximately 2009. PSR ¶ 113. As he developed his skills and shifted jobs for higher-paying positions, his compensation increased to approximately $245,000 annually at Company-1 by the time he decided to attack and extort his employer. PSR ¶ 106. He purchased and partially remodeled a four-bedroom home in Portland and was living an apparently comfortable middle class existence before choosing to commit these crimes. PSR ¶ 88-89. Simply put, Sharp's crimes were driven by ego and greed, and not by any financial necessity. He was disgruntled at his employer, planning to leave the company, and wanted to extort millions of dollars and cause damage on his way out.

Although it is true that this scheme represents the defendant's first criminal conviction, his criminal history (or lack thereof) is already factored into the Guidelines. He committed these carefully planned offenses at age 35 and they cannot be chalked up to some youthful indiscretion. The Government recognizes that like all defendants with children, Sharp's sentence of imprisonment will have a negative collateral effect on his family. While unfortunate, that is a consequence solely of Sharp's own making. Indeed, he committed these crimes from home, while his wife and children were around and oblivious to his criminal activities, with no apparent regard to the consequences on them should his crimes be detected.

Sharp has submitted multiple letters attesting to his dedication to his children, technical skills, a suffer-no-fools attitude, and a proffered narrative that he was somehow trying to help Company-1 in a misguided way. *See* Def. Mem., ECF 43-1, Ex. A-B, ECF 44. It is, of course, appropriate for the Court to take these letters into account in connection with sentencing. But these discussions of Sharp's positive personal qualities do not distinguish him from other similarly situated white-collar defendants—individuals who, despite having many opportunities and a network of people who love and support them, nonetheless choose to steal and extort. As Judge Marrero astutely observed, this sort of letter:

> falls into a pattern advanced by a subset of the white collar criminal. . . . The list of their achievements and virtues is long and impressive. Let us count the ways. At home, they are good family men and women, caring spouses, loving parents, loyal and reliable to friends. At work, they are looked up to as outstanding professionals and business partners. To their community's charities and public causes they are generous patrons and sponsors. . . .
>
> Yet, for all of their outward rectitude, these otherwise good people suffer a fatal flaw: they lead a double life. Somewhere at the core, in a distorted dimension of the soul, the public image they present is as false as the lies they tell to sustain the appearances of an exemplary life. And somehow, for reasons that always defy reason, they fall into crime, doing wrongful deeds that seem aberrational, selfish and greedy acts that, when caught, they claim are entirely out of character with their otherwise law-abiding lives.

United States v. *Regensberg*, 635 F. Supp. 2d 306, 308 (S.D.N.Y. 2009), *aff'd*, 381 F. App'x 60 (2d Cir. 2010). Similarly, Sharp's community involvement is not atypical for an educated white-collar offender and does not warrant a downward departure or variance. *See United States* v. *Vrdolyak*, 593 F.3d 676, 682-83 (7th Cir. 2010) ("[I]t is usual and ordinary, in the prosecution of similar white-collar crimes . . . to find that a defendant was involved as a leader in community charities, civic organizations, and church efforts," and the defendant "should not be allowed to treat charity as a get-out-of-jail card" (citation and internal quotation marks omitted)); *United States* v. *Crouse*, 145 F.3d 786, 792 (6th Cir. 1998) (defendant's civic contributions, not atypical for a prominent businessman, did not support nine-level downward departure); *United States* v. *Morken*, 133 F.3d 628, 630 (8th Cir. 1998) (defendant's charitable and other good works did not justify departure from Guidelines); *United States* v. *Haversat*, 22 F.3d 790, 796 (8th Cir. 1994) (defendant's charitable and volunteer activities did not make him atypical).

Sharp, like many white-collar criminals, led a double life. According to his friends and family, he was ambitious, hardworking, a good father and mentor. Yet for a large part of 2020 and 2021, Sharp, conceived, executed, concealed, and lied about a breathtaking hack. Sharp did not target some remote entity. He abused the trust of a company paying him close to a quarter of a

million dollars a year to help keep it safe. Sharp chose instead to steal their data, destroy their cybersecurity logs, frame his own co-workers, extort millions of dollars, and cause untold harm to the company's reputation after he was discovered to have been the perpetrator of the attack.

This sustained attack on his employer was not a fleeting lapse in judgment, or a momentary slip-up. Sharp did not simply log in once, copy a wide swath of files, and get out. This offense involved dozens, if not hundreds, of criminal decisions. Sharp engaged in considerable planning, including the purchase of Surfshark VPN six months before the attack and conducting digital reconnaissance of data he would later copy. Sharp had to know exactly which repositories he wanted to steal and to send specific coded requests targeting those repositories. Using his skill and insider's knowledge of his employer's digital ecosystem, Sharp deleted logs and created false session name artifacts. Then, for days and weeks, he deceived coworkers in intense collaborative meetings as they worked to remediate the hack he secretly perpetrated.

Relatedly, the letter writers' attestations to Sharp's positive qualities (*see, e.g.*, Letter of Brian Bradshaw, Dkt. 43-1 at 18 (referring to Sharp's "honesty with himself and others; his candor about how he views things; his dedication as a father and husband; his steadfastness as a friend and a mentor") should be taken with a grain of salt. In the course of conducting this attack and in its aftermath, Sharp skillfully lied to current and former co-workers, company lawyers, federal law enforcement agents, a journalist—and in turn the public—foreign and domestic regulators, and of course, close friends and family to whom he protested his innocence and blamed Company-1 for his own hack. Indeed, as discussed in more detail below, even now, Sharp is blaming the victim and presenting a contrived deception to the Court that this entire offense was somehow just a misguided security drill. Given that Sharp was successful in deceiving so many people close to him for so long, his family and friends' views that he is credible or trustworthy do not bear significant weight.

Third, to the extent that Sharp or the letter writers suggest that the defendant's loss of professional standing as a result of his conviction warrants a lighter sentence (*see, e.g.*, Def. Mem. at 8 ("Ruin of Reputation: Collateral Punishment . . . The humiliation associated with his conviction is something Mr. Sharp, as a 37-year-old, must confront daily for the rest of his life"), this claim should be rejected. "It is impermissible for a court to impose a lighter sentence on white-collar defendants than on blue-collar defendants because it reasons that white-collar offenders suffer greater reputational harm or have more to lose by conviction." *United States* v. *Prosperi*, 686 F.3d 32, 47 (1st Cir. 2012) (citing U.S.S.G. § 5H1.2); *see also United States* v. *Musgrave*, 761 F.3d 602, 608 (6th Cir. 2014) ("In imposing a sentence of one day with credit for the day of processing, the district court relied heavily on the fact that Musgrave had already 'been punished extraordinarily' by four years of legal proceedings, legal fees, the likely loss of his CPA license, and felony convictions that would follow him for the rest of his life. '[N]one of these things are [his] sentence. Nor are they consequences of his sentence'; a diminished sentence based on these considerations does not reflect the seriousness of his offense or effect just punishment." (citation omitted)).

Accordingly, even crediting the testimonials Sharp has submitted in connection with sentencing—and the Government does not in any way question their sincerity—the defendant has shown himself to be an inveterate liar and data thief, and not someone who deserves any benefit of the doubt with respect to this Court's judgment of his character.

C. The Need to Afford Adequate Deterrence

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). "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.*

The difficulty of investigating increasingly sophisticated hacking offenses elevates the need for general deterrence. In the modern professional workplace, sophisticated information technology specialists entrusted to maintain the integrity of workplace technology can abuse that access to devastating ends. A significant prison sentence—within the Guidelines range—is necessary to send a message that any such violation of trust will be met with serious punishment.

There is a heightened need for specific deterrence in this case. The defendant was not deterred by the prospect of losing his job and facing criminal charges while stealing his employer's files over and over again in December 2020. If other employees had not discovered the fact of a breach, it is at a minimum possible that the defendant would have continued to hack, steal files, alter logs, and frame co-workers. In January 2021, Company-1's discovery that the defendant's own home IP address was implicated in the offense did not deter him from carrying on with the scheme to victimize Company-1. He first put on a remarkable act across a series of messages, writing to the employee who first asked him about the IP address, "I can swear on anything in [the] world that I have literally no clue and don't have that repo on my computers and never have… but that looks like I did… so can we trust? . . . I think we need to lay it out… right?" "We need to war[]game it . . . fuck me… my heart… could be the caffeine but wtf", "my paranoia is off the fucking charts." Sharp attempted to turn the IP slip-up into the notion that someone else could be framing him for the offense and spreading doubt: "I'd be pretty fucking incompetent if I left my ip

in [the] thing I requested, downloaded, and uploaded" "shittiest cover up ever lol" "fuck it makes no sense except to spread doubt".

Then, despite having learned that his own IP was detected as part of the hack, Sharp chose to continue to cause harm and attempted to disseminate Company-1's pilfered data publicly. Subsequently, Sharp was entirely undeterred by the fact that the FBI had obtained a search warrant and had seized evidence of the crime from his home. He chose to again lash out at Company-1, spreading false news stories and whistleblower complaints about the attack he conducted. This is powerful evidence that in some real way, the defendant is undeterrable from committing misconduct when feeling aggrieved. Even now, as discussed below, Sharp presents a narrative that blames Company-1 and attempts to justify his actions as some sort of security drill. The Government respectfully submits that a Guidelines sentence is necessary to truly impress upon Sharp the wrongfulness of his actions and deter him from future misconduct.

V. Sharp's Arguments

Appearing to utterly ignore the severity of his offenses, Sharp argues for a sentence of no prison time, with a year of home confinement. Def. Mem. 10. In support of that request, Sharp has submitted an extraordinary letter to the Court, claiming that he engaged in this behavior because the CEO of Company-1 was somehow "preventing" his team from resolving outstanding security issues. ECF No. 43-1 at 20. He claims that his motivation for this crime was not malice or greed, but rather a desire to "point out weaknesses" in Company-1's security infrastructure and to help the company. *Id.* These self-serving assertions, which appear to continue the defendant's pattern of victimizing the company, are unsubstantiated by the evidence developed during the Government's investigation, and raise serious doubts that Sharp is truly accepting responsibility for his offense.

The defendant's new claim to have been conducting an "unsanctioned 'security drill'" for

Company-1's benefit, *id.*, is contradicted by the unobjected-to Presentence Report, which correctly concluded that the instant offense was motivated by financial gain. (PSR at p.32) At the time of his presentence interview, far from presenting himself as a cybersecurity vigilante trying to do right by his company, Sharp admitted "he felt mistreated by Company-1, noting that he was on call for long hours and cited that he left the company for 'more money and less stress.'" *Id.*

Indeed, the defendant's attempts to rationalize his own crimes after the fact are belied by his own actions. To begin with, Sharp is completely wrong that he merely engaged in a "security drill" to force the company to resolve supposed outstanding issues. This was not a "drill" in any meaningful sense of the term. Far from a hacker targeting a vulnerability open to third parties, Sharp used credentials legitimately entrusted to him by the company, to steal data and cover his tracks. Sharp *actually* stole data from the company, *actually* deleted the company's existing cybersecurity measures, *actually* attempted to frame innocent coworkers,[9] *actually* attempted to extort the company for millions of dollars, and then *actually* released the company's sensitive data on a public folder when the company refused to pay. Sharp (acting as the anonymous hacker) did not even reveal to Company-1 how the hacks were executed when Company-1 refused to pay him. Sharp was not engaging in a drill—he was actually attempting to harm Company-1 and make millions of dollars off of his crime. Sharp's own motives are also belied by the fact that Sharp had successfully applied for (and later obtained) a job at a different company, just days before he began stealing data from Company-1 at the end of 2020. Sharp had no interest in the long-term success of Company-1—he was already planning to leave the company, and it is clear that his goal was to hurt Company-1, embarrass his former co-workers and supervisors, and profit off of his crimes on

[9] Sharp ignores all these facts in his self-serving letter, and "apologizes to [his] colleagues" solely for making them "suffer unnecessary stress and unplanned work" due to his so-called "unsanctioned exercise". ECF No. 43-1 at 20.

his way out of the company.

Indeed, there is no evidence that Sharp would have even stopped the intrusion in late December 2020 had it not been discovered by other Company-1 employees independent of Sharp. *See, e.g.*, PSR ¶¶ 34-35 (other employees' discovery of intrusion two days after Sharp deleted logs to conceal own actions). Sharp remarkably attempts to take credit for all the remediations Company-1 undertook with the assistance of an outside forensic company afterwards, ignoring the fact that he was actively lying to the company about the intrusion and its potential causes during this time. Sharp's actions after the hack was discovered and remediated further demonstrate his true motives. If Sharp was truly interested in helping Company-1 to remain secure and to protect Company-1's customers, Sharp's crimes would have stopped after Company-1 took the remediation steps that he described in his letter. But instead, Sharp duped a cybersecurity journalist into publishing Sharp's whistleblower false statements about the cause and scope of the intrusions—leading to the company's stock price plummeting billions in value, hurting the company, its employees, and its shareholders.

The defendant's so-called "drill" also obstructed law enforcement. He destroyed evidence on the laptop he used to commit the crimes, and he made false statements to the FBI when confronted with evidence that he was responsible—all in an attempt to impede a governmental investigation. Even after being charged with the crimes in December 2021, Sharp did not admit guilt or accept responsibility for months. Rather, it was not until February 2023—more than a year later and just a few weeks before trial—when Sharp finally pleaded guilty and admitted that he was responsible. All of this behavior shows that the defendant committed these crimes out of greed and a desire to harm Company-1, not for any benevolent purpose. Ultimately, Sharp's misguided and unremorseful attempts to justify his behavior in advance of sentencing demonstrate that the defendant has not truly accepted personal responsibility for his crimes or appreciated the

gravity of the harm that he caused, even if he has admitted to engaging in the criminal conduct.

VI. Conclusion

Given the facts here, a sentence within the Guidelines range of 97 to 121 months is appropriate and just. Such a sentence would adequately reflect the seriousness of Sharp's crimes, provide just punishment, and send a message to would-be hackers that a substantial jail term is the likely consequence of such criminal conduct. A sentence substantially below the Guidelines range would be perceived by the public and the victim as a slap on the wrist and would fail to serve the essential sentencing goals of providing just punishment, affording deterrence and promoting respect for the law.[10]

Dated: New York, New York
May 3, 2023

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: /s/
Vladislav Vainberg
Andrew K. Chan
Assistant United States Attorneys
(212) 637-1029 / 1072

cc: Defense counsel (via ECF)

[10] Sharp also should be ordered to forfeit his interest in any personal property used to commit or to facilitate the commission of these offenses, including specific devices seized by law enforcement that will be detailed in a proposed order submitted to the Court. Consistent with his plea agreement, Sharp should be required to pay restitution of $1,590,487 to Company-1.