UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA v. AVIRAM AZARI, *Defendant*.	**S1 19 Cr. 610 (JGK)**

GOVERNMENT'S SENTENCING MEMORANDUM

DAMIAN WILLIAMS
United States Attorney
Southern District of New York

Juliana N. Murray
Olga Zverovich
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

I. PRELIMINARY STATEMENT

The United States respectfully submits this memorandum in connection with the sentencing of defendant Aviram Azari, scheduled for October 18, 2023, at 2:30 p.m., and in response to defendant's sentencing memorandum filed on October 6, 2023 ("Def. Mem.")

Azari played a critical role in executing a massive computer hacking campaign that targeted thousands of victims worldwide. Clients of Azari's Israeli private intelligence company paid Azari more than approximately $4.8 million over a nearly five-year period—from November 2014 through his arrest in September 2019—for managing intelligence-gathering and spearphishing campaigns. Azari executed his crimes deliberately and over an extended period of time, and did so primarily for his own self-enrichment, with no regard for the devastating personal, financial, and reputational impact this hacking had on his victims.

Despite Azari's and his co-conspirators' use of numerous aliases and anonymous emails, and their further efforts to evade law enforcement, U.S. law enforcement not only identified Azari, but also brought him to justice—a difficult achievement in the world of international cybercriminal investigations and prosecutions. Azari's sentence should reflect not only the enormous destructive impact that he has inflicted through his criminal conduct, but also serve as a clear message to deter other would-be criminals, here and elsewhere, from hacking and victimizing U.S. individuals and companies.

A Guidelines term of imprisonment is warranted to reflect the seriousness of the offense, to promote respect for the law, to avoid unwanted sentencing disparities, and to provide adequate deterrence.

II. STATEMENT OF FACTS

A. The Defendant's Offense Conduct

Until his arrest in September 2019, Azari, an Israeli citizen, operated an Israeli intelligence firm referred to as "Aviram Hawk" or "Aviram Netz." (Presentence Investigation Report ("PSR") ¶ 18; Dkt. 56). Clients hired Azari to manage various "Projects" that were characterized as intelligence-gathering efforts, but were, in fact, hacking efforts specifically targeting certain groups of victims. Once tasked with a Project, Azari employed the services of different hacking groups. (PSR ¶ 11). Azari facilitated the hacking scheme by directing groups of hackers, including a particular group of individuals based in India, to target specific victims' online accounts for hacking. (PSR ¶ 12). The hackers Azari hired would steal users' credentials, primarily by sending spearphishing emails that were designed to appear as though they originated from trusted sources (such as Google, Yahoo, and Apple, or the victims' employers).

By way of background, during a spearphishing attack, an email is sent to a target that induces the target to take action that will allow the sender to obtain unauthorized access to the recipient victim's account or system. This can be accomplished in a number of ways, including by: (a) tricking the target into clicking on a link or downloading an attached file that actually contains malicious software, or "malware," that infects the victim's account or system and provides the attacker with unauthorized remote control or access to the target account or system; or (b) tricking the target into unwittingly providing his account credentials (username and password) to allow the attacker to remotely login to, and obtain unauthorized access to, online accounts or systems. Oftentimes the attackers will conduct research on their targets (including the targets' interests, the types of online services online services to which they subscribe, or the

individuals with whom the targets frequently communicate) in order to trick the victims and gain unauthorized access.

When the victims clicked on links in these spearphishing emails, they would be redirected to servers that appeared to be legitimate web pages, either for the provider in question or for the victim's employer but that were, in fact, controlled by the hackers. When the victims attempted to log in to those websites, the hackers would steal, or "harvest," the victims' credentials—including their usernames and passwords. The hackers then used the victims' stolen credentials to gain unauthorized access to the content of the victims' accounts—including their email accounts (both work and personal), social media accounts, and online storage accounts. The hackers updated Azari about their attempted and successful hacking efforts and transmitted the stolen data to Azari, who passed the stolen data along to his own clients. (PSR ¶ 15). The purpose of the hacking was intelligence-gathering on behalf of Azari's paying clients, and Azari paid the hackers whom he had hired to complete the work. The value of the stolen data, as measured by the amount of money Azari was paid by his clients to direct the hacking efforts and provide stolen data, was more than approximately $4.8 million. (PSR ¶ 17).

Details of the Hacking Scheme

As described above, clients hired Azari to conduct various hacking campaigns, which Azari and the hackers he contracted referred to as Projects. Some of these individual Projects targeted victims who were affiliated with the following causes or organizations: (1) climate change advocacy (the "Climate Change Victims"); (2) individuals and companies critical of the (now defunct) German-based payment processor Wirecard A.G. (the "Financial Industry Victims");

(3) employees of the Bahamas gaming authority; (4) members of a Mexican political party; and (5) governmental officials from various African countries.[1] (PSR ¶ 13).

After Azari provided the hackers with information regarding specific Projects' targets, the leaders of the hacking group would task various hackers to work on these Projects. Among other things, the hackers were provided with information on the "Main" (or priority) targets for each Project—including but not limited to their names, their online accounts, and their phone numbers; information on the "Surrounding" targets—or individuals who were related to or "surround" the main targets, such as the main target's family, friends, or co-workers; and online infrastructure to facilitate the execution of the spearphishing campaign. (PSR ¶ 14).

The individual hackers emailed updates regarding their progress on individual Projects to the hacking leaders. These updates included identifying issues that the hackers encountered in attempting to infiltrate the accounts, and/or additional information or resources they needed to successfully hack the accounts at issue. Generally, in instances where an account was successfully hacked, a hacker would send an email to the hacking group leaders with the phrase "Success Report," the name of the Project, and the name of the individual victim. These emails included details evidencing the successful intrusion, including data regarding the type of account and username and password for the target and screenshots showing the inbox or landing page of the compromised account. In certain instances, the screenshots depicted specific searches within the compromised account for communications between the hacked account and other specific email accounts. (PSR ¶ 15). The leaders of the hacking group forwarded these update emails, Success

[1] This summary is merely representative and does not adequately capture the breadth and depth of Azari's spearphishing campaign. As an example, one email between Azari and the leaders of the hacking group in June 2016 identifies ***42*** active hacking Projects, listed in order of priority.

Reports, and tracking spreadsheets along to Azari. Azari would then receive the hacked data, which he passed along to his clients.

Through its investigation, the Government has confirmed the successful hacking of more than 100 of Azari's victims, including victims located in the Southern District of New York. The Government also specifically identified more than approximately 200 additional targets of the hacking Projects that Azari managed. (PSR ¶ 15). However, the true volume of individuals and entities who were targeted by Azari and the hackers he hired during the course of the spearphishing and hacking scheme, many of whom have not yet been identified by the Government, numbers in the thousands and spans the globe. (Dkt. 56 at 3-4).

Azari processed payments he received from clients who hired his firm for the spearphishing campaigns through another of his companies, which was based in Cyprus. During the charged time period, Azari generated approximately $4,844,968 in revenue for his intelligence-gathering efforts, which included the spearphishing Projects described above. Azari paid the hacking groups for their work using these client funds. (PSR ¶ 17).

Examples of Azari's Hacking of Climate Change Victims

One of Azari's Projects was focused on targeting individuals and organizations involved with climate change advocacy (*i.e.*, the Climate Change Victims). Some of the hacked documents that were stolen from various of the Climate Change Victims' online accounts were leaked to the press, resulting in articles relating to the New York and Massachusetts Attorneys General's investigations into Exxon Mobil Corporation's knowledge about climate change, and potential misstatements made by Exxon regarding what it knew about the risks from climate change. In particular, those news articles appeared designed to undermine the integrity of: (i) the state AGs' investigations into Exxon; or (ii) individuals working at the non-profit organizations purportedly involved in influencing the state AGs to investigate Exxon. In addition, the published articles

about the stolen and leaked documents were incorporated into court filings Exxon made in state and federal court while litigating against the state AGs' investigations.

Examples of Azari's Hacking of Financial Industry Victims

Another of Azari's Projects was focused on targeting certain individuals and financial firms that had been critical of the German payment processing company Wirecard A.G. (*i.e.*, the Financial Industry Victims). Specifically, starting as early as 2014, various financial analysts and firms were writing reports about Wirecard's financials and their belief that Wirecard's reported financials were based on fraudulent transactions. These criticisms were reported on by the mainstream financial press, including the Financial Times. In part as a result of these reports regarding suspected fraud at Wirecard, various financial firms took short positions on Wirecard's stock, which was then publicly traded in Germany. Public reporting on this topic also included reports that Wirecard had engaged intelligence and security consultants to surveil individuals critical of, or adverse to, Wirecard, and had targeted those individuals for hacking. Invoices obtained during the Government's investigation reflect that Wirecard was among the clients that hired Azari for intelligence-gathering Projects.

B. Impact of Azari's Crimes on his Victims

As described herein, the long-running spearphishing and hacking campaign that Azari managed targeted thousands of individuals and entities internationally. Several victims have submitted impact statements to the Court in connection with the defendant's sentencing. These victim impact statements detail the tangible and chronic harm caused by the spearphishing campaign and the theft of the victims' identities. Below is a summary of certain of these victims'

descriptions of the emotional, physical, and financial impact they suffered as a direct result of Azari's conduct.[2] For example:

- **Peter Frumhoff** is a climate scientist. Until 2021, Frumhoff worked as the director of science and policy and chief climate scientist at the Union of Concerned Scientists (UCS), which is one of the entities that was targeted for hacking as part of the Project focused on the Climate Change Victims. Frumhoff's work included a "climate accountability" campaign that "sought to spotlight the role of the major fossil fuel companies such as ExxonMobil in funding and spreading disinformation about climate science to try to prevent governmental action to address climate change." Frumhoff explains that he received "repeated, deceptive emails" that "indicated a sophisticated understanding of [his] interests and contacts." Azari and his co-conspirators successfully hacked Frumhoff's work email account, "causing [Frumhoff] a great deal of stress." Frumhoff states that the spearphishing campaign had an "inevitable chilling effect" on his organization's efforts to combat climate change.

- **Kert Davies**, the Director of the Climate Investigations Center, was another of Azari's Climate Change Victims. Davies was targeted for hacking through over 80 distinct spearphishing emails, disguised as messages from his friends, staff, and work colleagues. Davies explains that the "effect of this attack personally and on [his organization's] collective public interest advocacy work was tremendous." Davies describes the "anxiety, paranoia, depression, sleeplessness and fear" caused by Azari's cyber campaign against him and others in his industry. Davies provides details regarding the "most disturbing episode" of the hacking campaign—when a reporter reached out in early 2016, apparently interested in learning more about the non-profit's efforts to expose Exxon's internal studies of climate change as early as the 1980s. Rather than publishing an article supportive of the work of Davies and his colleagues, the reporter eventually published a story leaking details of one of the group's private meetings, along with two versions of the meeting agenda email. Davies states that it is "impossible to quantify how badly these stories and subsequent disparagement of our work have hampered my ability to succeed professionally."

- **Bradley Campbell** is the President of Conservation Law Foundation (CLF), an environmental advocacy organization. In various of his roles as a public official with the Department of Justice and other federal agencies, Campbell led or was involved in

[2] These victims have all consented to their names and details of the harms they suffered at the hands of Azari and his co-conspirators being made public. The Government also directs the Court to [redacted] another of Azari's victims, [redacted], who submitted a victim impact statement to the Court, but has requested to remain anonymous. [redacted]

high-profile regulation or litigation arising from pollution by major oil companies. In advancing work to address climate change and pollution, Campbell confers privately with other environmental leaders engaged in similar or related advocacy. The private meeting agenda and attendee list for one such closed meeting—a January 2016 meeting at the offices of the Rockefeller Family Fund in Manhattan—was leaked to the press "and simultaneously cited on an ExxonMobil webpage designed to dispel criticism of the company's climate stance." Campbell explains that he later learned that he and at least 24 members of his staff were Climate Change Victims (*i.e.*, victims of one of Azari's spearphishing Projects). Campbell describes the harms that Azari inflicted on him, his colleagues, and CLF as "significant and far-reaching." Those harms include substantial out-of-pocket financial costs associated with remediation, including technology upgrades and security. However, Campbell describes the "non-economic harms" from Azari's conduct as "far greater."

- **Dmitri Merinson** was the victim of another of Azari's Projects. Merinson explains that he was involved in a lengthy, costly, and "extremely stressful" court proceedings at the time his email account—which stored personal data and important financial information, as well as all of his confidential legal privileged communications with his lawyers—was hacked. Merinson continues to be "concerned for [his] personal safety" and the safety of his wife and three children "on a daily basis," as a result of Azari's crimes. He explains: "It is hard to understand the impact of Azari's crimes unless you are a victim."

These are the experiences of just four of the *thousands* of victims of Azari's extensive spearphishing and identity theft campaign. Azari's long-running criminal conduct—which he engaged in for his own financial benefit—has had a deleterious and lingering effect on his victims' personal, financial, and professional lives.

C. The Charges, the Defendant's Arrest, and the Defendant's Plea

On August 27, 2019, a sealed superseding indictment (the "Indictment") was filed in this District, charging Azari with conspiracy to commit computer hacking, in violation of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B) (Count One); conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349 (Count Two); wire fraud, in violation of 18 U.S.C. §§ 1343 and 2 (Count Three); and aggravated identity theft, in violation of 18 U.S.C. §§ 1028A(a)(1), (b), and 2 (Count Four).

(PSR ¶¶ 1-5). The defendant was arrested at JFK International Airport in New York on September 29, 2019, and has been detained since his arrest. (PSR ¶ 19).

On April 20, 2022, the defendant pled guilty to conspiracy to commit computer hacking (Count One), wire fraud (Count Three), and aggravated identity theft (Count Four), pursuant to a written plea agreement with the Government. (PSR ¶ 7).

III. THE GUIDELINES RANGE

On July 12, 2022, the Probation Department issued the final PSR for the defendant. The Probation Department calculated a combined total offense level of 29 for Group One (comprised of Counts One and Three). In contrast to the plea agreement, the PSR did not apply a two-level increase under § 2B1.1(b)(11) for this Group, citing the guidance in U.S.S.G. § 2B1.6, application note 2. (PSR ¶ 66). The Government and the defense agree with the Probation Department's Guidelines calculation. (*See* Def. Mem. at 4).

Accordingly, the Court should adopt the PSR's Guidelines calculation of a Guidelines range of 87 to 108 months' imprisonment on Group One (Counts One and Three), with a mandatory consecutive term of imprisonment of 24 months on Group Two (Count Four), for an effective Guidelines range of 111 to 132 months' imprisonment. (PSR ¶¶ 64, 65).

IV. APPLICABLE LAW

Following *United States v. Booker,* 543 U.S. 220 (2005) and *United States v. Crosby,* 397 F.3d 103 (2d Cir. 2005), the Guidelines continue to provide a critical touchstone. Indeed, while the Guidelines are no longer mandatory, they remain in place, and district courts must "consult" them and "take them into account" when sentencing. *Booker,* 543 U.S. at 264. As the Supreme Court has 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 calculating the Guidelines range, 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)(l)-(7). *See 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;
>
> (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).

V. DISCUSSION

Based on the factors set forth in 18 U.S.C. § 3553(a), a sentence within the Guidelines Range of 111 to 132 months' imprisonment is appropriate in this case. Specifically, such a sentence is appropriate to reflect the nature and seriousness of Azari's offense, to provide just punishment for the offense and promote respect for the law, and to afford adequate deterrence to

criminal conduct. *See* 18 U.S.C. §§ 3553(a)(1), (2)(A)-(B).

A. The Seriousness of the Offense, and the Need to Promote Respect for the Law and to Provide Just Punishment

The serious nature and circumstances of Azari's hacking scheme, as well as the need to promote respect for the law and provide just punishment for the offense, counsel strongly in favor of imposing a Guidelines sentence in this case. *See* 18 U.S.C. § 3553(a)(2)(A). For nearly five years, the defendant played a critical role in facilitating an extensive international spearphishing campaign that targeted thousands of individuals and entities for hacking. The conduct was directed: the Projects appear designed to undermine specific public interest groups or individuals and entities who took positions adverse to (or merely inconvenient for) various causes. The conduct was incredibly sophisticated: it involved extensive research into the family members, associates, hobbies, and habits of the hacking targets. And the conduct was *personal*: it has wreaked financial, professional, emotional, and physical devastation on Azari's victims.

The defendant knowingly took part in these crimes, and he profited handsomely for his role managing various hacking groups located in India and elsewhere and tasking them with stealing the identities and personal property of the victims of his hacking campaign. Azari pocketed millions of dollars for his oversight of the hacking groups, and he passed along the fruits of their hacking to his clients. He exhibited zero regard for the harm inflicted on his victims.

Azari's conduct had a devastating effect on the victims whose identities were stolen and misused; whose online accounts were taken over; whose communications and files were stolen and sold for Azari's own profit; who were tormented by the intrusions. Examples of the impact of the defendant's conduct on his victims, as presented in the victims' own statements to the Court, is summarized above. Azari and his co-conspirators stole their victims' identities; the victims' stolen names and passwords were then used to gain unauthorized access to their personal and

professional emails, documents, and communications; and, after that, certain materials that were stolen through those hacking efforts were published for all the world to see and, in some cases, were even used in an effort to undermine the work of these victims. The chronic harms described in the victim impact statements submitted to the Court are undoubtedly shared by countless other victims of the defendant's crimes.

The Government acknowledges the defendant's arguments for leniency. He cites the difficult conditions of confinement during the COVID-19 pandemic (Def. Mem. at 4-6, 24), and the health issues he has suffered during that confinement. (Def. Mem. at 6-11). The defendant reports having a supportive family (Def. Mem. 17-20), and highlights his prior military service (Def. Mem. at 12-17), and service to his community. (Def. Mem. at 20-21). The defendant has accepted responsibility and expressed remorse for his crimes and their impact on his victims. (Def. Mem. at 22). However, the Government submits that, when weighing these Section 3553(a) factors against the severity and extensive scope of the defendant's crimes—and the harm they inflicted and continue to inflict on his thousands of victims—the defendant's conduct warrants a sentence within the Guidelines range.

B. <u>The Need to Avoid Unwarranted Sentence Disparities Among Similarly Situated Defendants</u>

A Guidelines sentence such as that sought by the Government would also comport with "the need to avoid unwarranted sentence disparities among defendants." 18 U.S.C. § 3553(a)(6); *see also United States v. Ghailani*, 733 F.3d 29, 55 (2d Cir. 2013). As described above, Azari's criminal conduct was wide ranging and targeted a variety of industries. When compared against sentences for defendants convicted of hacking offenses of equivalent breadth, scope, and duration, a Guidelines sentence for Azari ensures that there are no unwanted sentencing disparities between Azari and other similarly culpable defendants. In this District and elsewhere, the sentences for

sophisticated hackers imposed by judges have been significant and lengthy. For instance, in *United States v. Tyurin*, No. 15 Cr. 333 (LTS), the defendant engaged in an extensive computer hacking campaign targeting financial institutions, brokerage firms, and financial news publishers in the U.S., and was responsible for the theft of personal information of over 100 million customers of the victim companies, earning over $19 million in profits for his far-reaching cyber campaign. The advisory Guidelines range for the defendant was 188 to 235 months' imprisonment. *See id.*, Gov't Sentencing Mem., Dkt. No. 165 (Dec. 1, 2020). Judge Swain sentenced the defendant to 144 months. In *United States v. Jeremy Hammond*, No. 12 Cr. 185 (LAP), the defendant was a recidivist computer "hacktivist" who between 2011 and 2012 hacked numerous businesses, individuals, and local law enforcement-related entities to deface websites and steal and post personal data, resulting in losses between $1 million and $2.5 million. The advisory Guidelines range for the defendant was the statutory maximum of 120 months' imprisonment; but for that statutory cap, the range otherwise would have been 151 to 188 months. *See id.*, Gov't Sentencing Mem., Dkt. No. 60 (Nov. 12, 2013). Judge Preska sentenced the defendant to 120 months. In *United States v. Hamza Bendelladj*, No. 11-CR-557-AT-2, in the Northern District of Georgia, the defendant, an Algerian-national hacker who managed botnets and used them to steal bank and credit card information belonging to 200,000 people, was arrested in Thailand while he was in transit from Malaysia to Algeria, extradited to the United States, and subsequently pled guilty to 23 felony counts. *See id.*, Gov't Sentencing Mem., Dkt. No. 158 (Mar. 2, 2016). Ultimately, Bendelladj's offense level was calculated as 34, yielding a Guidelines range of 151 to 188 months' imprisonment, and he was sentenced to 143 months' imprisonment. *See id.*, Dkt. No. 242, at 5 n.4 (Nov. 20, 2019) (adjusted Guidelines calculation in light of incorrect application of § 2B1.1(b)(4) enhancement); Amended Judgment, Dkt. No. 254 (Mar. 24, 2020). Finally, in *United States v.*

Yevgeniy Nikulin, No. 16 Cr. 440 (WHA), in the Northern District of California, the defendant, a Russian national, was found guilty after trial of hacking into LinkedIn, Dropbox, and another social networking company. The evidence at trial established that the defendant installed malware on the victims' networks, stole and then used login credentials for employees, and subsequently conspired to sell customer data stolen from these networks. It is the Government's understanding that the advisory Guidelines range was 108 to 131 months' imprisonment, with a mandatory consecutive 24-month term; the Judge sentenced Nikulin principally to 88 months' imprisonment, citing general deterrence as a significant factor in his sentencing decision, and expressing his hope that the sentence would send a clear message to deter anyone—including persons abroad—from engaging in similar conduct. *See id.*, Gov't Sentencing Mem., Dkt. No. 277 (Sept. 22, 2020); Judgment, Dkt. No. 281 (Oct. 5, 2020); Press Release, "Russian Hacker Sentenced to Over 7 Years in Prison for Hacking into Three Bay Area Tech Companies."[3]

In sum, in cases in this District and elsewhere, the significant incarceratory sentences that have been issued for defendants similarly situated to Azari strongly counsel in favor of a significant period of incarceration in this case within the Guidelines range.

C. <u>The Need to Afford Adequate Deterrence</u>

The sentence sought by the Government is also necessary here to "afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). The public's interest in deterrence is particularly acute in cases like this because deterrence is essential to reducing the ever-increasing costs of computer hacking. Deterrence is also a critical consideration in this defendant's case. The defendant played a vital link in this global hacking and identity theft chain. His crimes had

[3] *Available at* https://www.justice.gov/usao-ndca/pr/russian-hacker-sentenced-over-7-years-prison-hacking-three-bay-area-tech-companies (*last visited* October 12, 2023)

devastating effects on real victims and continue to haunt those victims to this day. And Azari's crimes show how easy it is for others to commit similar hacking and identity theft crimes. The defendant and his co-conspirators showed an utter disregard for the entities and individuals they were victimizing—going so far as to leverage information gleaned about their personal lives to further the crimes.

As was true in this investigation, investigations of major hacking cases are challenging. Investigators and law enforcement must work quickly to collect and preserve data from around the world before the bad actors have destroyed or encrypted it, analyze that data to accurately attribute the work to a particular individual, and then successfully apprehend that individual, oftentimes relying on extradition requests of foreign countries. Indeed, even in instances where U.S. law enforcement successfully collects evidence and identifies the bad actors at issue, bringing those individuals to justice in a U.S. court poses its own challenges, and the Government publicly announces charges without apprehending the defendants. *See, e.g.*, *United States v. Rafatnejad et al.*, 18 Cr. 94 (JMF) (charges announced against nine Iranian nationals who conducted cyber theft campaign against universities and companies to steal research, academic and proprietary data); *United States v. Hua et al.*, 18 Cr. 891 (VSB) (charges announced against two Chinese hackers who targeted intellectual property and confidential business information); *United States v. Iat Hong et al.*, 16 Cr. 360 (SHS) (charges announced against four individuals for insider trading based on information hacked from U.S. law firms; extradition request for defendant arrested in Macau was denied).

As a result of the significant resources required to successfully prosecute hackers, convictions are relatively rare. Consequently, the importance of affording general deterrence through meaningful sentences is particularly acute in criminal hacking cases: where the incidence

of prosecution is lower, the level of punishment must be higher to obtain the same level of deterrence. Moreover, the need for general deterrence is greatest in cases involving lucrative and difficult-to-detect hacking schemes, such as the sophisticated scheme that Azari managed. In light of the substantial public interest in this case, including its coverage in the press, the sentence that Azari receives will send a message to others here and elsewhere about the consequences they may face if they engage in similar behavior.

Judges in this District have recognized the need for general deterrence in hacking cases such as Azari's. For instance, in *United States v. Knowles*, 16 Cr. 5 (PAE), the defendant pled guilty to having hacked into email accounts of victims in the entertainment, sports, and media industries, and stolen scripts of movies and television shows that had yet not yet aired, as well as personally identifiable information of the victims. After determining that the appropriate Guidelines range was 27 to 33 months' imprisonment—a range significantly lower than Azari's—Judge Engelmayer sentenced the defendant principally to an above-Guidelines sentence of 60 months' imprisonment. In imposing this sentence, Judge Engelmayer articulated the importance of general deterrence as follows:

> At a time when much of the world has a presence on the Internet, at a time when so many people in this country and abroad keep sensitive material on line, whether personal data or confidential business information or works, at a time when remote hacking is regrettably an all-too-common topic in our news, it is vitally important that the law muscularly respond to the modern-day pirates like you who would plunder that material.
>
> The sentences in such cases of cybercrime need together to send a message that significant punishment awaits hackers who access accounts for purposes of theft and self enrichment. The sentence imposed here has the potential to convey that message to those, Mr. Knowles, who would follow your lead.
>
> That message is particularly acute in the context of international hackers. You carried your scheme from the Bahamas. Only the creative sting arranged by the undercover lured you to the United

> States where you were arrested. But for hackers who operate for abroad who damage the lives and business interests of Americans by remote means, it will often be hard to law enforcement to catch up with them.
>
> It's an unfortunate reality, but between different legal regimes, limited across-border cooperation among law enforcement, and the inherent challenges of identifying and catching cyberthieves, the difficulty of apprehending an overseas hacker is reality. So it is all the more important that when a hacker from outside the United States is caught, the punishment be meaningful to convey to others who operate from afar, so that even if the likelihood of apprehension may not be great, the consequences will be.
>
> I judge the interest in general deterrence as substantial.

See Knowles, Sentencing Tr. 49-51 (Dec. 6, 2016). Azari's criminal activity is greater in magnitude, scale, and duration than that of Knowles, and thus the punishment should be commensurately greater than that of Knowles.

As is clear from this case, it is all too easy to do what the defendant did, all too attractive, and all too difficult to detect until the fraud has reached a substantial scale. For these reasons, a meaningful sentence is warranted. *See, e.g.*, *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) ("Because economic and fraud-based crimes are 'more rational, cool, and calculated than sudden crimes of passion or opportunity,' these crimes are 'prime candidate[s] for general deterrence.' (quoting Stephanos Bibas, *White-Collar Plea Bargaining and Sentencing After Booker*, 47 Wm. & Mary L. Rev. 721, 724 (2005)) (alteration in original)); *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."); Francesco, Galbiati & Vertova, *The Deterrent Effects of Prison: Evidence From a Natural Experiment*, 117 J. of Political Econ. 257, 278 (2009) ("Our findings provide

credible evidence that a one-month increase in expected punishment lowers the probability of committing a crime. This corroborates the theory of general deterrence.").

The Court can—and should—send a strong message to others about the serious consequences of engaging in such flagrant criminal conduct. Spearphishing campaigns and identity theft schemes like the one the defendant perpetrated for years impose ruinous consequences on victims, and that conduct must be severely punished. Sentences for multi-year criminal hacking schemes, where hackers such as Azari engage in the conduct against U.S. victims from the comfort of their homes thousands of miles away, should be substantial, in order to afford adequate deterrence.

VI. CONCLUSION

Azari's crimes were extensive and devastating. Azari leveraged his unique skills and connections over an extended period of time to direct the targeting of thousands of victims around the globe. The cyberattacks were personal, and they have had continuing and lasting impacts on his victims.

Based on the facts and arguments set forth above, the Government respectfully submits that a significant Guidelines sentence is appropriate in this case.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

by: */s/*
Juliana N. Murray
Olga Zverovich
Assistant United States Attorneys
(212) 637-2314/-2514