IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. CONOR BRIAN FITZPATRICK, a/k/a "Pompompurin" Defendant.	Case No. 1:23-CR-119 Hon. Leonie M. Brinkema Sentencing: January 19, 2024

POSITION OF THE UNITED STATES WITH RESPECT TO SENTENCING

Defendant Conor Brian Fitzpatrick was the founder and lead administrator of BreachForums, an online website and cybercrime forum that was dedicated to furnishing the cyber underworld with access to customer and user databases that hackers stole from victim companies, organizations, and governmental entities. These databases often contained the sensitive personally identifying information (PII) of millions of Americans.

Created in March 2022, BreachForums quickly developed into the largest English-language data breach forum of its kind and fueled the illicit market for high-profile databases through two principal means. First, BreachForums operated an illegal marketplace where its more than 300,000 members could solicit for sale and purchase breached databases and other contraband, including stolen access devices, tools for committing cybercrime, and other services for gaining unauthorized access to victim systems. To support these efforts, the defendant enabled BreachForums members to post solicitations concerning the sale of hacked or stolen data on BreachForums, exchange direct private messages through a BreachForums private messaging function, and conduct secure transactions through a trusted "middleman" or escrow service that

the defendant personally operated. Second, BreachForums managed a section titled "Official" through which the defendant directly provided the forum's paying members with access to approximately 888 stolen databases containing over 14 billion individual records. These records included customer databases stolen from a wide variety of companies, organizations, and government agencies located in the United States and elsewhere.

The defendant did all of this knowing that his criminal service was illegal. Indeed, the defendant created and designed BreachForums with the express purpose of creating a substitute for Raidforums, the prior leading English-language data breach forum whose operations had been disrupted by law enforcement through the public arrest of its founder and seizure of its computer infrastructure in January and February 2022.

In addition, at the time of the defendant's initial arrest on March 15, 2023, evidence was recovered from a device seized from the defendant's home pursuant to search warrants that showed he knowingly possessed approximately 26 video files containing visual depictions of minors engaged in sexually explicit conduct, including videos depicting prepubescent minors.

The defendant has pleaded guilty to an Information charging him with conspiracy to commit access device fraud, in violation of 18 U.S.C. §§ 1029(b)(2) and 3559(g)(1) (Count 1); solicitation for the purpose of offering access devices, in violation of 18 U.S.C., §§ 1029(a)(6) and 2 (Count 2); and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count 3). The applicable Guidelines range has been correctly calculated in the Presentence Investigation Report ("PSR") as 120 months' imprisonment as to Counts 1 and 2 and 188 months to 235 months' imprisonment as to Count 3. *See* Dkt. No. 63 (PSR), at ¶ 122. The United States recommends that the Court impose a sentence of 188 months' imprisonment, which is sufficient, but not greater than necessary, to reflect the seriousness of the crime, the significant harm caused

by the defendant's crimes, the risk of recidivism, and to deter the defendant and others who may seek to profit from this type of widespread cybercrime in the future.

BACKGROUND

From at least in or around October 2020 through 2022, the defendant used the online moniker "Pompompurin" to make posts on Raidforums offering to sell valuable breached databases.[1] PSR ¶ 25. Then, starting in or around March 2022, the defendant leveraged the reputation he built on Raidforums to create and administer BreachForums with the assistance of co-conspirators, including an evolving staff of moderators. *Id.* ¶¶ 18, 26. The defendant and his co-conspirators gained at least $698,714 through the operation of BreachForums. *Id.* ¶ 39.

I. Defendant's Creation and Operation of BreachForums

In March 2022, the defendant founded and became the lead administrator of BreachForums. PSR ¶ 36. The defendant also hired and managed a staff of moderators (i.e., co-conspirators) who played an important role in ensuring that BreachForums operated properly and who performed traditional administrative activity, such as transmitting messages to warn members of conduct that violated BreachForums' rules. *Id.* ¶ 38.

As the name "BreachForums" suggests, the purpose of BreachForums, and the defendant's intent in operating the forum, was to traffic, and aid and abet others in trafficking, breached or

[1] In the modern digital economy, large companies and organizations often collect and store a significant amount of PII about their customers or users in large online repositories known as databases. The types of data stored in customer databases can range from limited identity information, such as customer name, email address, and contact information, to far more sensitive material, such as customer login credentials for accessing online accounts and services, bank account numbers, payment card data, social security numbers, dates of birth, and driver's license information. When this sensitive personal data falls into the wrong hands through computer hacking—often termed "data breaches"—or other means, it can be easily exploited by fraudsters to conduct unauthorized financial transactions or assume the identity of unsuspecting Americans in furtherance of other financial fraud schemes.

stolen databases containing access devices, among other things. PSR ¶ 27. In particular, the defendant intentionally ran BreachForums in a manner that made it an attractive marketplace for cybercriminals to frequent in an effort to buy, sell, or trade stolen or hacked access devices. *Id.*

To achieve these objectives, the defendant took a leading role in all aspects of BreachForums' operations. PSR ¶ 36. Among other things, he (i) designed and administered the website's software and computer infrastructure; (ii) registered domains to host or provide access to the BreachForums website in a manner that prevented the effective identification of him as the person who registered it;[2] (iii) established and enforced the website's rules; (iv) created and managed sections of the website dedicated to promoting the buying and selling of stolen data; (v) operated a middleman service; (vi) approved and uploaded breached databases to the BreachForums' "Official" network for delivering content; and (vii) provided other assistance to BreachForums members seeking to buy and sell illicit material on the website, including by investigating and sometimes vouching for the authenticity of stolen data. *Id.*

In accordance with the defendant's design, any individual with an Internet browser could access and view the BreachForums website without a membership. PSR ¶ 28. However, the website required an individual to sign up for a membership to solicit items for sale or to purchase items. *Id.* BreachForums offered tiers of membership options that cost varying amounts of money, including a "God" membership that offered almost unlimited access to the BreachForums website and features. *Id.*

The defendant further organized the BreachForums website into sections that enabled members to offer, purchase, and provide access to different categories of hacked or stolen data and

[2] Some of the domains registered by Fitzpatrick included breached.vc, breached.to, breachedforums.com, breachforums.net, breachforums.org.

other contraband. PSR ¶ 26. In a "Marketplace" section and "Leaks Market" subsection, for example, BreachForums members bought and sold hacked or stolen databases, tools for committing cybercrime, and other illicit material. *Id.* ¶ 29. Items commonly sold in this section included bank account information, social security numbers, other PII, and login information for compromised online accounts, such as usernames and passwords to access accounts with service providers and merchants. *Id.* BreachForums also supported additional sections in which users posted stolen data and discussed tools and techniques for hacking and exploiting that information, including in the "Cracking," "Leaks," and "Tutorials" sections. *Id.* ¶ 31. Examples of stolen data offered or trafficked in these sections include:

- On December 18, 2022, a BreachForums user with the moniker "USDoD" posted details of approximately 87,760 members of InfraGard, a partnership between the Federal Bureau of Investigation (FBI) and private sector companies focused on the protection of critical infrastructure. PSR ¶ 30.

- On January 4, 2023, information obtained from a major U.S.-based social networking site was posted by a user with the moniker "StayMad." PSR ¶ 30. This information included names and contact information for approximately 200 million users. *Id.*

- On January 21, 2023, a BreachForums user with the moniker "Sin" published a post advertising a list of approximately 20 million user records for a company that controls two U.S.-based background check services ("Victim-1"). PSR at p. 39-40 (Declaration of Victim-1). Victim-1 reports that the breached database contained the PII of user accounts created between 2011 and April 2019, including subscriber name, email address, sparse phone number, password reset token and hashed password. *Id.*

- On March 9, 2023, a BreachForums user with the moniker "denfur" also posted a message revealing the PII of tens of thousands of U.S. citizens. PSR ¶ 30. The message included a link to download a file containing names, dates of birth, social security numbers, employment information, and health insurance information stolen from a health insurance exchange. *Id.*

To facilitate transactions amongst BreachForums members operating in these sections, the defendant offered a "middleman" service in which he acted as a trusted middleman, or escrow,

between individuals on the website who sought to buy and sell information. PSR ¶ 32. The defendant's middleman service substantially facilitated and encouraged the dissemination of hacked or stolen data through BreachForums because it enabled purchasers and sellers to verify the means of payment and contraband files being sold prior to executing the purchase and sale. *Id.* The defendant's standardized middleman process required members to notify him of the "product" they sought to trade. *Id.* In a post announcing the service, the defendant boasted that he had already facilitated over $430,000 in transactions as a middleman with "zero issues" as of November 6, 2022—*i.e.*, the midpoint of the scheme. *Id.* ¶ 45. Examples of the transactions for which the defendant served as a trusted middleman include:

- In July 2022, the defendant served as the middleman for a transaction in which an FBI online covert employee ("OCE") in the Eastern District of Virginia paid a BreachForums user, expo2020, approximately $5,000 to purchase the PII and bank account information of approximately 15 million U.S. persons. PSR ¶¶ 46-47. The defendant facilitated the transaction despite receiving notice that expo2020 was offering "USA FULLZ. Name.ssn.dob.address.dl," and the data included birth dates, social security numbers, and bank account information for use in conducting financial scams. *Id.*

- Likewise, in August 2022, the defendant served as the middleman for a transaction in which an OCE paid a BreachForums user, jigsaw, to buy unauthorized access to the accounting system of a U.S. healthcare company ("Victim-2"), and sample files from the network containing driver's license photos, insurance cards, and partial credit card information for approximately 13 individuals. PSR ¶¶ 48-52. As with the prior purchase, the defendant completed the transaction after being notified that the buyer intended to use the unauthorized access to make money. *Id.* ¶ 51.

BreachForums also managed a section titled "Official," which the defendant described as a "[f]orum where databases stored on our own servers are kept." PSR ¶ 33. As of March 7, 2023, approximately 888 databases containing over 14 billion individual records were available for purchase on BreachForums' Official "content distribution network" (CDN) through a "credits" system that the website administered. *Id.* ¶¶ 33-34. Credits were available for purchase on the website or earned through contributing content. *Id.* BreachForums members seeking to post

databases to the Official BreachForums CDN were required to contact the defendant directly, who would then only upload those databases that he approved. *Id.*

For instance, on May 8, 2022, the defendant approved the addition to BreachForums' Official CDN of a customer database from a U.S.-based internet hosting and security services company that purported to contain the names, addresses, phone numbers, usernames, password hashes, and email addresses for approximately 8,000 customers, as well as payment card information for approximately 1,900 customers. PSR ¶ 42. The approval caused the database to be offered for sale through forum credits to BreachForums members on the Internet, including an OCE who viewed the solicitation. *Id.* On October 27, 2022, the FBI OCE purchased and downloaded this database for 8 credits[3] and confirmed that the database contained apparently stolen customer PII, such as usernames, password hashes, credit card numbers, expiration dates, and card verification values. *Id.* ¶¶ 43-44.

The defendant also knowingly and intentionally provided advice and other support that aided the illicit activities of BreachForums members. PSR ¶¶ 53-55. For instance, in September 2022, the defendant provided a BreachForums member with a roadmap for how to monetize a breached e-commerce database that included approximately 16 million records. *Id.* ¶ 55. In relevant part, the defendant advised the user to first try to extort the victim company for money, and then try to sell the database to others if the victim refused to pay. *Id.* ("I[']d try getting money out of them first, and if they refuse try selling it."). The defendant then explained that he would value the database at about "a few thousand" after the user sought pricing guidance. *Id.*

[3] As of October 20, 2022, credits cost approximately $0.25 each, and were available in bundles of 30, 60, 120, 240, and 500. Various forms of cryptocurrency were accepted as payment.

In addition, the defendant sometimes assured his members that he would help them obfuscate their identities from law enforcement. PSR ¶¶ 53-54. For instance, on May 11, 2022, the defendant sent a private message through BreachForums in which he agreed to delete the registration Internet Protocol (IP) address of a BreachForums member who wanted it deleted "for privacy reasons, I don't want cops randomly scouting it for dumb shit I do." *Id.* ¶ 53. Similarly, on May 24, 2022, the defendant sent a private message to a BreachForums member in which he promised to provide "falsified [registration] information" if law enforcement asked. *Id.* ¶ 54. As part of the reply, the defendant noted "[s]ure, although I doubt law enforcement would even bother making legal requests to a hacking forum lmao."

II. Fitzpatrick's Knowing Possession of Child Pornography

The defendant knowingly possessed approximately 26 digital files depicting minors engaged in sexually explicit conduct. PSR ¶ 56. The defendant saved these files in two folders on his Samsung solid state drive ("Samsung SSD"). *Id.* ¶¶ 56-57. These files included, for example, a video file with 13y-fully-nude in the title, which depicted a minor female who exposed her genitals to the camera and masturbated. *Id.* ¶ 59. The defendant saved this file to his Samsung SSD on February 9, 2023 and later opened it. *Id*. Another video file in the defendant's collection depicted two prepubescent girls who exposed their genitals to the camera and masturbated. *Id.* ¶ 60. The defendant also saved this file to his Samsung SSD on February 9, 2023 and later opened the file after he saved it. *Id*.

III. Procedural History and Pretrial Violation

On March 15, 2023, the defendant was arrested pursuant to a criminal complaint and arrest warrant, which charged him with conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(b)(2). The defendant made his initial appearance in the Southern District of New

York, where he was released on a personal recognizance bond and ordered to comply with pretrial supervision and various other terms and conditions of release. *See* Dkt. No. 10. On March 24, 2023, the defendant made his initial appearance in the Eastern District of Virginia and was ordered to not access VPN software as an additional condition of release. *See* Dkt. No. 16.

On July 13, 2023, the defendant pleaded guilty to a three-count Information that charged him with conspiracy to commit access device fraud, in violation of 18 U.S.C. §§ 1029(b)(2) and 3559(g)(1) (Count 1); solicitation for the purpose of offering access devices, in violation of 18 U.S.C., §§ 1029(a)(6) and 2 (Count 2); and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count 3).

The Honorable T.S. Ellis, III permitted the defendant to remain on bond pending sentencing, but imposed certain additional terms and conditions to the existing bond conditions ordered in March 2023. *See* Dkt. No. 44. Notably, the defendant was ordered to not access a computer and/or the Internet without computer monitoring software installed by pretrial services and that he not use any tools for obfuscating his identity, such as virtual private networks (VPNs). *See id.*

On December 21, 2023, Judge Ellis authorized an arrest warrant for the defendant based on a Petition submitted by the U.S. Probation Office (USPO) detailing the defendant's alleged violation of his conditions of release. *See* Dkt. No. 54. Details concerning the USPO petition and other relevant facts are set forth in Exhibits A and B.

SENTENCING ANALYSIS

I. Statutory Penalties and Sentencing Guidelines Calculations

Counts 1 and 2 of the Information each carry a maximum sentence of 10 years' imprisonment and a term of supervised release up to 3 years. *See* 18 U.S.C. §§ 1029(a)(6) and (b)

and 3853(b). The offense of possession of child pornography carries a maximum sentence of 20 years' imprisonment and a minimum term of supervised release of at least 5 years up to a lifetime term. *See* 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 3583(k).

Here, the PSR correctly calculated the total offense level for the defendant under the Guidelines (USSG) as follows:

Count Group 1: Conspiracy to Commit Access Device Fraud and Solicitation for the Purpose of Offering Access Devices

Guideline	**Offense Level**
Base offense level (USSG. § 2B1.1(a)(2))	6
Loss amount was more than $550,000 but less than $1,500,000 (USSG § 2B1.1(b)(1)(H))	+14
Offense involved 10 or more victims (USSG § 2B1.1(b)(2)(A)(i))	+2
Offense involved receiving stolen property, and the defendant was in the business of receiving and selling stolen property (USSG § 2B1.1(b)(4))	+2
Offense involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means (USSG §2B1.1(b)(10)(C))	+2
Offense involved production or trafficking of any unauthorized access device or counterfeit access device (USSG § 2B1.1(b)(11)(B)(i))	+2
Offense involved the unauthorized public dissemination of personal information (USSG § 2B1.1(b)(18)(B))	+2
Defendant was an organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive (USSG § 3B1.1(a))	+4
Statutory enhancement under U.S.C. § 3559(g)(1) applies (USSG § 3C1.4)	+2
ADJUSTED OFFENSE LEVEL	**36**

PSR ¶¶ 69-81.

The PSR also properly calculated an adjusted offense level of 27 for Count 3 as follows:

Count 3: Possession of Child Pornography

Guideline	Offense Level
Base offense level for a violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (USSG § 2G2.2(a)(1))	18
The material involved a prepubescent minor or a minor who had not attained the age of 12 years. (USSG § 2G2.2(b)(2))	+2
The offense involved the user of a computer or interactive service for the possession, transmission, receipt, or distribution of the material, or for accessing with intent to view the material. (USSG § 2G2.2(b)(6))	+2
The offense involved at least 600 images. (USSG § 2G2.2(b)(7)(D))	+5
ADJUSTED OFFENSE LEVEL	**27**

PSR ¶¶ 82-89.

In the final PSR, the defendant was not awarded a two-level decrease for acceptance of responsibility under USSG § 3E1.1(a), a decision that the government supports for the reasons set forth in Exhibit A. Accordingly, as explained in the PSR, the defendant's combined adjusted offense level of 36 and criminal history category of I results in a Guidelines range of 188 months to 235 months' imprisonment. PSR ¶ 122. Because Counts 1 and 2 have a statutory maximum sentence of 10 years, the Guidelines for those counts are 120 months' imprisonment. *Id*.

II. The Defendant's Objection to the PSR

The defendant has objected to not being awarded a two-level decrease for acceptance of responsibility. The government believes the defendant's objection should be overruled given the defendant's recent pretrial violation.

A defendant may be entitled to a two-level decrease of the offense level "if the defendant *clearly* demonstrates acceptance of responsibility for his offense." USSG § 3E1.1. While entry of a guilty plea prior to commencement of trial may constitute "significant evidence of acceptance

of responsibility . . . this evidence may be outweighed by conduct of the defendant that is inconsistent with such acceptance of responsibility. A defendant who enters a guilty plea is not entitled to an adjustment under this section as a matter of right." *Id.*, comment. (n. 3). Here, the defendant used the Internet to commit his crimes–namely, the creation of an online platform to facilitate the distribution and sale of victim data to cybercriminals worldwide. As part of his administration of this platform, he agreed to assist criminal users of his website in concealing their true identities to avoid detection by law enforcement. Since the entry of his guilty pleas, the defendant has used VPN services to conceal his use of the Internet and has repeatedly utilized an unauthorized and unmonitored electronic device to avoid detection by pretrial services. Thus, while the defendant did in fact plead guilty and admit to his crimes, he has not *clearly* demonstrated acceptance of responsibility since he has continued to engage in evasive behavior that is in direct violation of the orders of two different United States Judges.

III. Sentencing Recommendation

As the Court is aware, the Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).[4] Here, however, a sentence of 188 months (i.e., the low end of the Guidelines) is supported by the defendant's immense contributions to enabling widespread cybercrime, the circumstances of the offense, the risk of recidivism, and the need to adequately deter others from perpetrating similar crimes.

[4] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

A. Nature and Circumstances of the Defendant's Offenses

The known scope, breadth, and brazenness of the defendant's scheme to enable and fuel widespread cybercrime warrants a substantial period of incarceration. Indeed, as detailed above, the defendant's administration of BreachForums played an instrumental role in bringing together more than 300,000 members to solicit, distribute and access thousands of breached databases containing the stolen data of hundreds of companies, organizations, and governmental organizations of varying size and the PII of millions of U.S. persons. *See, e.g.*, PSR ¶¶ 26-52 at p. 33-42. By creating a platform for hackers and fraudsters to connect and conduct business, the defendant made it possible for BreachForums members to commit exponentially more crimes and more sophisticated crimes than any could have done alone. *See* Ben Collier et al., Cybercrime Is (Often) Boring: Maintaining the Infrastructure of Cybercrime Economies, at 1 (Cambridge Cybercrime Centre, 2020) ("It is generally accepted that the widespread availability of specialist services has helped drive the growth of cybercrime.") (hereinafter "Collier, Cybercrime Economies"), *available at* https://www.cl.cam.ac.uk/~bjc63/Crime_is_boring.pdf.

The criminal activity on BreachForums touched nearly every sector of U.S. society. As partly highlighted above, the defendant's victims included U.S.-based healthcare companies, a major public healthcare exchange, public health organizations, the FBI's InfraGard partnership for protecting critical infrastructure, major U.S.-based social media companies, U.S.-based merchants and service providers of varying size, and U.S.-based financial institutions. *See, e.g.*, PSR ¶¶ 26-52 at p. 33-41. The "Official" databases section of BreachForums alone claimed to provide access to approximately 888 stolen databases containing over 14 billion individual records. *Id.* ¶ 34.

The victim impact statements provided by victim corporations and organizations highlight some of the significant and far-reaching consequences of the defendant's crimes. Among other

things, the defendant's conduct has caused victims to (i) devote time and money investigating the data breaches posted on BreachForums and tracking the dissemination of their stolen data on the dark web; (ii) face regulatory scrutiny from the Federal Trade Commission (FTC) and class action lawsuits associated with their data security practices; and (iii) suffer reputational damage and business harm. *See, e.g.*, PSR at p. 33-41.

For instance, the victim impact statement of Victim-1 described how a single post by a BreachForums member, which offered to sell a database containing the sensitive PII of 20 million users of two background check services, caused them to incur direct expenses of more than $180,000 to investigate the data breach and track the movement of their stolen data on the dark web. *See* PSR at 40, ¶¶ 4-8. Victim-1 further detailed how the posts triggered requests from the FTC, and at least one complaint filed by an individual in the Western District of Michigan. *Id.* ¶ 7. To limit the reputational harm caused by the post, Victim-1 also spent approximately $11,492.50 on breach-related public relations.[5]

Likewise, a victim impact statement from a healthcare services company in California ("Victim-3") detailed how a BreachForums member made a post in January 2023 distributing approximately 45,523 lines of stolen data, including PII and Victim-3's source code. *See* Exhibit C (Victim Impact Statement of Victim-3). The data appears to have been stolen through a data breach a month earlier. *Id.* As a result of this incident, individuals whose PII was revealed in the data breach have initiated a class action lawsuit against Victim-3. *Id.* Victim-3 also describes incurring "substantial costs in the form of data breach response and remediation, security controls and improvements, business interruption, and the continued costs of litigation." *Id.*

[5] The government notes that harm to reputation is not a pecuniary harm under §2B1.1.

The activity on BreachForums also targeted the PII of ordinary Americans held by governmental entities. For instance, the Official CDN, which Fitzpatrick personally managed, uploaded a user database of the online training database for the Washington State Food Worker Course. *See* PSR at 42. The data trafficked on BreachForums included the user account information for approximately 1.5 million individuals, including name, date of birth, email address, and zip code, and the driver's license numbers of approximately 9,500 individuals. *See id.*; *see also* Tacoma-Pierce County Health Department, "Data breach exposed Food Worker Card records. We are notifying those affected," *available at* https://www.tpchd.org/Home/Components/News/News/356/286 (July 6, 2023). The Tacoma-Pierce County Health Department reports that the discovery of the breach and associated trafficking of the data on the Official CDN consumed enormous amounts of public resources, including (i) approximately 607 hours of staff time investigating the breach, (ii) approximately 208 hours of staff time responding to emails, phone calls, and public records request, and (iii) approximately 45 hours of communications staff time drafting public notifications, preparing public documentation, sending notifications to 1.5 million email addresses, and responding to the media and the Tacoma-Pierce County Board of Health. *See* PSR at 42. This is time that the staff of the Tacoma-Pierce County Health Department could have spent serving their actual mission—protecting the public health of the county.

As detailed above, Fitzpatrick also personally served as the middleman for another BreachForums member who, without authorization, sold to an FBI OCE access to the accounting system of Victim-2, another healthcare company, and sample PII stored therein. PSR ¶¶ 48-52 and p. 35-37. Although the FBI's involvement mitigated the harm, Victim-2 reports that the

incident still forced three senior engineers to spend approximately 63 hours investigating the breach and ultimately led it to detected unauthorized access from a foreign country. *Id.*

While the sheer volume of criminal activity on BreachForums, the victim impact statements, and the $698,714 of gain attributed to the defendant and his co-conspirators, underscore the seriousness of the defendant's crimes, the parties' stipulated gain enhancement reflects a highly conservative projection of the actual harm that the defendant caused. Indeed, this case presented a number of unique investigative challenges associated with quantifying the harm caused by the defendant's administration of BreachForums; particularly for the many millions of ordinary individuals whose PII was trafficked across the platform and then misused by unidentified BreachForums members to facilitate financial fraud schemes.[6] Indeed, the FBI's annual "Internet Crime Report" for 2022 indicates that approximately $742,438,136 of the $1,201,759,995 reported damages from data breaches in 2022 were suffered by ordinary individuals whose personal data was released into an unsecure environment—*e.g.*, places like BreachForums. *See* FBI Internet Crime Report (2022), at 22, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Further, in a recent report titled "Cost of a Data Breach: 2023," IBM Security reports that data breaches cost the average organization approximately $4.5 million and that customer PII, such as social security numbers, ultimately cost the organization approximately $183 per record. *See* Exhibit D (IBM Security, Cost of a Data Breach: 2023), at 9, 10, 18.

[6] Calculating a precise loss figure is also challenging here because (i) of the diverse array of PII that was sold, offered, and trafficked on the platform, and (ii) many of the customer databases trafficked through the BreachForums Marketplace were not visible to law enforcement. In addition, some victim businesses and organizations have struggled to quantify how the significant negative publicity and regulatory attention caused by the posting of their user databases on BreachForums ultimately impacted their existing business relationships and ability to attract new customers, future investment, and new employees to their organizations.

The defendant's possession of approximately 26 digital files depicting minors engaged in sexually explicit conduct, including two prepubescent minors, is also extremely serious. "It is well established that children featured in child pornography are harmed by the continuing dissemination and possession of that pornography. Such images are 'a permanent record of the children's participation and the harm to the child is exacerbated by their circulation.'" *United States v. Burgess*, 684 F.3d 445, 459 (4th Cir. 2012) (quoting *New York v. Ferber*, 458 U.S. 747, 759 (1982)); *accord United States v. Accardi*, 669 F.3d 340, 345 (D.C. Cir. 2012) ("[C]hild pornography creates an indelible record of the children's participation in a traumatizing activity, and the harm to the child is only exacerbated by the circulation of the materials."). "Every instance of viewing images of child pornography represents a renewed violation of the privacy of the victims and a repetition of their abuse." Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 501(2)(D), 120 Stat. 587, 624 (2006); *accord United States v. Sherman*, 268 F.3d 539, 547 (7th Cir. 2001) (recognizing that "[t]he possession, receipt and shipping of child pornography directly victimizes the children portrayed by violating their right to privacy, and in particular violating their individual interest in avoiding the disclosure of personal matters"). These children "must live with the knowledge that adults like [the defendant] can pull out a picture or watch a video that has recorded the abuse of [them] at any time," and they "suffer a direct and primary emotional harm when another person possesses, receives or distributes the material." *Sherman*, 268 F.3d at 547-48.

Here, through his possession of images and videos of child sexual abuse, the defendant perpetuated the victimization of the children whose exploitation is memorialized in those graphic depictions of their abuse. *See United States v. Daniels*, 541 F.3d 915, 924 (9th Cir.2008)

(explaining that "merely possessing child pornography is not a victimless crime; it fuels the demand for the creation and distribution of child pornography").

B. The History and Characteristics of the Defendant

The defendant's criminal acts were not the product of a momentary lapse of judgement. Rather, for more than a year, the defendant made countless decisions as part of a brazen effort to create and lead the largest English-language data breach forum in the world. *See* PSR ¶¶ 35, 118-119 (indicating that he has never been employed and was not in school after May 2022). The defendant made these choices despite knowing that his conduct was illegal. Indeed, the defendant only elected to create BreachForums in March 2022 after law enforcement had taken down Raidforums and arrested the Raidforums founder in January and February 2022 on similar access device charges. *Id.* ¶¶ 18, 25, 26. For the defendant, the creation of BreachForums reflected a willful and defiant escalation of the types of criminal activity that he began pursuing as a prolific distributor of data breaches on Raidforums in 2020. *Id.* As previously detailed, the defendant's statements to other BreachForums members, use of fictitious identities to register many of BreachForums' domains, and reliance on online aliases to obscure his control over the platform, further highlight the willfulness of his crimes. *Id*. ¶¶ 26, 37, 53-55.

In addition, as previously detailed, the Government received information from a messaging and social media platform indicating that the defendant was engaged in a sustained pattern of violations of his bond conditions even after entering a guilty plea in this case. The defendant's use of one or more unmonitored devices and obfuscation services is particularly concerning here given his history of committing cybercrime through false identities and anonymizing technology. *See also* Exhibit A (discussing history and characteristics of defendant).

Accordingly, although the defendant has no formal criminal history, the government believes the defendant's history of willful defiance of the law and malicious online activity suggests a likelihood of recidivism if left undeterred by a significant term of incarceration. The risk of recidivism is particularly acute here given the defendant's repeated decisions to choose cybercrime over legitimate pursuits despite having opportunities that were never within the reach of many offenders who come before this Court, including a stable upbringing, financial support from his parents, educational opportunities, and impressive technical skills.[7]

In recognition of the defendant's age and medical background, the government proposes a sentence of 188 months that is at the low end of the Guidelines. However, in view of the seriousness of the defendant's sustained and willful conduct, the defendant's history and characteristics do not merit any further variance or departure and support a significant sentence.

C. The Sentence Should Deter Leaders of Organized Cybercrime

According to the Internet Crime Report for 2022, the FBI received reports of 58,859 personal data breaches and 2,795 organizational data breaches that caused complained total losses of approximately $1,201,759,995 in 2022 alone. *See* FBI Internet Crime Report (2022), at 22 and 24. The IBM "Cost of a Data Breach Report" for 2023 estimate that U.S. organizations suffered data breach losses of approximately $9.48 billion. Exhibit D, at 11.

To deter and disrupt cybercriminals who would seek to profit from data breaches, it is critically important to punish the leaders of the cybercrime ecosystem. In recent years, judges in this District have considered, at sentencing, the widespread harm that leaders and organizers of cybercrime inflict. *See, e.g., United States v. Bondars et al.*, 1:16-cr-228-LO (E.D. Va.), Dkt. 233,

[7] "Criminals who have the education and training that enables people to make a decent living without resorting to a crime are more rather than less culpable than their desperately poor and deprived brethren in crime." *United States v. Stefonek*, 179 F.3d 1030, 1039 (7th Cir. 1999).

at 23–26 (sentencing transcript containing Court's observation that defendant who created and operated a tool "facilitating, aiding and abetting enormous numbers of hackers" needed to be deterred and that seriousness of crimes warranted 168-month sentence); *United States v. Burkov*, 1:15-cr-245-TSE (sentencing defendant to nine years in prison for his operation of two cybercrime websites that resulted in over $20 million in fraudulent purchases).

Here, the defendant incentivized and turbocharged the marketplace for data breaches by operating BreachForums in a manner designed to help cybercriminals overcome the "skill, trust, and funding barriers which inhibit the development of truly mass-scale cybercrime economies" and helped buyers "find sellers in scam-ridden underground communities." Collier, Cybercrime Economies, at 5. A significant sentence is needed to deter a future wave of leaders of the cybercrime ecosystem.

Further, as this case illustrates, cybercriminals exploit the invisibility afforded by the Internet, cryptocurrency, and other masking tools to evade detection for many years and earn significant rewards. Indeed, many Internet crimes go unsolved and unpunished due to the tremendous resources it takes for law enforcement to pierce through a cybercriminal's cloak of anonymity. As the Honorable J. Harvie Wilkinson, III observed in *United States v. Carver*, 916 F.3d 398 (4th Cir. 2019), in an access device prosecution:

> Financial fraud is a modern scourge. It preys especially upon the unsophisticated and vulnerable. As the district court noted, crimes like those in this case harm victims 'in almost irreparable ways by causing them loss of work, mental anguish, monetary loss, and loss of peace of mind.' J.A. 152. It raises costs for businesses, which must invest in security measures. These crimes require time and expertise to investigate and can be difficult to unravel and prove.

Id. at 404.

Accordingly, when a sophisticated cybercriminal like the defendant is identified and apprehended, a substantial sentence is needed to deter others from pursuing the same path. *See United States v. Hayes*, 762 F.3d 1300, 1308 (11th Cir. 2012) ("[G]eneral deterrence is an important factor in white-collar cases, where the motivation is greed."); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (Because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence" (internal quotations and citation omitted)).

D. Supervised Release

The Court must also determine the appropriate term of supervised release at sentencing. "Supervised release . . . is not a punishment in lieu of incarceration." *United States v. Granderson*, 511 U.S. 39, 50 (1994). Instead, it "fulfills rehabilitative ends, distinct from those served by incarceration." *United States v. Johnson*, 529 U.S. 53, 59 (2000). Under 18 U.S.C. § 3583(b)(2), the authorized term of supervised release for Counts 1 and 2 is not more than 3 years, and under Section 3583(k), the authorized term for Count 3 is at least five years and up to life. This five-year mandatory minimum term for Count 3 reflects a heightened concern for recidivism among sex offenders and the need for supervision over time. *See, e.g.*, H.R. Rep. No. 107-527, at 2 (2002) (explaining that "studies have shown that sex offenders are four times more likely than other violent criminals to recommit their crimes" and that "the recidivism rates do not appreciably decline as offenders age"). Notably, the Guidelines recommend a lifetime term of supervised release for sex offenders, USSG § 5D1.2(b) (Policy Statement), and the Fourth Circuit has observed that § 3583(k) and § 5D1.2(b) jointly "reflect[] the judgment of Congress and the Sentencing Commission that a lifetime term of supervised release is appropriate for sex offenders in order to protect the public." *Morace*, 594 F.3d at 351 (citations omitted).

The defendant's conduct—namely, his years-long use and subsequent administration of online cybercrime forums, his attempts to evade law enforcement detection, and his recent pretrial violation and associated failure to clearly demonstrate acceptance of responsibility for his crimes—underscores the need for a substantial term of supervised release to ensure the defendant is properly monitored and can access rehabilitation services. For these reasons, the United States respectfully recommends that the Court impose a substantial term of supervised release with the conditions of supervision contemplated under 18 U.S.C. § 3583(d) and USSG § 5D1.3(d)(7) for sex offenders required to register under the Sex Offender Registration and Notification Act.

E. Special Assessments Under the Justice for Victims of Trafficking Act (JVTA) & the Amy, Vicky, and Andy Child Pornography Victim Assistance Act (AVAA)

On December 7, 2018, Congress enacted the Amy, Vicky, and Andy Child Pornography Victim Assistance Act. The Act instructs that, in addition to any restitution or other special assessment, courts "shall assess . . . not more than $17,000 on any person convicted of an offense under section 2252(a)(4) . . . ." 18 U.S.C. §§ 2259A(a)(1). Assessments collected under this statute are deposited in the Child Pornography Victims Reserve, which provides monetary assistance to victims of trafficking in child pornography, *see* §§ 2259(d) & 2259B, and shall be paid in full after any special assessment under § 3013 and any restitution to victims of the defendant's offense, *see* § 2259A(d)(2). In determining the amount to be assessed under § 2259A, courts should consider the sentencing factors set forth in § 3553(a) and the guidance in § 3572 for the imposition of fines. § 2259A(c). The United States respectfully requests that the Court impose a reasonable special assessment under § 2259A, in addition to the $300 mandatory special assessment for the defendant's felony convictions pursuant to 18 U.S.C. § 3013.

Additionally, under the Justice for Victims of Trafficking Act, courts "shall assess an amount of $5,000 on any non-indigent person" convicted of certain enumerated offenses, including possession of child pornography. *See* 18 U.S.C. § 3014. The United States respectfully requests that the Court impose an assessment of $5,000 for the defendant's convictions pursuant to 18 U.S.C. § 3014.

F. Restitution

As part of the plea agreement entered into by the parties, and pursuant to 18 U.S.C. § 3663A(c)(1) and (c)(2), the defendant has agreed to entry of a Restitution Order for the full amount of the victims' losses as determined by the Court. The government has sought to obtain restitution amounts from the victims who submitted victim impact statements for inclusion in the PSR. At the time of this filing, the parties agree on the restitution amounts for Victim-1 and Victim-2. However, Victim-3 has indicated to the government that it needs more time to provide a restitution amount. Accordingly, with the consent of the defendant and in accordance with the terms of the Plea Agreement, the government asks that the Court defer imposition of restitution to a later date so as to allow Victim-3 to provide a restitution amount for their harm.

G. Forfeiture

The United States submitted a consent order for forfeiture, signed by the defendant and his counsel, during the plea agreement hearing. *See* Dkt. No. 42. The order was signed by the Court the same day.

CONCLUSION

For the reasons above, the United States respectfully requests that the Court impose a sentence at the low end of the Guidelines, a substantial term of supervised release, a $300 special assessment under § 3013, a $5,000 special assessment under § 3014, and a reasonable special assessment under § 2259A. The United States also requests that the Court schedule a future hearing to finalize restitution.

Respectfully submitted,

Jessica D. Aber
United States Attorney

Date: January 16, 2024

By: /s/

Lauren Halper
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: (703) 299-3700
Fax: (703) 299-3980
Email: Lauren.Halper@usdoj.gov

Aarash A. Haghighat
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division