IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
NEWNAN DIVISION

UNITED STATES OF AMERICA *v.* ROBERT PURBECK A.K.A. "LIFELOCK" A.K.A. "STUDMASTER" A.K.A. "STUDMASTER1"	Criminal Action No. 3:21-cr-0004-TCB-RGV

GOVERNMENT'S SENTENCING MEMORANDUM

Comes Now the United States of America, by and through counsel, Ryan K. Buchanan, United States Attorney for the Northern District of Georgia, and Michael Herskowitz, Nathan P. Kitchens, Alex R. Sistla, Assistant United States Attorneys, and Brian Z. Mund, Trial Attorney, Computer Crime and Intellectual Property Section, U.S. Department of Justice, and respectfully submits this Sentencing Memorandum in advance of the November 13, 2024, sentencing hearing for the defendant, Robert Purbeck ("Purbeck").

For the reasons discussed herein, the Government recommends that the Court sentence Purbeck to 70 months in the custody of the Bureau of Prisons, to be followed by three years of supervised release, and full restitution to the victims in the amount of $1,048,702.98.

Background and Pertinent Facts

Purbeck is a cybercriminal who hacked into computers of victims in our District and in other places across the country, threatened and attempted to extort victims, and possessed stolen personally identifiable information (PII) of over 132,000 people, including dates of birth and social security numbers. Purbeck's victims included a Florida orthodontist, a California dentist, the City of Newnan Police Department, a Griffin medical clinic, a Locust Grove medical clinic, a former mayor in Michigan, a medical billing service in Alaska, an optometry clinic, a safehouse for women and children who were victims of domestic violence, a dialysis clinic, a church in Stone Mountain, a correctional facility, an Idaho health department, and others. *See* Presentence Investigation Report (PSR) at ¶66.

In June 2017, Purbeck purchased access to the computer server of a Griffin medical clinic on a darknet marketplace. *Id.* at ¶18. He then used the stolen credentials to illegally access the computers of the medical clinic and removed records that contained sensitive personal information for over 43,000 individuals, including names, addresses, birth dates, and social security numbers. *Id.*

During the same month, Purbeck hacked and then attempted to extort a California dentist (identified in the PSR as "A.Y."), initially sending her an email demanding a payment of $10,000 in Bitcoin under threat to publicize her patients' PII on the dark web. *Id.* at ¶12. Purbeck, using the moniker "LifeLock," emailed A.Y.:

> If you do not pay me then I will be forced to cause you much consternation. I will be forced indeed to cause the closure practice. I will text each of your customers their SSN and DOB . . . You will be screwed in California. Further, I will sell the details I have obtained on your practice on my darkweb page devoted to identity theft.

Id.

In total, Purbeck sent approximately 27 extortion emails to A.Y., even threatening to issue warrants against her for sex crimes and place her family members on sex offender registries:

> Just so you know. I have access to several or more likely more than 100 police stations throughout the US. I can label your family members as sex offenders in any of those districts. You won't even know the districts where warrants have been issued in your name for crimes such as forcible rape and felony injury to a child among many other sadistic crimes I can pin on you and your family members. Even if you only get questioned at an airport it will be inconvenient. This is circle one of the hell I can put you in.

Id. at ¶13.

In furtherance of this threat, Purbeck purchased PII on A.Y.'s family members on the dark web that he used in at least one extortion email. *Id.* at ¶15. As a result of Purbeck's hacking and extortion against A.Y. and her patients, A.Y. suffered damages of $92,095.

About eight months later, in February 2018, Purbeck purchased access to a City of Newnan Police Department server on a darknet marketplace. *Id.* at ¶21. Purbeck used the stolen credentials to hack into the City of Newnan computer systems and stole police reports and other documents, including personal information for over

14,000 people. *Id.* The City of Newnan suffered losses of $113,935 associated with Purbeck's data breach. *Id.* at ¶23.

Purbeck's hacking and extortion campaign continued. In July 2018, Purbeck hacked and attempted to extort a Florida orthodontist (identified in the PSR as "D.S."), demanding payment in Bitcoin and threatening to sell patient and personal information unless D.S. paid the ransom. Purbeck harassed D.S. and his patients for 10 days with numerous threatening emails and text messages. Purbeck even threatened to sell the personal information of D.S.'s minor child.

Specifically, on July 3, 2018, Purbeck, after hacking D.S.'s practice, sent him an email that included one of his patient's name, date of birth, and social security number, and requested a payment of $15,000 in Bitcoin. *Id.* at ¶¶26-27. Purbeck then sent D.S. another email – this time identifying his minor daughter, her date of birth, social security number, and the school which she attended:

> and most importantly sweet [name of D.S.'s minor child], born the [date of birth] is [social security number]. She currently attends [name of school] and will hopefully continue to do so in a safe and secure way. Fear not my new friend, I do not mean threat or harm to your sweet child, I just needs you to be aware of what I know [*sic*] control. What I have.[1]

The following day, on July 4, Purbeck sent a text message to D.S.'s wife, demanding payment by midnight the following day or Purbeck would start contacting patients:

---

[1] This email is quoted in D.S.'s victim impact statement that has been separately provided to the Court and defense counsel.

> Hello... Enjoy America Birthday. Do not allow your husband to be a cheap jew. It is not good for your kid patients. Make sure he contact me on time. 5th July at midnight Florida time is as late as I go before I start contacting patients. Earlier is much better. You charge $5000 for peoples vanity. You can pay my fee.

Id. at ¶28.

When D.S. elected not to pay by the deadline, Purbeck made good on his threat and sent text messages to D.S.'s patients, sending one patient an x-ray of their teeth. *Id.* at ¶30. In another text message to a patient, Purbeck threatened:

> I'm not going to [expletive] with your families credit or bank accounts. However I do want you to make [D.S.] aware that there are consequences to not securing his network. I am extending you and your family a courtesy. If he does not reply to me tomorrow I will start draining his other clients bank accounts and his daughter [identifying daughter's name] accounts.

Id.

Purbeck's barrage of harassment of D.S., his family, and his patients continued for 10 days, even attacking D.S.'s religion:

> I know that you are of the Jewish faith and that family and community are of the most importance to you. Do not let them all down [D.S.]. That would end in much blood shed and tears. [2]

In one instance, Purbeck texted a teenage patient her social security number and bank account number as proof that her information had been stolen:

---

[2] This email is quoted in D.S.'s victim impact statement that has been separately provided to the Court and defense counsel.

> With child SSN I can do a number of things, from staring [*sic*] new lives for dangerous individuals that are looking for a fresh start, to buying homes, opening credit, staring banks accounts, staring businesses.[3]

As a result of Purbeck's extortion campaign, D.S. incurred expenses for forensic audits, notifications, remediation, and legal fees, which ultimately forced him to sell his orthodontic practice. In total, D.S. suffered losses of $285,980.13, which Purbeck has agreed to pay as restitution. *Id.* at ¶32. D.S. is expected to attend Purbeck's sentencing to read a victim impact statement and share with the Court the profound impact that this incident had on him and his family.

On August 21, 2019, the FBI executed a federal search warrant at Purbeck's home in Meridian, Idaho. *Id.* at ¶34. During the search, the FBI seized multiple computers and electronic devices, which contained personal information of over 132,000 individuals, obtained through Purbeck's numerous data breaches, including the City of Newnan, the Griffin medical clinic, and at least 17 other victims throughout the United States. *Id.* at ¶66. Many of these victims incurred substantial expenses, including remediation costs and disruption to business operations because of Purbeck's conduct.

On the date of the search warrant, the FBI interviewed Purbeck in his backyard, where he admitted that he was the hacker "Lifelock" and was responsible for various hacks and extortions, including of A.Y. *Id.* at ¶¶48-52. He acknowledged that he made approximately $48,000 from the extortions. *Id.* at ¶50. Purbeck also

[3] This email is quoted in D.S.'s victim impact statement that has been separately provided to the Court and defense counsel.

admitted that he committed "some minor identity theft" with stolen PII, including setting up "a few fake bank accounts" in the victims' names. *Id.* at ¶54. Purbeck added that he "searched for his former supervisor's personal data and used it to taunt him." *Id.* at ¶56.

On March 2, 2021, a Grand Jury sitting in this District returned an 11-count indictment against Purbeck, which charged him with violations of computer fraud and abuse, wire fraud, and access device fraud. (Doc. 1). On September 1 and 2, 2022, U.S. Magistrate Judge Russell G. Vineyard held an evidentiary hearing on Purbeck's motion to suppress statements where Purbeck and the FBI agents testified. (Docs. 64, 76-77). In recommending denial of the motion, Judge Vineyard found that "Purbeck's testimony at the hearing was illogical and even fanciful at times as he seemed to embellish and speculate about circumstances that he stated as fact." (Doc. 87 at 39). Judge Vineyard observed and found: "[i]n general, [Purbeck's] testimony was incredible" in that he "contradicted himself . . . and told an untenable story," and "[h]is testimony was not plausible." *Id.* at 61.

Following further pretrial litigation, Purbeck pleaded guilty on March 19, 2024, pursuant to a negotiated plea agreement to counts one and two of the indictment, which charged him with two counts of computer fraud and abuse, in violation of Title 18, United States Code, Sections 1030(a)(7)(B), 1030(c)(3)(A), and 2. (Doc. 116-1). Each count carries a 5-year maximum term of imprisonment. *See* PSR, Part D, Sentencing Options.

Pending Objections to the PSR and Guideline Applications

According to the PSR, Purbeck's total offense level is 27, criminal history category I, with a custodial Guideline range of 70 to 87 months. (PSR, Part D, Sentencing Options). Purbeck's pending objections to the PSR for consideration at sentencing are as follows:

- The PSR's assessment of a two-level increase to Purbeck's base offense level as the offense involved the production or trafficking of an unauthorized access device or counterfeit access device, pursuant to USSG § 2B1.1(b)(11)(B)(i), or involved the unauthorized transfer and unlawful use of means of identification to produce and obtain another means of identification, pursuant to USSG § 2B1.1(b)(11)(C)(i);
- The PSR's assessment of a two-level increase to Purbeck's base offense level for obstruction of justice pursuant to USSG § 3C1.1, as Purbeck provided untruthful testimony and materially false information to Judge Vineyard during the suppression hearing in this case; and
- The PSR's absence of a two-level reduction to Purbeck's base offense level for zero-point offender pursuant to USSG § 4C1.1, due to the financial harm that Purbeck caused D.S.

For the reasons detailed below, the Government submits that Purbeck's objections are without merit and should be overruled.

A. Purbeck Should Receive the Two-Level Unauthorized Access Device Enhancement.

Purbeck should receive a two-level enhancement to his base offense level pursuant to USSG § 2B.1(b)(11)(B)(i) & (C)(i).[4] Subsection (b)(11) provides, in relevant part, "[i]f the offense involved . . . (B) the production or trafficking of any (i) unauthorized access device or counterfeit access device . . . or (C)(i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification . . . increase by 2 levels."

Here, Purbeck's offense conduct involved the use of stolen victim data to open bank accounts in the names of those victims and the sale of some of those fraudulent bank accounts to other individuals. *See* PSR at ¶54. That offense conduct constitutes both production and trafficking of unauthorized access devices, as well as the unlawful use of a means of identification to produce another means of identification.

Purbeck's creation and sale of fraudulent bank accounts constitutes the production and trafficking of unauthorized access devices. The term "unauthorized access device" means "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." USSG § 2B1.1(b)(11) cmt. n.10(a). "Access device" is broadly defined and includes, as relevant here, routing and bank account numbers. *See United States v. Wright*, 862 F.3d 1265, 1275 (11th Cir. 2017) (citing *United States v. Williams*, 790 F.3d 1240, 1250 (11th Cir. 2015) (routing and banking numbers constitute access devices, when not

[4] Purbeck styles his objection to the application of this enhancement as a "conditional objection that is being raised pursuant to the plea agreement."

used on a paper check); 18 U.S.C. § 1029(e)(1). Accordingly, fraudulent bank accounts opened in the names of identity theft victims may constitute unauthorized access devices. *See United States v. Blain*, 711 F. App'x 589, 590 (11th Cir. 2018) (applying enhancement for fraudulent bank accounts opened and debit cards issued in names of identity theft victims).

Under Eleventh Circuit law, Purbeck "produced" the bank accounts within the meaning of the Guidelines. *See United States v. Taylor*, 818 F.3d 671, 678 (11th Cir. 2016) (concluding that a defendant "produces" unauthorized access device when causing bank to produce the device); *see also* USSG § 2B1.1(b)(11) cmt. n.10(a) (defining "production" as "manufacture, design, alteration, authentication, duplication, or assembly"). Thus, Purbeck's opening of bank accounts in the names of his identity theft victims qualify as producing an unauthorized access device for purposes this enhancement.

Moreover, Purbeck not only produced the unauthorized access devices, but also trafficked in those access devices for profit. While "trafficking" is not defined in the Guidelines commentary, accepted definitions of that term are generally consistent with the definition of "traffic" in 18 U.S.C. § 1029(e)(5), which means to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." *See United States v. Michell*, 728 F. App'x 953, 958 (11th Cir. 2018). Therefore, Purbeck's sale of fraudulently opened bank accounts to other individuals constituted trafficking of unauthorized access devices under the Guidelines—establishing an independent basis for the two-level enhancement.

Purbeck's use of stolen victim data to open unauthorized bank accounts also warrants imposition of the two-level enhancement pursuant to USSG § 2B1.1(b)(11)(C)(i), because it involved the unauthorized transfer and unlawful use of means of identification to produce and obtain another means of identification. Specifically, as set forth in the PSR, Purbeck obtained victim data without authorization and used that PII unlawfully to open bank accounts in the names of victims, thereby producing and obtaining bank account information. *See* PSR at ¶54. Both the victim data and bank account information qualify as "means of identification."[5] Indeed, the Guidelines commentary for this sub-provision specifically envisages the example of a defendant unlawfully obtaining an individual's name and address from a source and using that information to open a credit card in that individual's name. USSG § 2B1.1(b)(11) cmt. n.10(C)(ii)(II). Accordingly, the two-level enhancement in Section 2B1.1(b)(11) is also appropriate pursuant to subsection (C)(i).

[5] "Means of identification" is defined in relevant part as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," except that "such means of identification shall be of an actual (i.e., not fictitious) individual, other than the defendant or a person for whose conduct the defendant is accountable." U.S.S.G. § 2B1.1(b)(11) cmt. n.10(C)(ii)(II).

B. Purbeck Should Receive the Two-Level Obstruction Enhancement Under USSG § 3C1.1 Because He Testified Falsely During the Suppression Hearing.

The initial PSR recommended that Purbeck should receive the two-level obstruction enhancement under § 3C1.1 because he provided "untruthful testimony" or "materially false information to a judge" during the suppression hearing. Purbeck objects to the obstruction enhancement. *See* Purbeck Obj. at 4-5. The Court should overrule Purbeck's objection because he offered materially false testimony under oath at the suppression hearing about the circumstances of his non-custodial interview.[6]

The obstruction guideline provides that a defendant's offense level may be increased by two levels if: (1) he "willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to an investigation, prosecution, or sentencing" of his instant offense; and (2) his obstructive conduct

[6] In the final PSR, the probation officer recommended that Purbeck receive the obstruction enhancement based on a *pro se* civil filing he made in the United States District Court for the District of Idaho. (Final PSR ¶86). The Government disagrees with the probation officer that Purbeck's civil filing—even though it contains false information and untruthful allegations—provides the necessary factual predicate for imposing an obstruction enhancement. *See, e.g.*, *United States v. Campa*, 529 F.3d 980, 1016 (11th Cir. 2008) (explaining the relevant question in applying the obstruction enhancement is "whether the obstructive conduct occurred during the course of the investigation, prosecution, or sentencing" of the offense of conviction or a closely related offense). Accordingly, the Government does not rely on this civil filing (or the reasoning in the final PSR) as a basis for the Court to impose the obstruction enhancement under § 3C1.1. The Court may nevertheless consider Purbeck's various filings, including this most recent one in which he lodges numerous unfounded allegations against one of the government's attorneys, as part of its § 3553(a) analysis.

related to his "offense of conviction and any relevant conduct or . . . a closely related offense." USSG § 3C1.1. Example of conduct covered by this Guideline include "committing . . . perjury" or "providing materially false information to a judge or magistrate judge." *Id.*, cmt. n.4(B), (F). Perjury is "false testimony concerning a material matter with the willful intent to provide false testimony, rather than as a result of confusion, mistake, or faulty memory." *United States v. Duperval*, 777 F.3d 1324, 1337 (11th Cir. 2015) (quotation marks omitted). The application note defines materially false information as "information that, if believed, would tend to influence or affect the issue under determination." USSG § 3C1.1, cmt. n.6. "The [Eleventh Circuit] has noted that [the] threshold for materiality is 'conspicuously low.'" *United States v. Doe*, 661 F.3d 550, 566 (11th Cir. 2011) (quoting *United States v. Odedina*, 980 F.2d 705, 707 (11th Cir. 1993)) (additional citations omitted).

In determining whether to impose the enhancement obstruction because of false or perjured testimony, the preferable course is for the Court to "make specific findings by identifying the materially false statements individually, [but] it is sufficient if the [district] court makes a general finding of obstruction encompassing all the factual predicates of perjury." *Duperval*, 777 F.3d at 1337 (quotation marks omitted). Those factual predicates are finding that the testimony was: (1) under oath; (2) false; (3) material; and (4) given with the willful intent to provide false testimony. *United States v. Singh*, 291 F.3d 756, 763 & n.4 (11th Cir. 2002).

In the report and recommendation denying Purbeck's motion to suppress his statements, Judge Vineyard found his "testimony regarding all of the circumstances surrounding the interview was not fully credible as it was contradicted by the more credible and consistent of the testimony of the Agents[.]" (Doc. 87 at 38).[7] As noted above, the magistrate judge further observed that "Purbeck's testimony at the hearing was illogical and even fanciful at times as he seemed to embellish and speculate about the circumstances that he stated as fact." (*Id.* at 39). In particular, Purbeck falsely testified about the agents subjecting him "to inhumane physical conditions by being forced to sit for hours in direct sunlight in [] August heat without water or food." (*Id.* at 47-48). As a result, Purbeck testified that he was suffering from the symptoms of heat exhaustion, even believing that he was on the verge of organ failure. (*Id.* at 50, 54) (citations omitted). Purbeck's false testimony in this respect included claims that:

- The agents repeatedly ensured that Purbeck be interviewed in the direct sunlight, and in fact purposefully placed Purbeck in the direct sunlight. (*Id.* at 21 n.17, 37 n. 26 (transcript citations omitted)).
- He was suffering from heat cramps, had trouble walking to the bathroom, and had to be assisted by one of the agents. (*Id.* at 22 n. 18 (transcript citations omitted)).
- It was very painful for him to urinate, and his urine was "dark brown, like the color of cola." (Doc. 77, Sept. 2 Tr. at 95).

[7] There is no dispute that Purbeck was under oath when he testified at the suppression hearing.

- He was sweating heavily from sitting outside and being in the heat for a "prolonged period[] of time," which caused Purbeck to "get[] a little bit out of it." (Doc. 77, Sept. 2 Tr. at 100-01).
- He was in "bad condition" at the conclusion of the interview "due to the prolonged sun exposure, which was exacerbated by his blood pressure and psychiatric medications," and that he was even on the verge of organ failure. (*Id.* at 24 n. 21 (transcript citations omitted)).
- He had developed heat cramps, and the agents denied him water. The agents also failed to offer Purbeck any water despite drinking water in front of him, in fact taunting him about not having water. (Doc. 77, Sept. 2 Tr. at 78-80, 156, 158-59).
- He suffered from such severe sunburn that he had trouble sleeping in the days following the interview, developed a fever, and "wasn't fully functional for at least a couple of days." (Doc. 77, Sept. 2 Tr. at 114).

The magistrate judge concluded that "Purbeck's assertion that he was subjected to inhumane physical conditions was not supported by the credible evidence in the record." (Doc. 87 at 55) (citation, quotation marks omitted). In doing so, the magistrate judge did not simply rely on the agents' testimony, but evidence about the moderate weather on the day Purbeck was interviewed, as well as the fact that Purbeck "never sought any medical attention" for his alleged heat-related ailments "and even . . . flew to Atlanta for a proffer session with the [same interviewing] agents just weeks later." (*Id.* at 54).

Purbeck's false testimony about the agents' supposed actions and his alleged medical condition was material because he argued that this rendered his statements to the agents involuntary. (*Id.* at 50, 53, 55). In other words, if Purbeck's false testimony about being subjected to inhumane physical conditions had been believed, "it would [have] tend[ed] to influence or affect the issue under determination;" namely, the admissibility of his statements at trial. USSG § 3C1.1 cmt. n.6; (Doc. 87 at 47-54) (analyzing the voluntariness of Purbeck's statement in light of his allegations of being subjected to allegedly inhuman physical conditions) (citing, among other authority, *United States v. Lazarus*, 552 F. App'x 892, 895 (11th Cir. 2014)); *see also United States v. Bedolla-Zavala*, 611 F.3d 392, 396 (7th Cir. 2011) ("The relevant considerations are the kind of information provided and its tendency to influence the court, not the actual effect of a particular misstatement.") (cited approvingly by *United States v. Doe*, 661 F.3d 550, 567 (11th Cir. 2011)). Moreover, as reflected by his lengthy testimony at the suppression hearing, Purbeck willfully made these false statements about his health and being subject to inhumane conditions. He did not make them "as a result of a mistake, confusion, or faulty memory." *Singh*, 291 F.3d at 763 n.4.

The Court should therefore overrule Purbeck's objection and impose the two-level obstruction enhancement. Indeed, the Eleventh Circuit has routinely upheld the imposition of the obstruction enhancement based on a defendant providing false testimony and information in pretrial hearings. *See, e.g.*, *Doe*, 661 F.3d at 566-67 (affirming obstruction enhancement where defendant provided false information to the probation officer in advance of the magistrate judge's bond

determination); *United States v. Hubert*, 138 F.3d 912, 915 (11th Cir. 1998) (holding that district court did not err in imposing obstruction enhancement based on defendant's false testimony at "trial and two prior bond revocation hearings"); *United States v. Tran*, 171 F. App'x 758, 761-72 (11th Cir. 2006) (affirming obstruction enhancement where defendant falsely testified at suppression hearing that he had requested his bankruptcy lawyer's business card in an effort to demonstrate he had invoked his right to counsel); *see also, e.g.*, *United States v. Guevara*, No. 14-cr-20792, 2019 U.S. Dist. LEXIS 6710, at *7 (S.D. Fla. Jan. 15, 2019) (imposing obstruction enhancement based on defendant's false testimony at suppression hearing because this "testimony at the motion to suppress could have been case-dispositive . . . and the Government's case would have been significantly impacted") (citing *United States v. Lincecum*, 220 F.3d 77, 80-81 (2d Cir. 2000) (affirming obstruction of justice enhancement based on defendant making false statements in his affidavit in support of a motion to suppress); *United States v. Matos*, 907 F.2d 274, 275 (2d Cir. 1990) (affirming obstruction of justice enhancement based on defendant's false testimony at a suppression hearing)).

C. Purbeck Has Not Met His Burden to Show that He is Entitled to the Two-Level Zero-Point Offender Reduction.

Purbeck will not be able to meet his burden of showing that he "did not personally cause substantial financial hardship" to qualify for the two-level zero-point offender reduction under the Guidelines. *See* USSG § 4C1.l(a) (limiting reduction to circumstances where "the defendant meets all of the following criteria"); *Id.* § 4C1.l(a)(6) ("[T]he defendant did not personally cause substantial

financial hardship"); *United States v. Cubero*, 754 F.3d 888, 892 (11th Cir. 2014) ("The government bears the burden of proving the applicability of a sentencing guidelines increase, while the defendant bears the burden of proving the applicability of a sentencing guidelines reduction.")

"In determining whether the defendant's acts or omissions resulted in 'substantial financial hardship' to a victim, the court shall consider, among other things, the non-exhaustive list of factors provided in Application Note 4(F) of the Commentary to § 2B1.1 (Theft, Property Destruction, and Fraud)." *See* USSG §4C1.1(b)(3). Application Note 4(F) of the Commentary to § 2B1.1 provides, in pertinent part:

> In determining whether the offense resulted in substantial financial hardship to a victim, the court shall consider, among other factors, whether the offense resulted in the victim—
> (i) becoming insolvent;
> (ii) filing for bankruptcy under the Bankruptcy Code (title 11, United States Code);
> (iii) suffering substantial loss of a retirement, education, or other savings or investment fund;
> (iv) making substantial changes to his or her employment, such as postponing his or her retirement plans;
> (v) making substantial changes to his or her living arrangements, such as relocating to a less expensive home; and
> (vi) suffering substantial harm to his or her ability to obtain credit.

See USSG § 2B1.1, Application Note 4(F).

Here, Purbeck cannot demonstrate that he did not "personally cause substantial financial hardship" to D.S, who is expected to testify at sentencing that

Purbeck's hacking and extortion resulted in D.S. "making substantial changes to his employment" by selling his orthodontic practice to alleviate nearly $300,000 in losses personally caused by Purbeck. D.S. may also testify that for two years he and his family were teetering on the edge of bankruptcy, both personal and professional, due to the damage caused by Purbeck.[8]

Even though Purbeck's intent to cause financial harm is not required, it is telling that Purbeck hoped that D.S. would in fact suffer significant financial hardship, as one of his emails stated:

> You deserve to have your entire malpractice and umbrella policies drained your house sold at auction and your family to be made homeless by the bankruptcy court. You will lose your wife and daughter because they are greedy twats just like you.[9]

For these reasons, the Government respectfully submits that Purbeck does not qualify for the zero-point offender reduction - as the PSR recommends.

Argument Under Section 3553(a) Factors

A thorough consideration of all the sentencing factors set forth in 18 U.S.C. 3553(a) suggests that the most appropriate sentence for Purbeck is the Government's recommended sentence of 70 months in custody, to be followed by three years of supervised release, and full restitution to the victims in the amount

[8] D.S. will also read his victim impact statement to the Court as part of the Government's § 3553(a) presentation.

[9] This email is quoted in D.S.'s victim impact statement that has been separately provided to the Court and defense counsel.

of $1,048,702.98. The Government submits that the Section 3553(a) factors should be applied to Purbeck as follows:

1. Nature and Circumstances of the Offense and the History and Characteristics of the Defendant.

The nature and circumstances of Purbeck's offense were simply egregious. Purbeck hacked numerous victims throughout the country and stole PII, such as social security numbers and dates of birth, including those of minors. If that were not enough, Purbeck used the stolen data and information as a weapon. He sent threatening and harassing text messages and emails to victims, their family members, and at times their patients, demanding money to make it stop. These hacks and threatening messages caused disruption, anxiety, and stress to victims, patients, and companies, and resulted in over a million dollars in collective losses.

In fairness to Purbeck, the serious nature and circumstances of the offense need to be balanced by mitigating factors. Purbeck is 45 years old with no prior criminal history. Aside from his recent despicable antisemitic civil filing, which is further discussed below, where he researched and doxed one of the Assistant U.S. Attorneys prosecuting this case, it appears that Purbeck has otherwise done well on pretrial release for nearly four years. He agreed to resolve the case without the necessity of a multi-week trial with victims needing to travel from all over the country to relive these difficult events. Purbeck also agreed to pay full restitution of over one million dollars to the victims.

In agreeing to recommend a custodial sentence of 70 months (and nothing higher), the Government considered both aggravating and mitigating factors and asks the Court to take account of both factors as well.

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

For the reasons mentioned, this is an incredibly serious case, and Purbeck is deserving of a significant punishment. A 70-month sentence will reflect the seriousness of the offense, promote respect for the law, and provide just punishment to Purbeck for his crimes. The Government submits that a sentence of 70 months is sufficient, but not greater than necessary, to comply with the purposes of this subsection and the overall factors in 3553(a).

3. The Need to Afford Adequate Deterrence to Criminal Conduct and to Protect the Public from Further Crimes of the Defendant.

The Court should fashion a sentence for Purbeck that will deter him from future criminal conduct, as well as send a strong message to others who are involved in cybercrimes, that they will be punished with a significant term in federal prison. The Government submits that 70 months in prison, together with a judgment of over a million dollars in restitution, should hopefully deter Purbeck (who will be in his early 50s upon release) from future crimes, as well as send an appropriate message to other cybercriminals. While Purbeck is in federal prison, the public will also be protected from any future crimes.

A meaningful prison sentence of 70 months is also necessary to provide adequate deterrence—both specific and general—against further criminal conduct. *See* 18 U.S.C. § 3553(a)(2)(B). The prolonged nature of Purbeck's threatening communications heightens the importance of deterrence, and the public's interest in deterrence is particularly acute in cases like this given the ever-increasing costs of cyber extortion.

Purbeck's conduct in this case, both before and after facing charges, reflects the need for specific deterrence. For more than a year from mid-2017 through October 2018, Purbeck conducted sinister cyber extortion attacks against seven victims by threatening to disclose sensitive data for his own personal gain. PSR ¶¶12–33. This cyber extortion scheme "required 'careful calculation and deliberation,'" which is an "aggravating factor" supporting a substantial sentence. *United States v. Matthews*, 477 F. App'x 585, 588 (11th Cir. 2012) (affirming consideration of "repeated" deposits of stolen checks worth more than $400,000 over "prolonged period" of several months as "aggravating factor"). This conduct was not a mistake, a poor decision in the heat of the moment, or an aberration—his conduct over a lengthy period calls for a sentence to deter him from future criminal activity.

Purbeck's conduct since his guilty plea underscores the need for specific deterrence. Specifically, Purbeck filed a *pro se* civil pleading in the U.S. District Court for the District of Idaho in August 2024 containing harassing language consistent with his prior extortionate activity. *See Robert Purbeck v. United States, et al.*, No. 1:24-CV-00356-DCN (D. Idaho) (Aug. 12, 2024) (Doc. 1) (Attached as Exhibit 1). For example, Purbeck victimized D.S., in part, by (1) publicizing

personal information about the victim, PSR ¶¶26, 30; (2) disclosing personal information about the victim's patients, *id.* ¶30; and (3) harassing his family with antisemitic rhetoric, including warning the victim's wife not to allow her husband "to be a cheap jew," *id.* ¶28. Similarly, in his civil filing, Purbeck targeted a prosecutor in this matter by (1) publicizing personal information about the prosecutor, including identifying his place of worship and discussing his family members, (2) disclosing personal information about two of his victims in this matter, including discussing their religious beliefs and charitable donations, and (3) littering his filing with antisemitic conspiracy theories targeting the prosecutor, including calling him an "apostate Jew" who attends a "wicked church" and "is no different than a Jihadist." *See* Exhibit 1 at 22–24. Purbeck's continued efforts to weaponize personal information, including discussing minor children of his targets, even months after his guilty plea highlight the necessity of a prison sentence of 70 months to deter him from further threatening communications.

The devastating scale of Purbeck's cyber extortion supports a sentence that recognizes an "important goal of sentencing in a white-collar crime prosecution: the need for general deterrence." *United States v. Kuhlman*, 711 F.3d 1321, 1328 (11th Cir. 2013). The Eleventh Circuit has recognized that "[b]ecause 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 marks and alteration omitted); *see also United States v. Howard*, 28 F.4th 180, 209

(11th Cir. 2022) ("General deterrence is more apt, not less apt, in white collar crime cases.").

The public's interest in deterring cybercrime cannot be overstated. The Internet Crime Complaint Center ("IC3"), the FBI unit that receives and tracks cybercrime complaints from victims, received a total of 48,223 complaints of cyber extortion in 2023, with reported losses of nearly $75 million.[10] These figures highlight that cyber extortion schemes impose a tremendous cost beyond the cost of any ransom paid because the victim must expend considerable resources to identify the full scope of the breach and fix any vulnerabilities, ensure the protection of sensitive data, notify clients, and, in certain cases, report and respond to federal and state regulatory agencies in the aftermath of a breach.

Moreover, the need for general deterrence is greatest in cases involving particularly lucrative and difficult-to-detect cyber schemes, such as the sophisticated scheme in which Purbeck participated, that "may easily go undetected and unpunished." *United States v. McQueen*, 727 F.3d 1144, 1158–59 (11th Cir. 2013) (reversing lenient sentence because it "sap[ped] the goal of general deterrence," which is one of the "'key purposes of sentencing'"); *see also United States v. Engle*, 592 F.3d 495, 502 (4th Cir. 2010) (explaining that because tax evasion offenses are infrequently prosecuted, "[w]ithout a real possibility of imprisonment, there would be little incentive for a wavering would-be evader to choose the straight-and-narrow over the wayward path); *United States v. Heffernan*,

[10] *See* Federal Bureau of Investigation, 2023 Internet Crime Report, at 20–21, *available at* https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.

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.").

Investigations of cyber extortion cases are challenging, as law enforcement must work quickly to collect and preserve data before it is destroyed or encrypted, analyze that data to attribute the work to the perpetrator, and then successfully apprehend that individual. Criminals like Purbeck use increasingly sophisticated tools and techniques to obfuscate their true identities, and their infrastructure is frequently scattered across multiple jurisdictions. Consequently, the importance of affording general deterrence through meaningful sentences is particularly acute in cyber cases: where the incidence of prosecution is lower, the level of punishment must be higher to obtain the same level of deterrence.

A substantial sentence sends a message that even if the likelihood of being apprehended is not substantial, the consequences of such conduct will be. By contrast, a lenient sentence would do little to dissuade Purbeck or others from committing a similar crime in the future. For all these reasons, sentences for sophisticated cyber extortion schemes should be substantial to afford adequate deterrence consistent with Section 3553(a).

Although Purbeck is free to argue for a lower sentence, the Government respectfully submits that any sentence below 70 months in custody will not offer adequate deterrence, address the seriousness of the offenses, or promote just respect for the law given the breadth and impact of Purbeck's conduct.

Conclusion

Based upon the foregoing, the Government respectfully requests that the Court impose upon defendant Robert Purbeck a 70-month prison sentence, to be followed by three years of supervised release, and full restitution to the victims in the amount of $1,048,702.98. The Government will also ask that Purbeck be taken into custody following the sentencing hearing.

This 8th day of November 2024.

Respectfully submitted,

RYAN K. BUCHANAN
United States Attorney

Michael Herskowitz
/s/MICHAEL HERSKOWITZ
Assistant United States Attorney
Georgia Bar No. 349515
Michael.Herskowitz@usdoj.gov

/s/NATHAN P. KITCHENS
Assistant United States Attorney
Georgia Bar No. 263930
Nathan.Kitchens@usdoj.gov

/s/ALEX SISTLA
Assistant United States Attorney
Georgia Bar No. 845602
Alex.Sistla@usdoj.gov

/s/ BRIAN Z. MUND
Trial Attorney, Computer Crime and Intellectual Property Section
U.S. Department of Justice
California Bar No. 334699
Brian.Mund@usdoj.gov

600 U.S. Courthouse
75 Ted Turner Drive S.W.
Atlanta, GA 30303
404-581-6000