IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

United States of America, Plaintiff, vs. Nathan Wyatt Defendant.	4:17CR522 RLW **GOVERNMENT'S SENTENCING POSITION** Hon. Ronnie L. White Sentencing: September 21, 2020

POSITION OF THE UNITED STATES ON SENTENCING

The defendant aligned himself with sophisticated computer hackers and used his technical skill to assist his co-conspirators in concealing the source of their attacks on victims in the Eastern District of Missouri. He created, validated, and maintained phone accounts, a PayPal account, virtual private networks, and a Twitter account that were used to maliciously hack and extort multiple U.S. companies. These attacks unscrupulously preyed on the sensitivity of personal medical and financial records to stoke fear and seek ransom payments. The defendant acted from overseas, where he believed he was beyond the reach of U.S. law enforcement. As a consequence of the defendant's deliberate actions, victims in the Eastern District of Missouri suffered significant financial loss and experienced lasting human trauma. PSR 11 ¶ 40. The defendant is expected to plead guilty to conspiring to commit computer fraud and aggravated identify theft, in violation of 18 U.S.C. § 371, and be sentenced at the same hearing. *See* Administrative Order regarding Court Operations Restrictions Due to COVID-19 Response (Apr. 29, 2020) (Sippel, C.J.).

The probation officer calculated the defendant's guidelines range at 70–87 months in prison. In the Plea Agreement, the parties agreed to a guideline calculation of 51–63 months. The statutory maximum for the crime of conviction is 60 months. The government respectfully submits that a sentence within the agreed guideline range is

necessary to reflect the harm caused by this conspiracy, to protect the public from the defendant's repeated criminal activity, and to send a message of deterrence: the United States will not stand idly by where conspirators hide behind foreign borders and attack the privacy and livelihoods of our citizens.

I. Offense of Conviction

The defendant is expected to plead guilty to conspiring to commit computer fraud and aggravated identify theft, in violation of 18 U.S.C. § 371. Since at least April 2016, a hacker group known as "The Dark Overlord" (TDO) remotely accessed the computer networks of multiple U.S. companies without authorization, obtained sensitive records from those companies, and then threatened to release the stolen data unless the companies paid ransoms in bitcoin. Plea Agreement at 3; PSR ¶¶ 13, 15. The defendant played a key role in TDO by facilitating the availability of anonymous communication accounts and virtual private networks. Plea Agreement at 3–4.

In the Eastern District of Missouri, TDO targeted healthcare companies and an accounting firm. After hacking and exfiltrating data from each victim's computer network, TDO sent detailed ransom demands to the company owners. PSR ¶¶ 17, 21, 23, 30. The ransom demands provided proof of the network intrusions; each demand included private and sensitive personal identifying information about patients and clients and threats to release the data unless the ransom was paid.

These ransom demands sometimes included disturbing and thoroughly researched details about the victims' families. For example, one ransom demand, which is redacted here, threatened, "[w]e imagine that the same, careful, delicate care you give your patients, you also give your beautiful wife. What was her name? S******? S.M.V. (***-**-****)? Let's hope that she stays beautiful and that nothing unfortunate happens to her. Who knows? It's bound to happen with you leaving her alone all the time over there on [address] (Parcel ID **-**-**-**-***-****.**). We heard that it is for sale and maybe we will check it out sometime." Gov't Sealed Exhibit A. The letter went on to list details about the owner's children, and even included threats to the owner's parents: "[y]our elderly parents

do not need this sort of stress in their golden years. What were their names again?," and then listed the full names and social security numbers of the victim's parents. PSR ¶ 23; Gov't Sealed Exhibit A.

Another ransom demand stated, "While we wait for your initial shock to pass, we'll sit here and look at all these neat pictures you took of your patients. We found them in Medflex. It would be embarrassing if these were public, don't you think? Here are some of your internal pictures blasted onto a semi-public photo viewer (but dont worry only you have the link.)". Gov't Sealed Exhibit B.

Perhaps most disturbingly, members of the conspiracy sent ominous text messages to the daughter of one of the victims. Using a telephone account registered by the defendant, TDO sent the following message:

> *hi [K] you look peaceful….by the way did your daddy tell you he refused to pay us when we stole his company files..in 4 days we will be releasing for sale thousands of patient info. including yours… 19 in febuary?...weve all had a look and we all think your hot. soon some really evil men will be looking at you..possibly thru your window. your father is also looking at multiple felonies..so say good bye to the house.. all bcs daddy wouldnt pay a much smaller sum to make all this go away. Daddys fucked you [K]….And incest is a crime… sweetdreams*

Gov't Sealed Exhibit C**.**

There is no question that TDO understood how distressing the ominous text messages were, and there is no question that TDO understood the criminal nature of their acts. In a subsequent email to the victim's office, TDO threatened violence and taunted the victim for contacting law enforcement, writing: "Hey [P]. We are going to come for your family next. Ask [victim] what is going on with his beautiful daughter, [K]. Tell [victim] we will get physical and we will get violent. We have acquired assets in your area and we are not afraid to use them. We will hear a response or things will get nasty. We are not fucking around. Tell the FBI we say hello. Thank you." Gov't Sealed Exhibit D.

Each victim was ordered to pay between $75,000 and $300,000 in bitcoins. Although the victims in the Eastern District of Missouri ultimately did not pay the ransoms,

they nonetheless suffered significant losses from the criminal scheme; together, they reported nearly $1,500,000 in losses directly attributable to responding to and mitigating the network intrusions conducted by the members of the conspiracy. Moreover, TDO offered the private data stolen from the victims' networks for sale on online criminal forums. The extent of the losses suffered by this second wave of victims – those patients and clients whose identifying information was subsequently purchased by criminal actors – is unknown.

The defendant actively participated in the computer fraud and identity theft scheme by enabling members of the conspiracy to act with anonymity. He created, validated, and maintained phone accounts, a PayPal account, a Twitter account, and virtual private network accounts that were used in the course of the scheme to access victim computer networks, threaten and extort victims, and attempt to steal funds. Plea Agreement at 3–4; PSR ¶¶ 18, 19, 20. The defendant knew these accounts would be used by members of the conspiracy in the course of the scheme, he understood the extent of the scheme, and he expected to benefit financially from his efforts to assist other conspirators in avoiding detection.

II. Government's Position on Sentencing

The United States respectfully requests that the court impose a sentence within the guideline range. In particular, the nature and circumstances of the offense and the need for the sentence to reflect its seriousness, the history and characteristics of the defendant and the need to protect the public from him, and the need for deterrence all compel the government to request a guidelines sentence. *See* 18 U.S.C. § 3553(a).

1. **The Sentence Should Reflect the Serious Nature and Circumstances of the Offense.**

The nature and circumstances of this offense merit a guidelines sentence. The Dark Overlord hacking group is sophisticated and notorious; they have targeted dozens of U.S. victims, including healthcare providers, educational institutions, entertainment companies,

and others. TDO targeted victims in this district opportunistically, preying upon victims' databases of highly sensitive medical and financial records. They purposefully exploited private information to make money. When victims declined to meet TDO's demands, the conspirators sold the stolen personal identifying information on online criminal forums, creating a second wave of victims whose identifying information was subsequently purchased and exploited by other bad actors. In communications with the victims, TDO relished the mayhem they caused. One ransom note read, "[i]t has been a great time, you guys. We have really enjoyed all of the fun. We will continue to leak and begin our mass retail of your records and other retrieved information. You may not be contacted again, but rest assured we will be actively aiding your opposition in this fight." Gov't Sealed Exhibit E.

The defendant's involvement in TDO was important to the group's tradecraft. By using accounts that were validated or maintained by diffuse and obscured actors, TDO was able to harness a measure of anonymity in their attacks on U.S. victims. The defendant's conduct obscured the identities of other members of the group, allowing them to act with impunity; other TDO actors have not yet been apprehended. To the defendant, preying on U.S. citizens was a victimless sport. He encouraged the criminal activity with levity, even creating a rap song for TDO to use to mockingly induce the victims to pay, which he posted on YouTube. As the defendant's own words make clear, he was well aware of the goals of the conspiracy:

> *Yo Jim I've got a message you can suck my dick*
> *Didn't I tell you that I've got all of your fucking shit?*
> *I've got your medflex and your email, I've got everything*
> *You want them back man you've got to give me some fucking g's*
>
> *Get on your email mate. Check it out. See what I've got.*
> *Trust me bruv, you're going to get one call from me, yeah?*
> *Pay up, because I've got some funny looking shit on your server bruv, you understand what I'm saying?*
> *You know what I mean? Get it done, or I'm going to cause you some fucking shit bruv.*

> *Best bit of advice for ya. Take it, read it, pay it, forget it.*
> *We will fuck you up. You won't get us. You won't get away.*
> *Have a good day.*

available at https://www.youtube.com/watch?v=DzApepLbA70&feature=youtu.be.

The sentence imposed by the court should reflect the seriousness of this offense. As one victim reported, reflecting on the text messages sent from a phone account registered by the defendant, the "memory of the trauma can't be erased by monetary repayment;" "our daily lives have never been the same since reading the emails and messages." PSR ¶ 40.

2. **The Sentence Should Reflect the Defendant's History and Characteristics.**

Although the defendant has no criminal history points as computed under the guidelines, he was convicted of several fraud offenses in the United Kingdom before his extradition to the United States. PSR ¶¶ 97, 137. The government is not seeking a departure based on the defendant's criminal record, but it is a relevant consideration in our request for a guidelines sentence. In particular, the defendant previously pled guilty to a similar scheme in which he sought a ransom payment from a British law firm in exchange for data stolen from that firm's computer network. PSR ¶ 96; Gov't Exhibit F. He was also convicted for credit card fraud schemes. *Id.* The defendant was sentenced to 42 months in prison for these convictions. Had these convictions occurred domestically, the defendant would likely been in a criminal history category II, and his guideline range would be 57–71 months. U.S.S.G. § 4A1.1(a).

Upon his release from prison, the defendant will likely be repatriated to the United Kingdom, where he will not be subject to supervision by the Probation Office and where U.S. law enforcement will have limited ability to monitor his actions. A guidelines sentence is especially appropriate in light of the fact that meaningful supervised release is unlikely.

3. **The Sentence Should Deter Organized Computer Hacking.**

Criminal operations like this conspiracy represent a significant threat to public

safety. Our society relies on internet-connected computers and networks to safeguard our most private data, like the medical and financial records exploited by the defendant. Imposing a serious punishment would reflect society's substantial interest in safeguarding our computers and systems from the kind of unlawful activity that the defendant engaged in. The sentence should resonate with the defendant and the many current and would-be hackers who calculate cybercrime to be a low-risk, high-reward proposition, especially those who believe that foreign borders protect them from facing justice in the United States for their crimes against American victims.

III. Conclusion

For all of these reasons, the United States asks the Court to accept the plea agreement and impose a sentence within the sentencing guidelines.

Respectfully submitted this 14th day of September, 2020.

JEFFREY B. JENSEN
UNITED STATES ATTORNEY

/s/ Laura-Kate Bernstein
LAURA-KATE BERNSTEIN
Senior Counsel
Maryland Bar Number 1212110224
Computer Crime & Intellectual Property Section
U.S. Department of Justice
Email: Laura-Kate.Bernstein@usdoj.gov

/s Gwendolyn E. Carroll
Gwendolyn E. Carroll #NY4657003
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, Missouri 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on September 14, 2020, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the Attorneys of Record.

/s/ Laura-Kate Bernstein
LAURA-KATE BERNSTEIN