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

Alexandria Division

UNITED STATES OF AMERICA v. ALEXANDER KONSTANTINOVICH TVERDOKHLEBOV, Defendant.	Case No. 17-CR-9

AMENDED POSITION OF THE UNITED STATES ON SENTENCING

The defendant, Alexander Tverdokhlebov, ran a sophisticated scheme to steal and traffic sensitive personal and financial information in the online criminal underground. For nearly ten years, Tverdokhlebov belonged to elite Russian-speaking cybercrime forums whose sole purpose is to facilitate crime, much of which targets U.S. businesses and citizens. Through his membership on these forums, Tverdokhlebov forged lucrative business partnerships with other Russian-speaking cybercriminals, with whom he exchanged tools, services, and stolen personal and financial information. As part of his scheme, the defendant controlled botnets (i.e., large groups of computers infected with malicious software) that enabled Tverdokhlebov to extract sensitive personal information and financial account information from victims' computers. In order to "cash out," or turn stolen personal financial information into money, Tverdokhlebov recruited Russian students visiting the United States on J-1 visas. Tverdokhlebov convinced these students to open bank accounts in their names, receive money into those accounts from victim accounts controlled by Tverdokhlebov or his co-conspirators, and then transfer the money to Tverdokhlebov or his co-conspirators.

Cybercrime was profitable for the defendant. He earned over a million dollars of criminal proceeds, drove a BMW, and frequently took lavish vacations. PSR ¶ 26. When the Secret Service finally caught up to him, they seized $272,000.00 in one hundred dollar bills, which Tverdokhlebov had spread across four safe deposit boxes in Los Angeles and Las Vegas.

The defendant pled guilty and stipulated to a loss of $9.5 to $20 million. Based on this loss, and the other stipulated enhancements, the presentence report correctly calculated the defendant's guidelines range as **97-121 months' imprisonment**. The government respectfully recommends a sentence within this range given the breadth of the harm caused by the defendant's conduct and the need to deter similarly sophisticated crime.

I. Offense of Conviction

The defendant became a member of elite Russian-speaking cybercrime forums beginning in or around 2008. PSR ¶ 10. Membership to these forums is lucrative: it gives a cybercriminal access to other highly skilled cybercriminals with whom he or she can exchange advice and services in the furtherance of schemes more complex and far-reaching than ones many cybercriminals could undertake alone. The forums also serve as a marketplace for cybercriminals to sell stolen credit card information, known as "dumps," or recruit others to help them "cash out," or extract money using stolen financial information.

The cybercrime forums to which the defendant belonged allowed him to do exactly that. Tverdokhlebov used the forums to sell stolen credit card and other financial information to buyers. *Id.* Some of the stolen credit card and financial information had been obtained using "botnets." Botnets are networks of victim computers (known as "bots") which have been infected with malicious software ("malware"). They can be used for a number of criminal purposes, including

to steal sensitive information from the victim computers, or to use the victim computers to attack other computers, such as through a Distributed Denial of Service (DDoS) attack. From 2010 through 2015, the defendant used a botnet to steal sensitive financial information from at least 100 victims, which included the Pay Pal account of at least one victim residing in the Eastern District of Virginia. PSR ¶ 25. As noted below, in addition to personally using botnets to steal financial information, the defendant also offered to rent his botnet to other cybercriminals.

Contacts the defendant made through the cybercrime forums became important collaborators in his criminal activities. From May 2008,[1] through on or about February 2010, Tverdokhlebov used ICQ, a brand of software for instant chat messaging, to communicate with another cybercriminal, for the purpose of devising and executing a scheme to defraud. PSR ¶ 20. In particular, he discussed with a Russian cybercriminal, known as V.P., who was then located abroad, how to use stolen online banking passwords and login credentials to make fraudulent transfers; how to use a botnet to steal online banking passwords and login credentials; and how to mine stolen data to find victims' online banking passwords and login credentials. *Id.*; Statement of Facts (hereinafter, "SOF") ¶ 6-8. The defendant also instructed V.P. to make fraudulent purchases using stolen passwords and credentials. SOF ¶ 8.

As part of his scheme, Tverdokhlebov also recruited and supervised others in the creation of financial accounts that were used to receive and transfer stolen money. PSR ¶ 10. For example, Tverdokhlebov recruited Russian students living in the United States to open bank accounts to receive funds stolen from a compromised bank account and to transfer that money to Tverdokhlebov and his co-conspirators. *Id.* ¶¶ 11, 24.

[1] The Sentencing Memorandum filed on June 30, 2017 contained a typographical error that stated that Tverdokhlebov used ICQ from May 2007 onwards.

A sampling of the defendant's messages on cybercrime forums provides a window into the scope of his criminal enterprise. At various dates between 2009 and 2013, the defendant made the following representations on criminal online forums;

- That he possessed 40,000 stolen credit card numbers and was soliciting buyers for the stolen information, SOF ¶ 9(a);
- That he had control of or operated a botnet with 10,000 bots and that cybercriminals could contact him to rent this botnet, SOF ¶ 9(b);
- That he had control of or operated a botnet with 300,000 bots and that cybercriminals could contact him to rent this botnet, SOF ¶ 9(c);
- That he had control of or operated a botnet with 500,000 bots and that cybercriminals could contact him to rent this botnet, SOF ¶ 9(d); and
- That he was willing to sell stolen credit card numbers in increments of 1,000 and that the "validity" of these "dumps" was 90%, meaning that 90% of these credit card numbers were active, and thus could be used to extract funds, SOF ¶ 9(e).

On February 1, 2017, federal agents arrested the defendant in his Los Angeles home and executed a search warrant on his home. They recovered numerous digital devices. They also recovered keys to safe-deposit boxes located in several different Los Angeles bank locations, as well as one located in Las Vegas. Those safe-deposit boxes contained a total of **$272,000 in cash**, in addition to electronic devices.

On March 31, 2017, the defendant pled guilty to Count One of the Indictment, which charged him with Wire Fraud, in violation of 18 U.S.C. § 1343. In exchange for his guilty plea, the United States moved to dismiss the remaining counts. Count One carries maximum penalties of twenty years' imprisonment, a $1 million fine, restitution and forfeiture, a special assessment, and three years' supervised release.

II. Guidelines Range

The probation officer correctly calculated the defendant's offense level as follows:

Guideline	Offense Level
Base Offense Level (Sections 2B1.1(a)(1))	7
Loss amount between $9 Million but less than 25 Million	+20
Offense involved receiving stolen property and the defendant was in the business of receiving and selling stolen property (Section 2B1.1(b)(4))	+2
Substantial part of offense committed abroad (Section 2B1.1.(b)(10))	+2
Offense involved the production or trafficking of an unauthorized access device or counterfeit access device, or authentication feature (Section 2B1.1(b)(11))	+2
Acceptance of responsibility (Section 3E1.1)[2]	-3
TOTAL	**30**

PSR ¶¶ 37-49. Based on the defendant's Category I Criminal History, the resulting Guidelines Range is **97-121 months' imprisonment**. *Id.* ¶¶ 73-75.

III. Sentencing Recommendation

As the Court is well aware, the Sentencing 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).[3] Here, however, a within-Guidelines sentence is also supported by the other § 3553(a) factors, particularly the need for a sentence that reflects the seriousness of the offense and adequately deters others from perpetrating similar crimes.

[2] The Government hereby moves, under U.S.S.G. § 3E1.1(b), for a third point to be reduced from the defendant's offense level, based on the defendant's timely acceptance of responsibility.

[3] 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. The Sentence Should Reflect the Harm Caused to Individuals, the Banking Industry, and Businesses.

The full harm caused by the defendant's scheme is difficult to calculate. The parties have stipulated to a provable loss amount of $9 million to $25 million based on a conservative estimate of the 42,000 stolen credit card numbers or identifiers that the defendant possessed and attempted to sell in bulk to others. The Advisory Notes to Section 2B1.1 of the U.S. Sentencing Guidelines provide that, "[i]n a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and *shall be not less than $500 per access device*" (emphasis added).[4] Accordingly, the loss associated with 42,000 stolen credit card numbers or identifiers is $21 million,[5] or the result of 42,000 multiplied by $500. *See* PSR ¶¶ 23, 38.

Additionally, a loss of $77,000 resulted from the defendant's recruitment and supervision of two Russian students who opened bank accounts to receive stolen funds from a compromised

[4] "Access device" is defined at 18 U.S.C. § 1029(e)(1) as any "card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds . . . ." "Counterfeit access device" is defined at 18 U.S.C. § 1029(e)(2) as "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device." "Unauthorized access device" is defined at 18 U.S.C. § 1029(e)(3) as "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud."

[5] The United States' previous filing inadvertently reported this figure as $20 million.

J.P. Morgan Chase Bank account and transferred and attempted to transfer those funds to the defendant. PSR ¶¶ 11, 24, 38.

Because of the high volume of stolen information trafficked by Tverdokhlebov over the span of the offense conduct, it is difficult to identify specific harms that may have befallen those whose information was stolen and traded. However, it is possible that Tverdokhlebov's buyers used the stolen credit card information they had purchased from him to commit fraud in individual victims' names, and that those individual victims incurred expenses to rectify identity theft or to prevent future identity theft.

Further, when banks and businesses sustain fraud-related losses or expenses, they generally pass these costs on to the average American in the form of higher prices, fees and other indirect charges. *See* Lydia Segal, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743, 754, 775 (2011) (banks and credit card companies pass on costs of fraud to consumers in the form of higher prices, banking costs, and other charges); *see also* Ronald Mann, *Credit Cards and Debit Cards in the United States and Japan*, 55 VAND. L. REV. 1055 (2002) (credit card companies pass on costs of fraud to cardholders and merchants).

Finally, it is hard to overstate the disruption to the nation's banking industry and the erosion of consumer confidence in online transactions caused by sophisticated criminal operations like the defendant's. The defendant's sentence should reflect the seriousness of these harms.

B. The Sentence Should Be Sufficient to Deter Others from Engaging in Lucrative Schemes Like the Defendant's.

The defendant earned a significant profit from his scheme. Prior to the defendant's arrest, the defendant owned and drove a BMW, and had **$272,000 in cash** divided amongst several safe-

deposit boxes in Los Angeles and Las Vegas, which he had opened in case of a "bad day." These emergency funds represent a small fraction of the criminal proceeds of his crimes; prior to his arrest, the United States learned that the defendant had received approximately **one million dollars** in wire transfers from Russia and China and was aware he had assets in bank accounts located in the United States and abroad. In the years leading up to the defendant's arrest, the defendant vacationed in exotic locations all over the world several times a year, often staying in luxury resorts.

The defendant's lifestyle and profits are relevant because they demonstrate a larger problem: cybercriminals like the defendant are able to make massive amounts of money by victimizing innocent people from the comfort and anonymity of their living rooms. Like the defendant, these criminals often operate with impunity for years and begin to feel invincible. And all too many people are willing to commit the crimes the defendant committed for a chance at the extravagant lifestyle he enjoyed.

Unfortunately, high rewards and relatively low risk of detection are basic features of cybercrime that are not going to change anytime soon. The only way to affect the cost-benefit analysis of these crimes is to impose meaningful sentences on those who are caught. If the Court does so, there is every reason to believe that many would-be criminals will get the message. Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor the government's response to cybercrime and plan accordingly. Achieving general deterrence in this area therefore appears particularly promising. *See 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").

IV. Conclusion

The government respectfully recommends a sentence of 97-121 months' imprisonment, as well as the agreed-upon forfeiture and restitution orders.

Dana J. Boente
United States Attorney

By: /s/
Laura Fong
Kellen S. Dwyer
Assistant United States Attorneys

July 3, 2017

Certificate of Service

I hereby certify that on July 3, 2017, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to counsel of record for the defense.

I also certify that on July 3, 2017, I will send a true and correct copy of the foregoing by e-mail to the following:

Quentin Lowe
United States Probation Officer
Quentin_Lowe@vaep.uscourts.gov

By: /s/
Laura Fong
Kellen S. Dwyer
Assistant United States Attorneys
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
laura.fong@usdoj.gov
kellen.dwyer@usdoj.gov