ALEX G. TSE (CABN 152348)
Acting United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JOHN H. HEMANN (CABN 165823)
JEFFREY SHIH (MABN 663195)
Assistant United States Attorneys

SCOTT K. MCCULLOCH (DCBN 1020608)
CHRISTOPHER OTT (CABN 235659)
Trial Attorneys, National Security Division

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
john.hemann@usdoj.gov; 415.436.7478
jeffrey.shih@usdoj.gov; 415.436.7168

Attorneys for the United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. KARIM BARATOV, Defendant.	CASE NO. 3:17-CR-103 VC UNITED STATES SENTENCING MEMORANDUM Sentencing Date: April 24, 2018 Time: 10:30 a.m. Court: Honorable Vince Chhabria

I. INTRODUCTION

Between 2010 and 2017, Defendant Karim Baratov hacked into the webmail accounts of more than 11,000 victims, broke into his victims' digital records, and sold that stolen access to his victims' private lives. To enrich his own life and to live lavishly, he took customer orders to target specific victims and gave his customers the ability to exploit those victims even further without needing any explanation from his customers about their identity, motives, or plans. And between 2014 and 2016, as an international hacker-for-hire, the defendant hacked without any discussion or hesitation for a paying customer who turned out to be Co-Defendant Dmitry Dokuchaev, an officer for the Russian Federal

Security Service (the "Russian FSB"). Co-Defendant Dokuchaev engaged criminal hackers to break into computers around the world, hacked into the Yahoo network with other co-conspirators, and based on information stolen in the Yahoo hack, paid the defendant to target and break into at least 80 webmail accounts of individuals that were of interest to Russian intelligence.

For his criminal conduct, the defendant pleaded guilty pursuant to Rule 11(c)(1)(A) and 11(c)(1)(B) to Count One, charging him with conspiracy to commit computer fraud and abuse in violation of 18 U.S.C. § 1030(b), and to Counts Forty through Forty-Seven, charging him with aggravated identity theft in violation of 18 U.S.C. § 1028A. The United States concurs with Probation that the defendant's applicable Sentencing Guidelines range is 70 to 87 months for Count One and that the defendant faces a consecutive term of 2 to 16 years for Counts Forty through Forty-Seven. For the following reasons, especially the pressing need to deter international cybercriminals from providing hacker-for-hire services that facilitate additional criminal activity (including acts for foreign intelligence services), the United States respectfully recommends that the Court impose a sentence of 94 months imprisonment (low end of the Guidelines range, plus 2 years consecutive), 3 years supervised release, and restitution and fine amounts that encompass any and all of his assets.

II. BACKGROUND

A. Summary of Criminal Conduct

Between 2010 and 2017, Defendant Karim Baratov hacked into more than 11,000 webmail accounts in exchange for money. Plea Agreement ¶ 2.a, d. The defendant operated his illegal hacking business from his home in Ontario, Canada. Through websites he hosted, the defendant advertised his services to Russian-language speakers throughout the world and collected orders from interested customers, who identified specific webmail accounts for the defendant to target. *Id.* ¶ 2.b.

One of the defendant's Russian websites was named "webhacker," advertised his services as providing "Hacking of email accounts without prepayment," and stated that he could hack into webmail accounts maintained by Google and Russian webmail providers, such as Mail.ru and Yandex. *Id.*; PSR ¶ 10. The defendant stated on the website that he would provide the customer with a screen shot of the hacked email account. Additionally, the defendant stated that he could change the login challenge question and answer in order to ensure that the customer could maintain stolen access to the victim's

webmail account. PSR ¶ 11. The defendant directed potential customers to submit through his websites their "order[s] for hacking of email account[s]" by completing and submitting a form (*e.g.*, customer email account, webmail account to hack, additional services requested, method of payment). *Id.*

The defendant hacked into the webmail accounts by spear phishing his victims. Specifically, to trick his victims to provide him the passwords to their webmail accounts, the defendant fraudulently impersonated the webmail providers that his victims trusted. Plea Agreement ¶ 2.c. He constructed fraudulent "spoofed" websites that mimicked the appearance of the login page of the actual webmail providers. He also created fraudulent email accounts with addresses that combined the actual (or slightly misspelled) names of webmail providers with terms such as "support. After receiving a customer's order to target a specific victim webmail account, the defendant used his fraudulent email accounts to send an email mimicking the webmail provider's customer support and directing the victim to click on a link to one of his "spoofed" websites. A victim who clicked on the link would be asked to enter the password to the victim's webmail account, and scripts embedded in the "spoofed" websites by the defendant would send the victim's password to him by email. *Id.* Upon stealing a victim's password, the defendant used the stolen password to access the contents of the victim's webmail account and to take a screen shot of the victim account's contents. The defendant used such screen shots as proof to demand payment from his customers. After receiving payment, the defendant sent the stolen password to the customer that targeted the victim. *Id.* ¶ 2.d. The defendant setup his infrastructure, including over eighty advertising and "spoofed" websites, fraudulent customer support email accounts, and email accounts he used to receive customer orders and stolen passwords, on servers throughout the world. *Id.* ¶ 2.b, c; PSR ¶ 9.

With the stolen passwords, the defendant knew that his customers had full access to the information contained in and full control of the victim accounts, including the victims' private communications. Plea Agreement ¶ 2.d. Indeed, at times, the defendant personally deleted the contents of victims' webmail accounts or changed the passwords for those accounts. Additionally, the defendant at times commandeered the webmail accounts he hacked and operated through them to conceal his identity while hacking the webmail accounts of other victims. *Id.* ¶ 2.h.

The defendant maintained records of the webmail accounts that he successfully hacked. Decl. of FBI Special Agent Aleksandr Kobzanets ("Kobzanets Decl.") ¶ 2. The digital records that the defendant maintained (and did not delete), much like the digital records of the victims that he hacked into, spanned years of his life. For example, he kept his email correspondence with customers through which he demanded payment and provided screen shots of the contents of the victim accounts as proof of his successful hacking. That correspondence identified the more than 11,000 webmail accounts that the defendant hacked in exchange for money. Kobzanets Decl. ¶ 2.a. That correspondence also showed that as long as he was paid, the defendant hacked into victim webmail accounts with little, if any, discussion with his customers about their identity, motives, or plans. *Id.* In July 2010, for example, the defendant received an email from one of his customers that contained a list of services with prices for hurting or killing people. The FBI was unable to ascertain the identity of this customer, and the correspondence did not indicate whether the email was solicited by or intended to be sent to the defendant. Nonetheless, the defendant subsequently provided that customer with stolen passwords for targeted victims; and the defendant exchanged emails with that customer through August 2012 about the hacking of and payment for additional victims' webmail accounts. *Id.* ¶ 2.b. The defendant also had a correspondence folder titled "victims," in which he maintained some of his correspondence with victims who had discovered that their accounts had been hacked. For example, in certain instances the defendant deleted the victim account's emails because the customer refused to pay, and the victim responded with an email to the defendant asking for the return of the victim's emails. *Id.* ¶ 2.c.

The defendant's customers included Co-Defendant Dmitry Dokuchaev, who the defendant knew at the time as "Patrick Nagel" or "Patrick Nag". Plea Agreement ¶ 2.a. Between 2014 and 2016, Co-Defendant Dokuchaev requested that Defendant Baratov hack into at least 80 webmail accounts, including at least 50 at Google, in exchange for money. *Id.*; Indictment ¶ 83. As with most of the defendant's other customers, the defendant did not discuss with Co-Defendant Dokuchaev his identity, motives, or plan, *e.g.*, how Co-Defendant Dokuchaev was an officer with the Russian FSB, how he had engaged other co-conspirator criminal hackers to break into the Yahoo network, or how, based on information stolen in the Yahoo hack, the targeted victims were of interest to Russian intelligence. Plea Agreement ¶ 2.a, i.

Regardless, in exchange for money, the defendant agreed to and attempted to hack into the webmail accounts targeted by Co-Defendant Dokuchaev and other co-conspirators, including the webmail accounts of prominent leaders in the commercial industries and senior government officials (and their counselors) of Russia and countries bordering Russia. PSR ¶ 13; *see also* Indictment ¶¶ 7, 34.b, 42-46. Of the more than 80 webmail accounts, the defendant succeeded in hacking into 18, including the webmail accounts at Google charged in Counts Forty through Forty-Seven. Co-Defendant Dokuchaev paid the bounty for each of the accounts that the defendant succeeded in hacking. Kobzanets Decl. ¶ 2.d; Plea Agreement ¶ 2.g.

The defendant accepted payment in various currencies from his customers, such as Co-Defendant Dokuchaev, through U.S. or foreign online payment services located throughout the world, including PayPal, WebMoney, and Yandex. Plea Agreement ¶ 2.e; Kobzanets Decl. ¶ 6.a. Through his criminal hacking, the defendant received approximately $100 each for hacking more than 11,000 victim webmail accounts. These criminal payments constituted his only significant source of income. Plea Agreement ¶ 2.d, e; PSR ¶¶ 15, 61. To use those funds, the defendant either converted funds to cash through brokers in Canada or transferred funds to PayPal or bank accounts in Canada.[1] Kobzanets Decl. ¶ 6.b, c. As reflected in the numerous posts on his social media accounts, *id.*, at ¶ 3, the defendant spent his criminal proceeds on a lavish lifestyle. He financed a $650,000 home, bought and financed a number of high-end luxury vehicles (*e.g.*, Lamborghini, Porsche, Aston Martin, Mercedes, BMW), and posted photographs of himself on social media with a fanned-out stack of $100 Canadian bills. *Id.*; PSR ¶ 14, 64-65.



[1] As described in his financial deposition, the defendant provided his accountant records only for his bank account at the Royal Bank of Canada, which received only a portion of his criminal proceeds. *See* Kobzanets Decl. ¶ 6.

The defendant appears to have spent his illegal proceeds as he was paid and to have leveraged those proceeds to spend even more. PSR ¶¶ 63-65. Indeed, the only assets that appear to remain are the $30,000 CAD (from his home) and $900 CAD (from his wallet) that the Royal Canadian Mounted Police seized at the time of his arrest, and $1,500 USD in his PayPal account. PSR ¶ 66; Kobzanets Decl. ¶¶ 4, 7.

B. Procedural History

In February 2017, the Grand Jury returned an Indictment in the Northern District of California charging Defendants Dokuchaev, Igor Sushchin, Alexsey Belan, and Karim Baratov with a number of offenses relating to the hacking of webmail accounts at Yahoo and other service providers. Docket No. 1. In connection with the Indictment, Interpol Red Notices were requested and issued, or updated, for each of the charged defendants. PSR ¶ 5. Defendants Dokuchaev, Sushchin, and Belan[2] have been reported to be in Russia, which has no extradition treaty with the United States. *Id.*

Defendant Baratov was arrested by the Royal Canadian Mounted Police and the Toronto Police Department on March 14, 2017. PSR ¶ 6. The Superior Court of Justice in Ontario ordered him detained on April 11, 2017. Kobzanets Decl. ¶ 4. The Court of Appeal for Ontario affirmed that decision on June 9, 2017. *Id.* Defendant Baratov waived extradition to the United States on August 22, 2017, and made his initial appearance in the Northern District of California in August 23, 2017. PSR ¶ 6. Under the Plea Agreement, he pleaded guilty to Counts One and Forty through Forty-Seven on November 28, 2017. Docket No. 25.

Pursuant to the Crime Victims' Rights Act, codified at 18 U.S.C. § 3771, the Court authorized the United States to employ alternative notification procedures, specifically, the Justice Department's website for large cases in order to provide notice to the large number of potential victims in this case in December 2017. Docket No. 27. The United States made that website available at https://www.justice.gov/largecases and https://www.justice.gov/usao-ndca/us-v-dmitry-dokuchaev-et-al. Additionally, the United States emailed victim notifications to and requested Victim Impact Statements

[2] Defendant Belan had been previously indicted for hacking the computer networks of e-commerce companies in Nevada in 2012 and in California in 2013, but absconded to Russia after he was arrested on those earlier charges (not the Indictment in this case) and released on bail in Greece. PSR ¶ 5.

(and documentation supporting restitution claims) from the more than 11,000 webmail accounts[3] that Defendant Baratov hacked. PSR ¶ 17. Of those accounts, approximately 9,000 were operated by service providers in Russia and 2,000 were operated by service providers in the United States. *Id.*; Kobzanets Decl. ¶ 5. More than 4,000 of the victim notifications that the United States emailed were returned as undeliverable. PSR ¶ 17; Kobzanets Decl. ¶ 5.

To date, the United States received responses from three victims, which are summarized in this public filing without identifying information as follows:[4]

1. ************age@gmail.com** ("Victim 1"): Victim 1 stated in an email response that (a) he operates a company that tours in the Russian Federation and a country bordering Russia; (b) he detected the intrusion in August 2017; and (c) his business correspondence and more than 200 copyrighted items were stolen, resulting in losses of more than $50,000. PSR ¶ 22 (referring to victim information forwarded by Probation to Court, *see* PROTECTED-3); *see also* PSR ¶ 18. The United States requested, but did not receive, a Victim Impact Statement.

2. *********led@gmail.com** ("Victim 2"): Victim 2 stated that he received several items of strange correspondence in 2015 to 2016, which he interpreted as an attempt to hack into his email. Victim 2 stated that he worked at the time for the state administration of a Regional Governor in a country bordering Russia. Victim 2 did not know if his email account had been hacked and had no financial losses to claim. Victim 2 did state, however, that the potential for damage constantly disturbs him and he provided a Victim Impact Statement. PSR ¶ 22 (referring to victim information forwarded to Court, *see* PROTECTED-28 to 37); *see also* PSR ¶ 19.

3. *******uzi@gmail.com** ("Victim 3"): Victim 3 stated in a Victim Impact Statement that (a) he was a lawyer in a country bordering Russia; (b) the email account that he used for both his personal and business email was hacked in April 2015 by one of his client's

[3] As noted in the United States motion to use these alternative notification procedures, these constituted the primary, if not the only, identifying information of the known potential victims of Defendant Baratov's spear phishing. Additionally, to the extent that the victims continued to use the accounts hacked by the defendant, attempts by the United States to contact the victims may have appeared similar to the defendant's spear phishing criminal conduct, in which he impersonated trustworthy entities through fraudulent email accounts and "spoofed" websites. Docket No. 26, at 3.

[4] The United States has provided the victim responses to the defendant, to Probation, and (through Probation) to the Court as documents Bates-stamped PROTECTED-3 through 49.

adversaries; (c) to steal his webmail account password, the adversary paid for the services of a hacker, who used the email account corp@eml.cc;[5] (d) using Victim 3's stolen password and webmail account, the adversary distributed private information and photographs of Victim 3's client to over 300 users of a website and a mobile application; (e) Victim 3 sustained a financial loss of approximately $2,000, which the adversary paid after being convicted in the country bordering Russia for having Victim 3's account hacked; and (f) he sustained a consequential loss of business from his client of approximately $10,000.[6] PSR ¶ 22 (referring to victim information forwarded to Court, *see* PROTECTED-4 to 27, 38 to 49); *see also* PSR ¶ 20. Victim 3 provided a copy of the foreign judgment against the adversary, which has been translated and indicates a sentence of "punishment in the form of restraint for a period of 1 (one) year and 6 (six) months" and monetary judgments to the client, the victim, and the government. PSR ¶ 22 (referring to victim information forwarded to Court, *see* PROTECTED-48 to 49).

III. SENTENCING GUIDELINES CALCULATION

A. Count One: Conspiracy to Commit Computer Fraud

The United States concurs with Probation's calculation of the Sentencing Guidelines for Count One. *See* PSR ¶¶ 27-39, 43-44, 71, 78. Specifically, for Count One, the total adjusted offense level is 27, which includes:

a.	**Base Offense Level**, USSG §2B1.1(a)(2):	6
b.	**Loss Amount**, USSG § 2B1.1(b)(1)(J): The defendant hacked into webmail accounts by deceiving victims into disclosing their passwords and selling those stolen passwords. Under Application Note 3(F)(i) of USSG § 2B1.1, the loss from such conduct "shall be not less than $500 per access device," *i.e.*, stolen password. As he admitted in Paragraph 2.d of his Plea Agreement, the defendant hacked into the webmail accounts of more than 11,000 victims and thus, for Sentencing Guidelines purposes, his hacking conduct caused a loss of more than $3.5 million.[7]	+18
c.	**Ten or More Victims**, USSG § 2B1.1(b)(2)(A)(i):	+2

[5] This is one of the accounts that the defendant created, maintained, and used to spear phish his victims. Kobzanets Decl. ¶ 2.

[6] The United States requested documentary support for this consequential loss of business. The victim stated that he could not provide such documentation without the consent of his client and thus, relied only on the foreign judgment.

[7] For 11,000 hacked accounts, a loss of $500 per account results in a loss of $5.5 million.

d. **Sophisticated Means**, USSG § 2B1.1(b)(10): +2

e. **Conviction of Offense Under 18 U.S.C. § 1030 With Intent to Obtain Personal Information**, USSG § 2B1.1(b)(17)(A): +2

f. **Acceptance of Responsibility**, USSG § 3E1.1: -3[8]

See also Plea Agreement ¶ 7. The defendant has no prior convictions and no criminal history points and thus, falls into Criminal History Category I. PSR ¶¶ 43-44. The resulting Sentencing Guidelines range for Count One is a term of imprisonment of 70 to 87 months. PSR ¶ 71. Based on the offense level, the Sentencing Guidelines also provide for a fine range of $25,000 to $250,000. PSR ¶ 78.

B. Counts Forty Through Forty-Seven: Aggravated Identity Theft

For Counts Forty through Forty-Seven, the United States concurs with Probation that 18 U.S.C. § 1028A(b)(2) provides for a 2-year term of imprisonment that must be imposed consecutively to any term of imprisonment for Count One. PSR ¶¶ 40, 70; *see also* Plea Agreement ¶ 7; USSG § 5G1.2 (stating that statutory violations providing a consecutive term of imprisonment shall be determined by statute and imposed independently).

Under 18 U.S.C. § 1028A(b)(4) and Application Note 2(B) of USSG § 5G1.2, the Court may run the 2-year terms for the § 1028A counts concurrently with one another. The United States concurs with Probation that the 2-year terms for Counts Forty through Forty-Seven should run concurrently with one another pursuant to 18 U.S.C. § 1028A(b)(4). PSR Sentencing Recommendation, at 3; Plea Agreement ¶ 21; *see also* USSG § 5G1.2, Application Note 2(B) (providing consideration of 18 U.S.C. § 3553(a)(2) factors). The United States thus concurs with Probation that Counts Forty through Forty-Seven should result in the addition of 2 years (*i.e.*, not 16 years) to the term of imprisonment imposed for Count One.

[8] The defendant waived extradition to the United States approximately four months after his arrest in Canada, and agreed to and did plead guilty approximately three months after his initial appearance in the United States. Assuming that the defendant continues to admit his guilt and manifest an acceptance of responsibility through sentencing, the United States agrees that the third-point for acceptance of responsibility is appropriate under USSG § 3E1.1.

IV. SENTENCING RECOMMENDATION

The United States recommends that the Court impose a sentence of 94 months imprisonment (low end of the Guidelines range, plus 2 years consecutive), 3 years supervised release, and restitution and fine amounts that encompass any and all of his assets.

A. Sentence of Imprisonment

As indicated by the Sentencing Guidelines range, a significant sentence of imprisonment is necessary to reflect the nature, circumstances, and seriousness of the offense, to promote respect for the law, to provide just punishment, and to afford adequate deterrence to such criminal conduct. *See* 18 U.S.C. § 3553(a)(1), (2)(A), 2(B). Such imprisonment is especially necessary in this case where the defendant sold his hacker-for-hire services and targeted victims with little to no consideration of his customers' identities, motives, or plans, including Co-Defendant Dokuchaev who worked for the Russian FSB and who perpetrated with other co-conspirators the largest reported data breach in history by hacking into the Yahoo network.

Defendant Karim Baratov's criminal conduct is egregious, extensive, and reprehensible. For years, he profited as an international cybercriminal, taking orders from paying customers to break into the private digital records of more than 11,000 victims. Sitting behind a keyboard at his home in Canada, he setup and used a hacking infrastructure, including eighty advertising and "spoofed" websites, fraudulent customer support email accounts, and email accounts he used to receive customer orders and stolen passwords, on servers throughout the world so that he could conceal his identity and location. Similarly, he advertised his services to Russian-language speakers and accepted payment at online payment services throughout the world, including WebMoney and Yandex. Hacking with impunity, the defendant gave little to no consideration to what his customers did with the passwords that the defendant stole or the potential impact on the victims that he and his customers targeted. Indeed, as long as he was paid, the defendant went about hacking into victim accounts and enjoying the criminal proceeds.

In effect, the defendant stole and provided to his customers the keys to break into the private lives of targeted victims. As the Supreme Court recognized in *Riley v. California*, 134 S. Ct. 2473 (2014), people maintain "digital record[s] of nearly every aspect of their lives" with the pervasive and insistent modern technologies that have become part of daily routines. *Id.* at 2490 (holding that search

incident to arrest exception to warrant requirement does not apply to cell phones). Such digital records contain caches of personal information (*e.g.*, addresses, communications, locations, notes, prescriptions, bank statements, photographs, videos) that can span years and that can enable all aspects (whether mundane or intimate) of an individual's private life to be reconstructed. *Id.* at 2489-2490. The passwords that the defendant fraudulently stole through spear phishing allowed his customers to view and to use for any purpose all of the digital records maintained by the victims, including any and all private and intimate communications, photographs, and videos. The defendant also provided additional services (*e.g.*, changing login challenge questions and answers) to ensure that his customers could attempt to maintain stolen access to the victim accounts after the victims realized their accounts had been hacked.

Moreover, the defendant's hacker-for-hire services enabled his customers not only to view the entire contents of, but also to commandeer the targeted victim accounts. Victim 3, for example, provided a foreign judgment that described (i) the defendant stealing the password to Victim 3's account for the defendant's customer, and (ii) the customer subsequently using Victim 3's account to distribute private information and photographs of Victim 3's client. The defendant himself at times used the webmail accounts that he previously hacked in order to hack other victims, thereby further concealing the defendant's identity. Similarly, it is not uncommon for individuals to use the same password for more than one account. *See, e.g.*, "Reusing Passwords on Multiple Sites," Center for Internet Security, June 15, 2016, *available at* https://www.cisecurity.org/reusing-passwords-on-multiple-sites/ (last visited April 17, 2018) (citing surveys showing password reuse rates between 31% and 55%). The access to a victim's email account also facilitates access to a victim's other web accounts, including financial accounts and social media accounts. *See, e.g.*, "The Value of a Hacked Email Account," Krebs on Security, June 10, 2013, *available at* https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/ (last visited April 17, 2018) (describing how person in control of hacked email account can reset password for and gain access to other victim services and accounts). This was the full and stolen access to the victims that the defendant sold, and the access for which the defendant's customers paid.

This is not a case of a teenager making an isolated mistake on the Internet out of curiosity. Rather, this is a case of the defendant making a profession out of breaking into the private lives of

thousands of victims. The defendant setup, operated, and grew a criminal hacker-for-hire business that gave his customers the ability (and provided a layer of concealment for their identities) to commit a whole spectrum of additional crimes (*e.g.*, against the victims' dignity, finances, safety, privacy, or other interests). The defendant's decision to engage in such criminal activity repeatedly for profit should not be lightly punished.

The defendant has no reasonable excuse for this criminal conduct. The defendant grew up in a close and supportive family. His parents were employed professionals, involved in his life, and provided him a financially stable environment, in which he lived in nice neighborhoods and his basic needs were always met. PSR ¶ 50. Despite these opportunities and resources, which many other individuals who come before this Court do not have, the defendant decided to use the Internet to deceive and to steal from others so that he could live a more lavish life.

A significant sentence of imprisonment in this case is particularly important to promote respect for the law and to deter others sufficiently from such criminal conduct. This case has generated substantial media attention, and international cybercriminals like the defendant are often skilled and well-informed. They know that they can generate massive profits at a keyboard, at a young age, without ever having face-to-face contact with their criminal co-conspirators and victims. For minimal costs, they know that they can setup and operate their hacking at a distance – through accounts, websites, and servers across the world – to conceal their identities and whereabouts and to make efforts required for law enforcement investigations more burdensome.[9] They know that targeting populations outside of their countries of residence can further reduce the risk of law enforcement investigation in their countries of residence and can make the investment of law enforcement resources from abroad more difficult. Even if they are identified and caught, they know that the number of different accounts, websites, and servers that they use can conceal the full scope of their criminal conduct from the authorities. In light of these aspects of the defendant's criminal conduct, significant consequences should be imposed on cybercriminals such as the defendant who advertise their services blatantly and who hack thousands of accounts that are specifically targeted by customers.

[9] Compared to other crimes like bank robbery, hackers who spear phish can operate with little risk of being apprehended. Such hackers can operate both openly and anonymously.

Co-Defendant Dokuchaev did not discuss his true identity and motivations with Defendant Baratov.[10] The fact that Defendant Baratov was hired and agreed to hack webmail accounts for an officer of the Russian FSB, however, underscores the need for a significant and strong message of deterrence. First, it corroborates the prolific nature of the defendant's criminal conduct. The defendant was so successful in his hacker-for-hire business that an officer of the Russian FSB enlisted his help to further the Russian FSB's interests. Second, it further corroborates that the defendant hacked thousands of victims indifferently and/or indiscriminately[11] in exchange for money. Such conduct must be deterred. Third, it serves as an example of how the Russian FSB used a cybercriminal as a proxy.[12] These aspects of the defendant's criminal conduct make it even more imperative that there be clear and severe penalties for cybercriminal proxies that are identified, caught, and brought to justice. For cybercriminals like the defendant, there must be a significant sentence of imprisonment that accounts for hacking in such a prolific and indifferent manner that one is hired as a proxy for the Russian FSB. Burying one's head in the ground to the identities, motives, and plans of one's criminal customers should not be a complete shield to the consequences of working for such customers.

For all of these reasons, the United States recommends that the Court impose a sentence within the Sentencing Guidelines range for Count One. The United States agrees with Probation that the low end of the range appears appropriate because the defendant has no criminal history, no prior contact with the criminal justice system, consented to extradition, accepted responsibility quickly, and demonstrated

---

[10] As such, the United States agreed that the Sentencing Guidelines calculation for Defendant Baratov is based on the webmail accounts that he personally hacked, not the criminal conduct of his co-conspirators in hacking Yahoo's computer network. *See id.* ¶ 2.d ("for Sentencing Guidelines purposes, [the defendant's] hacking conduct caused a loss of more than U.S. $3.5 million), ¶¶ 7, 21 (agreeing to +18 loss amount enhancement for Count One).

[11] The alternative explanation, which the parties have agreed is not the case, would be that the defendant discussed the reasons for targeting the victims and affirmatively agreed that the victims that the Russian FSB targeted should be hacked.

[12] Journalists have written about the use of cybercriminals as proxies by governments. *See, e.g.*, Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," Slate, February 2, 2018, *available at* https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html (last visited on April 16, 2018). The use of proxies may, for example, be a method of concealing the nation states that are responsible. *See, e.g.*, Sam Jones, "Cyber crime: states use hackers to do digital dirty work," Financial Times, September 4, 2015, *available at* https://www.ft.com/content/78c46db4-52da-11e5-b029-b9d50a74fd14 (last visited on April 16, 2018) (quoting Admiral Michael Rogers, U.S. Cyber Command chief and director of the National Security Agency, discussing use of surrogates to overcome abilities in attribution).

remorse, which mitigate the needs for specific deterrence and to protect the public from further crimes of this defendant. PSR Sentencing Recommendation, at 2-3. For the same reasons, the United States agrees with Probation that the 24-month consecutive terms for Counts 40 through 47 should run concurrently to one another, pursuant to 18 U.S.C. § 1028A(b)(4).

Therefore, the United States respectfully recommends that the Court impose a sentence of 94 months imprisonment (low end of the Guidelines range for Count One, plus 2 years consecutive for Counts Forty to Forty-Seven).

B. Restitution and Fine

For purposes of restitution, the United States bears the burden of proving by a preponderance of the evidence that a person or entity is a victim and of proving the amount of the loss. *United States v. Andrews*, 600 F.3d 1167, 1171 (9th Cir. 2010). In this case, as summarized in Section II.B above, the United States to date has received responses from three victims. Victim 1 claimed a loss of $50,000, but did not provide a Victim Impact Statement or supporting documentation. Victim 2 did not assert a monetary loss. Victim 3 claimed a consequential business loss of $10,000, but did not provide documentation to support that loss amount. As such, based on the information received to date, the United States does not recommend that the Court impose restitution.

Instead, pursuant to Paragraph 10 of the Plea Agreement, the United States recommends that the Court impose a fine in an amount that encompasses any and all of the defendant's remaining assets, *i.e.*, $30,900 CAD and $1,500 USD. The imposition of such a fine is within the Sentencing Guidelines range for the offense (as stated in Section III.A above, $25,000 to $250,000). Such a fine also ensures that the defendant disgorges any remaining illegal proceeds from his criminal conduct pursuant to 18 U.S.C. § 3572(a)(5) and is sufficient, but not greater than necessary to comply with the purposes of 18 U.S.C. § 3553(a)(2).

C. Supervised Release

As Probation recommends, the sentence of imprisonment should be followed by 3 years of supervised release with an expanded computer search condition. Plea Agreement ¶ 8; PSR Sentencing Recommendation, at 3-4.

V. CONCLUSION

Accordingly, in full consideration of the Sentencing Guidelines and the factors enumerated in 18 U.S.C. § 3553(a), the United States respectfully recommends that the Court impose a sentence of 94 months imprisonment, 3 years supervised release, and restitution and fine amounts that encompass any and all of his assets.

Respectfully submitted,

ALEX G. TSE
Acting United States Attorney

DATED: April 17, 2018

/s/ Jeffrey Shih
JEFFREY SHIH
Assistant United States Attorney

SCOTT K. MCCULLOCH
Trial Attorney, National Security Division