

1 BRIAN J. STRETCH (CABN 163973)
United States Attorney

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

4 JOHN H. HEMANN (CABN 165823)
JEFFREY SHIH (CABN 296945)
5 Assistant United States Attorneys

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

8 450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
9 john.hemann@usdoj.gov; 415.436.7478
jeffrey.shih@usdoj.gov; 415.436.7168

10 Attorneys for United States of America

11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA
13 SAN FRANCISCO DIVISION
14

15 UNITED STATES OF AMERICA,

16 v.

17 KARIM BARATOV,
a/k/a "Kay,"
18 a/k/a "Karim Taloverov,"
a/k/a "Karim Akehmet Tokbergenov."
19 Defendant.
20

) NO. 17-CR-103 VC

) PLEA AGREEMENT

21 I, KARIM BARATOV, a/k/a "Kay," a/k/a "Karim Taloverov," a/k/a "Karim Akehmet
22 Tokbergenov," and the United States Attorney's Office for the Northern District of California (hereafter
23 "the government") enter into this written Plea Agreement (the "Agreement") pursuant to Rule
24 11(c)(1)(A) and 11(c)(1)(B) of the Federal Rules of Criminal Procedure:

25 **The Defendant's Promises**

26 1. I agree to plead guilty to Counts One and Forty through Forty-Seven of the captioned
27 Indictment charging me with conspiracy to commit computer fraud and abuse, in violation of 18 U.S.C.
28 § 1030(b), and aggravated identity theft, in violation of 18 U.S.C. § 1028A.

PLEA AGREEMENT
17-CR-103 VC

FILED

NOV 28 2017

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

1 Count One: Conspiracy to Commit Computer Fraud:

2 I agree that the elements of Count One, which alleges a violation of 18 U.S.C. § 1030(b),
3 are as follows:

- 4 (1) Beginning in or about January 2014, and ending on or about December 1, 2016, I
5 agreed with one or more persons to commit at least one of the computer fraud and
6 abuse crimes as charged in Count One of the indictment, specifically, (a) to
7 intentionally access a protected computer without authorization, in violation of 18
8 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii),¹ or (b) to intentionally damage a
9 protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B);²
10 and
- 11 (2) I became a member of the conspiracy knowing of at least one of its objects and
12 intending to help accomplish it.

13 I agree that the maximum penalties for Count One are as follows:

- 14 a. Maximum prison term 10 years

15 ¹ I agree that the elements of the substantive crime of intentionally accessing a protected
16 computer without authorization, in violation of 18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), are as
17 follows:

- 18 (1) I intentionally accessed without authorization or exceeded authorized access to a computer;
- 19 (2) by accessing without authorization or exceeding authorized access to a computer, I obtained
20 information from a computer that was used in or affected interstate or foreign commerce or
21 communication, or was located outside the United States but was used in a manner that
22 affects interstate or foreign commerce or communication of the United States; and
- 23 (3) the offense was committed for purposes of commercial advantage or private financial gain,
24 the offense was committed in furtherance of any criminal or tortious act in violation of the
25 Constitution or laws of the United States or of any State, including invasion of privacy, or the
26 value of the information obtained did, and would if completed, exceed \$5,000.

27 ² I agree that the elements of the substantive crime of intentionally damaging a protected
28 computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), are as follows:

- 29 (1) I knowingly caused the transmission of a program, a code, a command, or information to a
30 computer;
- 31 (2) as a result of the transmission, I intentionally caused damage, which includes impairing
32 without authorization the integrity or availability of data, a program, a system, or
33 information;
- 34 (3) the computer was used in or affected interstate or foreign commerce or communication, or
35 was located outside the United States but was used in a manner that affects interstate or
36 foreign commerce or communication of the United States; and
- 37 (4) the offense caused, or would if completed have caused, loss aggregating at least \$5,000 in
38 value to at least one person during a one-year period from a related course of conduct
affecting a protected computer, or damage affecting 10 or more protected computers during a
one-year period.

- b. Maximum fine \$250,000, or twice the gross gain or gross loss, whichever is greater
- c. Maximum supervised release term 3 years
- d. Mandatory special assessment \$100
- e. Restitution
- f. Forfeiture
- g. Potential Deportation

Counts Forty Through Forty-Seven: Aggravated Identity Theft:

I agree that the elements of Count Forty through Forty-Seven, each of which alleges a violation of 18 U.S.C. § 1028A, are as follows:

- (1) I knowingly transferred, possessed, and used, without legal authority a means of identification of another person;
- (2) I knew that the means of identification belonged to a real person; and
- (3) I did so during and in relation to the conspiracy to commit computer fraud described in Count One.

I agree that the maximum penalties for each of Counts Forty through Forty-Seven are as follows:

- a. Maximum prison term 2 years
- b. Minimum prison term 2 years
- c. Maximum fine \$250,000, or twice the gross gain or gross loss, whichever is greater
- d. Maximum supervised release term 1 years *ALM KB J.L.*
- e. Mandatory special assessment \$100
- f. Restitution
- g. Forfeiture
- h. Potential Deportation

I acknowledge that pleading guilty may have consequences with respect to my immigration status if I am not a citizen of the United States. Under federal law, a broad range of crimes are removable offenses, including the offense to which I am pleading guilty. Removal and other

1 immigration consequences are the subject of a separate proceeding, however, and I understand that no
2 one, including my attorney or the district court, can predict to a certainty the effect of this conviction on
3 my immigration status. I nevertheless affirm that I want to plead guilty regardless of any immigration
4 consequences that may result from my guilty pleas, even if the consequence is my automatic removal
5 from the United States.

6 I understand that under 18 U.S.C. § 1028A, I am subject to a mandatory consecutive sentence of
7 2 years of imprisonment for that violation in addition to any sentence I may receive for the other
8 violation in Count One to which I am pleading guilty.

9 I understand that I am pleading guilty to multiple violations and that the Court may order that my
10 sentence for each violation run consecutively.

11 2. I agree that I am guilty of the offenses to which I am pleading guilty, and I agree that the
12 following facts are true:

13 a. Beginning in or about January 2014, I knowingly agreed with an individual who I
14 knew at the time as Patrick Nagel or Patrick Nag, who I now agree the government can prove
15 beyond a reasonable doubt was an officer in the Russian Federal Security Service (FSB) actually
16 named Dmitry Dokuchaev and was a hacker who targeted U.S. and other webmail providers
17 (hereinafter, "Dokuchaev"), (i) to access computers without authorization and exceed authorized
18 access to computers, in the Northern District of California and elsewhere, for the purposes of
19 commercial advantage and private financial gain; and (ii) to cause the transmission of programs,
20 information, codes, and commands, in the Northern District of California and elsewhere, and as a
21 result of such conduct, to cause damage without authorization to protected computers. Since in
22 or about 2010, through in or about March 2017, I hacked thousands of private webmail accounts
23 in exchange for money, in the manner described below. Dokuchaev was one of my clients.
24 Specifically, Dokuchaev requested of me, I agreed, and I attempted to hack for Dokuchaev at
25 least 80 webmail accounts in exchange for money.

26 b. I operated my illegal hacking business from my home in and around Ontario,
27 Canada. I advertised my services to Russian language speakers throughout the world and
28 focused on gaining unauthorized access to webmail accounts maintained by Google and Russian

1 webmail providers, including Mail.ru and Yandex. I operated several websites that advertised
2 my services and would collect orders from interested customers. I hosted those advertising
3 websites at servers throughout the world. Interested customers would send me the list of their
4 targeted webmail accounts. Upon receipt of this information, I would attempt to gain
5 unauthorized access to those accounts.

6 c. I spear phished my victims to harvest their passwords. As part of my spear
7 phishing efforts, I created emails that appeared to be from the corresponding webmail provider,
8 often by creating email addresses that used the webmail provider's name and "support" or other
9 such terms in them to make them appear as trustworthy customer support e-mails. I would then
10 send the victim a spear phishing email that contained a link to a "spoofed" website that I
11 constructed to mimic the appearance of a log-in page of the same webmail provider from which
12 the spear phishing email purported to originate. I hosted my spoofed websites on servers
13 throughout the world. When victims clicked on the link, they would view the spoofed website in
14 their web browser, and be asked to enter the password to their webmail account. When victims
15 did so, scripts in those spoofed websites would then send the stolen password information to me
16 at various webmail accounts that I maintained at providers located throughout the world.

17 d. After successfully stealing a victim's password, I personally used the password to
18 access the contents of the victim's webmail account and to take a screen shot of the account
19 contents, which I used as proof to demand payment from my customers. After I received
20 payment, I sent the victim's stolen password to the customer. When I sold these stolen
21 passwords to my customers, such as Dokuchaev, I knew that the customer would have full access
22 to the personal communications and information contained in those victim accounts. I hacked
23 the webmail accounts of more than 11,000 victims in the manner described in paragraphs 2.c and
24 2.d. I agree that, for Sentencing Guidelines purposes, my hacking conduct caused a loss of more
25 than U.S. \$3.5 million.

26 e. For each successful hack, I received approximately \$100. I accepted payment
27 from my customers, such as Dokuchaev, through various U.S. or foreign online payment
28 services, including PayPal and WebMoney. The proceeds that I received from this criminal

1 hacking activity, and the assets that I purchased with or derived from those proceeds, constituted
2 (and has been at all times) my only source of income. I agree that in relation to my purchase of
3 assets in the names of other people, including my parents, I did not represent to those other
4 people that I held legitimate, non-criminal employment or other, non-criminal sources of funds
5 that could have paid for those assets.

6 f. I agree that the government can prove beyond a reasonable doubt that the
7 conspiracy I joined described in Count One caused damage to more than 10 computers, caused
8 greater than \$5,000.00 in damages within a single year, and caused the unauthorized access of
9 information the value of which exceeded \$5,000.00.

10 g. From on or about December 26, 2014, through on or about March 25, 2016, I
11 successfully hacked the accounts listed in Counts Forty through Forty-Seven of the Indictment.
12 For each of those accounts, I accessed the account contents, sent Dokuchaev the associated
13 passwords, and received payment. I knew that each of the accounts was maintained by a real
14 person, I did not have the permission of those people to access the accounts, and I agreed with
15 Dokuchaev to steal the passwords for, and to hack into, the accounts.

16 h. Additionally, in hacking webmail accounts for other clients (*i.e.*, not Dokuchaev),
17 at times I personally deleted the contents of victims' webmail accounts and changed the
18 password of accounts. At other times, I also gained unauthorized access to victims' webmail
19 accounts, for which I had previously stolen passwords, and used those accounts to conceal my
20 true identity while hacking the webmail accounts of other victims.

21 i. I did not discuss with Dokuchaev, or his fellow FSB officer Igor Sushchin, their
22 reasons for targeting our victims. Likewise, I did not discuss with Dokuchaev or my other co-
23 conspirators their conduct in hacking into Yahoo. However, I agree that the government could
24 prove beyond a reasonable doubt that some of those targets whose accounts that I hacked were of
25 interest to Russian intelligence and were identified by my co-conspirators as a result of their
26 hack of Yahoo.

27 3. I agree to give up all rights that I would have if I chose to proceed to trial, including the
28 rights to a jury trial with the assistance of an attorney; to confront and cross-examine government

1 witnesses; to remain silent or testify; to move to suppress evidence or raise any other Fourth or Fifth
2 Amendment claims; to any further discovery from the government; and to pursue any affirmative
3 defenses and present evidence.

4 4. I agree to give up my right to appeal my conviction, the judgment, and orders of the
5 Court, as well as any aspect of my sentence, including any orders relating to forfeiture and/or restitution,
6 except that I reserve my right to claim that my counsel was ineffective.

7 5. I agree not to file any collateral attack on my conviction or sentence, including a petition
8 under 28 U.S.C. § 2255 or 28 U.S.C. § 2241, except that I reserve my right to claim that my counsel was
9 ineffective. I also agree not to seek relief under 18 U.S.C. § 3582.

10 6. I agree not to ask the Court to withdraw my guilty pleas at any time after they are
11 entered. I understand that by entering into this Agreement: (a) I agree that the facts set forth in
12 Paragraph 2 of this Agreement shall be admissible against me under Fed. R. Evid. 801(d)(2)(A) in any
13 subsequent proceeding, including at trial, in the event I violate any of the terms of this Agreement, and
14 (b) I expressly waive any and all rights under Fed. R. Crim. P. 11(f) and Fed. R. Evid. 410 with regard to
15 the facts set forth in Paragraph 2 of this Agreement in such subsequent proceeding. I understand that the
16 government will not preserve any physical evidence obtained in this case.

17 7. I understand that the Court must consult the United States Sentencing Guidelines and
18 take them into account when sentencing, together with the factors set forth in 18 U.S.C. § 3553(a). I
19 also understand that the Court is not bound by the Guidelines calculations below; the Court may
20 conclude that a higher Guidelines range applies to me, and, if it does, I will not be entitled, nor will I ask
21 to withdraw my guilty pleas. I further agree that regardless of the sentence that the Court imposes on
22 me, I will not be entitled, nor will I ask, to withdraw my guilty pleas. I agree that the Sentencing
23 Guidelines offense level should be calculated as set forth below, and that I will not request a downward
24 departure under the Sentencing Guidelines from that offense level although I reserve the right to seek a
25 downward variance based on the factors set forth in 18 U.S.C. § 3553(a). I understand that the
26 government is free to oppose any such request. The parties have reached no agreement regarding my
27 Criminal History Category.

Count One: Conspiracy to Commit Computer Fraud:

a.	Base Offense Level U.S.S.G. §2B1.1(a)(2)	6
b.	Loss more than \$3.5 million USSG § 2B1.1(b)(1)(P)	+18
c.	10 or more victims USSG § 2B1.1(b)(2)(A)	+2
d.	Sophisticated means USSG § 2B1.1(b)(10)	+2
e.	Offense under § 1030 to obtain personal information USSG § 2B1.1(b)(17)(A)	+2
f.	Acceptance of Responsibility USSG § 3E1.1 (If I meet the requirements of U.S.S.G. § 3E1.1, I may be entitled to a three-level reduction for acceptance of responsibility, provided that I forthrightly admit my guilt, cooperate with the Court and the Probation Office in any presentence investigation ordered by the Court, and continue to manifest an acceptance of responsibility through and including the time of sentencing.)	- 3
g.	Adjusted Offense Level	27

Counts Forty Through Forty-Seven: Aggravated Identity Theft: +2 years consecutive

8. I agree that regardless of any other provision of this Agreement, the government may and will provide the Court and the Probation Office with all information relevant to the charged offenses and the sentencing decision. I agree that, based on the nature of the offenses, the Court should impose the following special condition of supervised release, which is reasonably related to deterrence and rehabilitation:

Special Condition (Searches)

The defendant shall submit his person, residence, office, vehicle, electronic devices and their data (including cell phones, computers, and electronic storage media), and any property under defendant's control to a search. Such a search shall be conducted by a United States Probation Officer or any federal, state, or local law enforcement officer at any time, with or without suspicion. Failure to submit to such a search may be grounds for revocation; the defendant shall warn any residents that the premises may be subject to searches.

9. I agree to pay full restitution for all losses caused by all the schemes or offenses with which I was charged in this case, and I understand that the amount of restitution will not be limited to

1 the loss attributable to the Counts to which I am pleading guilty, pursuant to 18 U.S.C. § 3663(a)(3), and
2 will include losses suffered by the owners of the more than 11,000 email accounts I hacked. I
3 understand that the Court will not consider my economic circumstances in determining the restitution
4 amount. I agree to pay restitution in an amount to be set by the Court at the time of sentencing or at
5 hearing held in accordance with 18 U.S.C. § 3664(d)(5) and § 3771(d)(2).

6 10. Additionally, I agree to pay a fine in an amount, up to the combined statutory maximum
7 for Counts One and Forty through Forty-Seven (i.e., \$2,250,000), that includes any and all assets I have
8 that are not applied to restitution. I agree that the assets I have that are not applied to restitution shall be
9 applied to this fine, for which I further agree an upward variance is reasonable and appropriate under 18
10 U.S.C. § 3572(a), including but not limited to § 3572(a)(5) (i.e., the need to deprive the defendant of
11 illegally obtained gains from the offense).

12 11. Any restitution and fine payments shall be paid through the Office of the Clerk of the
13 District Court by bank or cashier's check or money order made payable to the "Clerk, United States
14 District Court." I understand that the restitution and fine payments described above create liens in favor
15 of the United States on all property and rights to property I may possess upon entry of judgment and
16 continues for 20 years or until the debt is paid in full. I further understand the government will record a
17 notice of the lien in any county where I reside or have property. I further understand that this order of
18 restitution and imposition of a fine cannot be discharged in bankruptcy and that if I default on the
19 payment of a fine or restitution, the Court may revoke probation or a term of supervised release, modify
20 the terms or conditions of probation or supervised release, resentence me, hold me in contempt of court,
21 order the sale of property, enter or adjust a payment schedule, or take any other action necessary to
22 obtain compliance.

23 12. Within thirty days of the execution of this Plea Agreement, I agree to complete, under
24 penalty of perjury, a financial statement provided by the U.S. Attorney's Office and to update that
25 statement with material changes within seven days of the change. I understand that I must identify all
26 assets and financial interests valued at more than \$1,000. I further understand that these assets and
27 financial interests include all assets and financial interests in which I have an interest, direct or indirect,
28 whether held in my own name or in the name of another, in any property, real or personal. Furthermore,

1 I agree to be deposed under oath within forty-five days of the execution of this Plea Agreement, by the
 2 U.S. Attorney's Office, about my assets, financial interests, and information provided in the financial
 3 statement provided to the U.S. Attorney's Office.

4 13. I agree to surrender assets I obtained as a result of my crimes, and to release and
 5 repatriate all foreign assets, funds and property under my control in order to pay any fine, forfeiture, or
 6 restitution, including but not limited to any and all interests in the following property:

- 7 a. all funds held on deposit in PayPal account number ending in 9844, held in the
- 8 name of "Elite Space Corporation" (the "Funds");
- 9 b. a grey Aston martin DBS, license plate identification "MR KARIM";
- 10 c. a black Mercedes Benz C-class, license plate identification "CAWE693";
- 11 d. all funds held in two Royal Bank of Canada checking accounts, ending in -1239
- 12 and -8882, held in the name Karim Baratov;
- 13 e. all funds held in Canadian Imperial Bank of Commerce checking account, ending
- 14 in -0035, held in the name Elite Space Corporation; and
- 15 f. all funds held in Webmoney accounts R277827924712; Z347354582559;
- 16 U296267290477; E361460411410; R730506335350; Z218688555965;
- U428190136698; E385447301479; R362076697446; Z218225309180;
- U407455865587; E287422735598; R205445595879; Z196527417386;
- U353393352355; and E200629168489.

17 I further agree to notify the Financial Litigation Unit, United States Attorney's Office ("FLU") before
 18 transferring any interest in property owned directly or indirectly by me, including any interest held or
 19 owned under any other name or entity, including trusts, partnerships, and/or corporations. I also agree to
 20 notify the FLU of any interest in property valued at more than \$1,000 that I may obtain, directly or
 21 indirectly, including any interest obtained under any other name, or entity, including a trust, partnership,
 22 or corporation, after the execution of this Plea Agreement until the fine or restitution is paid in full.

23 14. I agree that any fine, forfeiture, or restitution imposed by the Court against me will be
 24 due immediately and subject to immediate enforcement by the government as authorized by 18 U.S.C.
 25 § 3613. I further understand that the government may seek immediate collection of the entire fine,
 26 forfeiture, or restitution from any assets without regard to any schedule of payments imposed by the
 27 Court or established by the Probation Office and that monetary penalties imposed by the Court will be
 28

1 submitted to the Treasury Offset Program so that any federal payment or transfer of returned property I
2 receive may be offset and applied to federal debts.

3 15. I agree not to commit or attempt to commit any crimes before sentence is imposed or
4 before I surrender to serve my sentence. I also agree not to violate the terms of my pretrial release; not
5 to intentionally provide false information to the Court, the Probation Office, Pretrial Services, or the
6 government; and not to fail to comply with any of the other promises I have made in this Agreement. I
7 agree that if I fail to comply with any promises I have made in this Agreement, then the government will
8 be released from all of its promises in this Agreement, including those set forth in the Government's
9 Promises Section below, but I will not be released from my guilty pleas.

10 16. I agree to remain remanded to the custody of the United States Marshal upon entry of my
11 guilty pleas pursuant to 18 U.S.C. § 3143(a)(2).

12 17. I agree that this Agreement contains all of the promises and agreements between the
13 government and me, and I will not claim otherwise in the future. No modification of this Agreement
14 shall be effective unless it is in writing and signed by all parties.

15 18. I agree that the Agreement binds the U.S. Attorney's Office for the Northern District of
16 California only, and does not bind any other federal, state, or local agency.

17 **The Government's Promises**

18 19. The government agrees to move to dismiss any open charges pending against the
19 defendant in the captioned Indictment at the time of sentencing.

20 20. The government agrees not to file any additional charges against the defendant that could
21 be filed as a result of the investigation that led to the captioned Indictment.

22 21. Unless the defendant violates the terms of the Agreement above or fails to accept
23 responsibility, the government agrees to recommend a sentence as set out in paragraph 7 above,
24 specifically, within the range associated with the Guideline calculations for Count One plus two years
25 consecutive for the combination of Counts Forty through Forty-Seven (i.e., the government agrees to
26 recommend that Counts Forty through Forty-Seven run concurrently with one another pursuant to 18
27 U.S.C. § 1028A(b)(4)).
28

1 The Defendant's Affirmations

2 22. I agree that my participation in the District Court's Conviction Alternative Program is not
3 appropriate and that I will not request to be considered for and will not participate in that program as a
4 result of my convictions for these offenses.

5 23. I confirm that I have had adequate time to discuss this case, the evidence, and the
6 Agreement with my attorney and that my attorney has provided me with all the legal advice that I
7 requested.

8 24. I confirm that while I considered signing this Agreement, and at the time I signed it, I
9 was not under the influence of any alcohol, drug, or medicine that would impair my ability to understand
10 the Agreement.

11 25. I confirm that my decision to enter guilty pleas is made knowing the charges that have
12 been brought against me, any possible defense, and the benefits and possible detriments of proceeding to
13 trial. I also confirm that my decision to plead guilty is made voluntarily, and no one coerced or
14 threatened me to enter into this Agreement.

15
16 Dated: 11/28/2017


KARIM BARATOV
Defendant


BRIAN J. STRETCH
United States Attorney

17
18
19
20
21 Dated: 11/28/2017


JEFFREY SHIH
JOHN H. HEMANN
Assistant United States Attorneys

1 26. I have fully explained to my client all the rights that a criminal defendant has and all the
2 terms of this Agreement. In my opinion, my client understands all the terms of this Agreement and all
3 the rights my client is giving up by pleading guilty, and, based on the information now known to me, my
4 client's decision to plead guilty is knowing and voluntary.

5
6 Dated: 11/28/17



ANDREW MANCILLA
Attorney for Defendant

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28