Chief Judge Ricardo S. Martinez

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. ANDRII KOLPAKOV, Defendant.	NO. CR18-159RSM **PLEA AGREEMENT**

The United States of America, by and through undersigned counsel, and Defendant ANDRII KOLPAKOV, and his attorney, Vadim A. Glozman, enter into the following Agreement, pursuant to Federal Rule of Criminal Procedure 11(c)(1)(A) and (B):

1. **Charges**. Defendant, having been advised of the right to have this matter tried before a jury, agrees to waive that right and enters a plea of guilty to the following charges contained in the Indictment:

a. Conspiracy to Commit Wire Fraud, as charged in Count 1, in violation of Title 18, United States Code, Section 1349.

b. Conspiracy to Commit Computer Hacking, as charged in Count 16, in violation of Title 18, United States Code, Section 371.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

By entering these pleas of guilty, Defendant hereby waives all objections to the form of the charging document. Defendant further understands that before entering his guilty pleas, he will be placed under oath. Any statement given by Defendant under oath may be used by the United States in a prosecution for perjury or false statement.

The United States agrees to seek dismissal of Counts 2 to 15, and 17 to 26 at the time of sentencing.

2. **Elements of Offenses**. The elements of the offenses to which Defendant is pleading guilty are as follows:

a. The elements of Conspiracy to Commit Wire Fraud, as charged in Count 1, in violation of Title 18, United States Code, Section 1349, are as follows:

First, two or more persons, in some way or manner, agreed to try to accomplish a common and unlawful plan to commit a fraud crime listed in Title 18 Chapter 63, as charged in the indictment, namely, Wire Fraud, in violation of Title 18, United States Code, Section 1343; and

Second, the defendant knew the unlawful purpose of the plan and willfully joined in it.

The elements of Wire Fraud, are as follows:

First, the defendant knowingly participated in a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or omitted facts;

Second, the statements made or facts omitted as part of the scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;

Third, the defendant acted with the intent to defraud, that is, the intent to deceive or cheat; and

Fourth, the defendant used, or caused to be used, an interstate or foreign wire communication to carry out or attempt to carry out an essential part of the scheme.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. The elements of Conspiracy to Commit Computer Hacking, as charged in Count 16, in violation of Title 18, United States Code, Section 371, are as follows:

First, there was an agreement between two or more persons to commit at least one crime as charged in the indictment, namely, Accessing a Protected Computer in Furtherance of Fraud, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A); and, Intentional Damage To a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i);

Second, the defendant became a member of the conspiracy knowing of at least one of its objects and intending to help accomplish it; and

Third, one of the members of the conspiracy performed at least one overt act for the purpose of carrying out the conspiracy.

The elements of Accessing a Protected Computer in Furtherance of Fraud, are as follows:

First, the defendant knowingly accessed without authorization, or exceeded authorized access to, a computer used in or affecting interstate or foreign commerce or communication, or located outside the United States but using it in a manner that affected interstate or foreign commerce or communication of the United States;

Second, the defendant did so with the intent to defraud;

Third, by accessing the computer without authorization, or exceeding authorized access to the computer, the defendant furthered the intended fraud; and,

Fourth, the defendant by accessing the computer without authorization, or exceeding authorized access to the computer, obtained anything of value.

The elements of Intentional Damage to a Protected Computer, are as follows:

First, the defendant knowingly caused the transmission of a program, a code, a command, or information to a computer;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Second, as a result of the transmission, the defendant intentionally impaired without authorization the integrity or availability of data, a program, a system, or information;

Third, the computer was used in or affected interstate or foreign commerce or communication, or located outside the United States but was used in a manner that affects interstate or foreign commerce or communication of the United States; and,

Fourth, the offense caused (i) loss to one or more persons during a 1-year period aggregating at least $5,000.00 in value, or (ii) damage affecting 10 or more protected computers during a 1-year period.

3. **The Penalties**. Defendant understands that the statutory penalties applicable to the Offenses to which he is pleading guilty are as follows:

a. For the offense of Conspiracy to Commit Wire Fraud, as charged in Count 1: A maximum term of imprisonment of up to twenty (20) years, a fine of up to $250,000.00, a period of supervision following release from prison of up to three (3) years, and a mandatory special assessment of one hundred dollars ($100).

b. For the offense of Conspiracy to Commit Computer Hacking, as charged in Count 16: A maximum term of imprisonment of up to five (5) years, a fine of up to $250,000.00, a period of supervision following release from prison of up to three (3) years, and a mandatory special assessment of one hundred dollars ($100).

If a probationary sentence is imposed, the probation period can be for up to five (5) years. Defendant agrees that the special assessment shall be paid at or before the time of sentencing.

Defendant understands that supervised release is a period following imprisonment during which he will be subject to certain restrictive conditions and requirements. Defendant further understands that if supervised release is imposed and he violates one or more of the conditions or requirements, Defendant could be returned to prison for all or part of the term of supervised release that was originally imposed. This could result in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Defendant's serving a total term of imprisonment greater than the statutory maximum stated above.

Defendant understands that as a part of any sentence, in addition to any term of imprisonment and/or fine that is imposed, the Court may order Defendant to pay restitution to any victim of the offense, as required by law.

Defendant further understands that a consequence of pleading guilty may include the forfeiture of certain property either as a part of the sentence imposed by the Court, or as a result of civil judicial or administrative process.

Defendant agrees that any monetary penalty the Court imposes, including the special assessment, fine, costs, or restitution, is due and payable immediately and further agrees to submit a completed Financial Statement of Debtor form as requested by the United States Attorney's Office.

4. **Immigration Consequences**. Defendant recognizes that pleading guilty may have consequences with respect to Defendant's immigration status if Defendant is not a citizen of the United States. Under federal law, a broad range of crimes are grounds for removal, and some offenses make removal from the United States presumptively mandatory. Removal and other immigration consequences are the subject of a separate proceeding, and Defendant understands that no one, including Defendant's attorney and the Court, can predict with certainty the effect of a guilty plea on immigration status. Defendant nevertheless affirms that Defendant wants to plead guilty regardless of any immigration consequences that Defendant's guilty pleas may entail, even if the consequence is Defendant's mandatory removal from the United States.

5. **Rights Waived by Pleading Guilty.** Defendant understands that by pleading guilty, he knowingly and voluntarily waives the following rights:

a. The right to plead not guilty and to persist in a plea of not guilty;

b. The right to a speedy and public trial before a jury of his peers;

c. The right to the effective assistance of counsel at trial, including, if Defendant could not afford an attorney, the right to have the Court appoint one for him;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. The right to be presumed innocent until guilt has been established beyond a reasonable doubt at trial;

e. The right to confront and cross-examine witnesses against Defendant at trial;

f. The right to compel or subpoena witnesses to appear on his behalf at trial;

g. The right to testify or to remain silent at trial, at which trial such silence could not be used against Defendant; and

h. The right to appeal a finding of guilt or any pretrial rulings.

6. **United States Sentencing Guidelines**. Defendant understands and acknowledges that the Court must consider the sentencing range calculated under the United States Sentencing Guidelines and possible departures under the Sentencing Guidelines together with the other factors set forth in Title 18, United States Code, Section 3553(a), including: (1) the nature and circumstances of the offenses; (2) the history and characteristics of Defendant; (3) the need for the sentence to reflect the seriousness of the offenses, to promote respect for the law, and to provide just punishment for the offenses; (4) the need for the sentence to afford adequate deterrence to criminal conduct; (5) the need for the sentence to protect the public from further crimes of Defendant; (6) the need to provide Defendant with educational and vocational training, medical care, or other correctional treatment in the most effective manner; (7) the kinds of sentences available; (8) the need to provide restitution to victims; and (9) the need to avoid unwarranted sentence disparity among defendants involved in similar conduct who have similar records. Accordingly, Defendant understands and acknowledges that:

a. The Court will determine Defendant's Sentencing Guidelines range at the time of sentencing;

b. After consideration of the Sentencing Guidelines and the factors in 18 U.S.C. 3553(a), the Court may impose any sentence authorized by law, up to the maximum term authorized by law;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. The Court is not bound by any recommendation regarding the sentence to be imposed, or by any calculation or estimation of the Sentencing Guidelines range offered by the parties or the United States Probation Department, or by any stipulations or agreements between the parties in this Plea Agreement; and

d. Defendant may not withdraw a guilty plea solely because of the sentence imposed by the Court.

7. **Ultimate Sentence**. Defendant acknowledges that no one has promised or guaranteed what sentence the Court will impose.

8. **Restitution.** The parties agree that they will recommend that the Court apportion liability for restitution owed to all victims of the criminal conduct committed by the criminal organization charged in the conspiracies described herein, including the fraud loss on card issuers, financial institutions, breached victim companies, insurance companies, cardholders, and vendor businesses. Defendant agrees to pay restitution in the apportioned amount of $2,500,000.00 (which shall not be joint and several with any other FIN7 defendant). Said amount shall be due and payable immediately and shall be paid in accordance with a schedule of payments as proposed by the United States Probation Office and ordered by the Court.

9. **Forfeiture of Assets**. Defendant agrees, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), to forfeit to the United States, immediately, all of his right, title, and interest in any and all property, real or personal, which constitutes or is derived from proceeds traceable to the offense set forth in Count 1 of the Indictment, including but not limited to a sum of money representing, in part, the proceeds that Defendant obtained as a result of the offense set forth in Count 1.

Defendant understands and acknowledges that the sum of money the United States seeks to forfeit is separate and distinct from the restitution that is ordered in this case.

Defendant further agrees, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), to forfeit to the United States, immediately, all of his right,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

title, and interest in any and all property constituting, or derived from, proceeds Defendant obtained, directly or indirectly, as the result of the offense set forth in Count 16 of the Indictment, and further to forfeit Defendant's interest in any personal property that was used, or intended to be used, to commit, or to facilitate the commission of, that offense, including but not limited to the following:

a. Asus laptop, model no. X510U (serial no. HANOCX24R525436);

b. Toshiba 128 GB SSD (serial no. 671510BATMXT);

c. SATA hard drive (serial no. 87VEC1G9T SWF HDKCB8888E0A01T);

d. Gold colored Samsung SM J500H Galaxy J5 cell phone (serial no. RV1H40M03WV, IMEI 357950071755024/01 and 35800071755027/0); and

e. Various SIM cards.

Defendant agrees to fully assist the United States in the forfeiture of the above-described property and to take whatever steps are necessary to pass clear title to the United States, including but not limited to: surrendering title and executing any documents necessary to effectuate such forfeiture; assisting in bringing any assets located outside the United States within the jurisdiction of the United States; and taking whatever steps are necessary to ensure that assets subject to forfeiture are not sold, disbursed, wasted, hidden, or otherwise made unavailable for forfeiture. Defendant agrees not to file a claim to any of the above-described property in any federal forfeiture proceeding, administrative or judicial, which may be or has been initiated.

The United States reserves its right to proceed against any remaining property not identified in this Plea Agreement, including any property in or over which Defendant has any interest or control, if that property is subject to forfeiture under any federal statute.

10. **Abandonment of Contraband/Property**. Defendant agrees that if any federal law enforcement agency seized any firearms, ammunition, firearm accessories, or contraband that were in Defendant's direct or indirect control, Defendant abandons any and all interest in those assets and consents to their federal administrative disposal,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

official use, and/or destruction by the federal law enforcement agency that seized them. Defendant further agrees to abandon his interest in, and consents to the destruction of, the following electronic devices and any data contained within:

a. Asus laptop, model no. X510U (serial no. HANOCX24R525436);

b. Toshiba 128 GB SSD (serial no. 671510BATMXT);

c. SATA hard drive (serial no. 87VEC1G9T SWF HDKCB8888E0A01T);

d. Gold colored Samsung SM J500H Galaxy J5 cell phone (serial no. RV1H40M03WV, IMEI 357950071755024/01 and 35800071755027/0); and

e. Various SIM cards.

11. **Statement of Facts**. The parties agree on the following facts. Defendant admits he is guilty of the charged offense or offenses:

a. Defendant Andrii Kolpakov is a Ukrainian national and has used various aliases and nicknames, including, but not limited to "Andrey Kolpakov," "Andriy Kolpakov," "Andre Kolpakov," "Andrew Kolpakov," as well as "santisimo," "santisimoz," and "AndreyKS." As discussed below, Defendant Kolpakov, while residing in Ukraine, was a member of a sophisticated foreign-based hacking operation that targeted victims in the United States and elsewhere.

b. From approximately at least April 2016 to his arrest on June 28, 2018, Defendant was a member of a financially-motivated hacking group commonly referred to as "FIN7." Beginning at a time unknown, but no later than August 2015, and continuing through Defendant's arrest, FIN7 launched attacks against hundreds of U.S. companies in an effort to breach the network security of those victims and to steal financial information and non-public information. FIN7 consists of dozens of experienced computer specialists located in multiple countries. As discussed below, Defendant knowingly and intentionally entered into an agreement with other members of FIN7 to gain unauthorized access to protected computers and servers of hundreds of protected computer networks

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

located in the Western District of Washington, and elsewhere in the United States, with the goal of stealing financial information that could then be sold for financial gain.

c. One of FIN7's primary objectives was to steal payment card information from victim companies. FIN7 stole information for tens of millions of payment cards from U.S. companies, and then offered that stolen information for sale, including for sale on underground forums such as Joker Stash. That payment card information typically included the payment card number, the name of the payment cardholder, and the zip code in which the card was used, among other data. FIN7 members understood that the stolen payment card data would be used to conduct fraudulent transactions across the United States and in foreign countries.

d. FIN7 used a front company called Combi Security to recruit hackers and to provide a veil of legitimacy to the illegal enterprise. Combi Security portrayed itself as a legitimate computer security company that provided penetration-testing services to a variety of companies around the world. On its public website, Combi Security presented itself as "one of the leading international companies in the field of information security." In truth and fact, Combi Security carried out no legitimate work, and was not hired by any company to provide security-related services.

e. FIN7 carried out its attacks primarily through the use of phishing emails and the use of social engineering techniques to encourage the recipients of the phishing emails to inadvertently activate malware contained in or attached to the emails. Once activated, the malware would connect a compromised victim computer to a network of command and control servers located around the world. Through its command and control infrastructure, FIN7 would upload additional malware onto victim computers, conduct surveillance, and otherwise maintain remote control of victim computers. After breaching a particular victim's computer, FIN7 would use that computer to establish a foothold in the victim's network, and then move laterally through the network to locate sensitive financial information, such as payment card information, that could be stolen and monetized.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Among other targets, FIN7 sought to locate point-of-sale ("POS") systems through which it could remotely upload malware onto POS terminals that were used to process payment card transactions at thousands of retail and commercial locations across the United States. FIN7 then used the malware to scrape and exfiltrate the payment card information. In doing so, FIN7 caused to be transmitted in interstate and foreign commerce, numerous wire communications and electronic commands, including communications and commands to POS terminals located in the Western District of Washington.

g. Defendant Kolpakov served as a high-level hacker, whom the group referred to as a "pentester," and was directly involved in breaching the networks of numerous prominent U.S. businesses. Defendant Kolpakov also managed other hackers tasked with breaching the security of victims' computer systems. For instance, on or about January 12, 2017, a FIN7 member introduced himself to a new FIN7 recruit and indicated that Kolpakov would be his supervisor.

h. One means of private communication used by FIN7 members is Jabber. Jabber is an instant messaging service that allows members to communicate through a privately hosted server. Defendant Kolpakov and his various co-conspirators used Jabber to coordinate hacking efforts. For instance, among the numerous Jabber communications made in furtherance of the conspiracy:

i. On or about May 29, 2017, Defendant Kolpakov informed co-conspirator Dmytro Fedorov that he had successfully located POS terminals and accounting technology on a particular victim company's network.

ii. On or about September 18, 2017, Defendant Kolpakov and Dmytro Fedorov discussed the file types used in phishing emails, and Defendant Kolpakov informed Fedorov of the development of an enhanced malware file that is activated without being double-clicked upon by the phishing email recipient.

i. FIN7 conspirators, including Defendant Kolpakov, frequently used the project management software JIRA, hosted on private virtual servers in various countries,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to coordinate their malicious activity and to manage the assorted network intrusions. JIRA is a project management and issue-tracking program used by software development teams. JIRA allows team members to create "projects" containing posted "issues" under which other team members can make comments and share data. Under each issue, FIN7 members would track their progress breaching the victim's security, upload data stolen from the victim, and provide guidance to each other. As but one example:

i. On or about September 7, 2016, co-conspirator Fedir Hladyr created a JIRA "issue" for Jason's Deli ("Victim-6"), a U.S.-based casual delicatessen restaurant chain with hundreds of locations. The same date, and on several days following, Defendant Kolpakov uploaded comments to the issue containing information stolen from Victim-6, such as IP addresses, a list of computers within Victim-6's internal network, account information, and usernames, passwords, computer names.

ii. On or about December 21, 2017, a large cache of payment card information stolen from Victim-6 were offered for sale through an underground vending site called Joker's Stash.

j. While Defendant was working for FIN7, a number of companies publicly reported that they had suffered data breaches involving the theft of payment card information that were later attributed to FIN7. For example, Chipotle (Victim-3) publicly disclosed a data breach that impacted approximately 3.9 million payment cards, and Jason's Deli (Victim-6) publicly disclosed a data breach that impacted approximately 2 million payment cards. Moreover, FIN7 members, including Kolpakov, were aware of reported arrests of other FIN7 members, including Hladyr and Fedorov, but nevertheless continued to attack U.S. businesses.

k. During the course of the scheme, Defendant received compensation for his participation in FIN7, which far exceeds comparable legitimate employment in Ukraine. For the purposes of this plea agreement, the parties agree that – during Defendant's participation in the malware scheme – FIN7 illegal activity resulted in over $100 million in losses to financial institutions, merchant processers, insurance companies, retail

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

companies, and individual cardholders. These losses included, *inter alia*, costs associated with fraudulent purchases made with the stolen payment card information, replacing compromised payment cards, removing FIN7's malware from compromised systems, and responding to law enforcement requests for information in connection with this prosecution. In addition, FIN7 caused loss to 10 or more victim companies by breaching the victim companies' network security that far exceed $5,000 in each year from 2015 to 2018.

l. On about June 28, 2018, Defendant was arrested by Spanish police in Lepe, Spain. At the time, he was in possession of electronic devices, including an Asus laptop computer (with hard drives), storage devices, and a mobile phone, described in paragraph 9, above, which were used to facilitate the scheme. For instance, on those devices, Defendant knowingly possessed, among other things, multiple thousands of payment card numbers and employee credential information stolen from various U.S. victim companies through the aforementioned hacking activity on behalf of the FIN7 hacking group. Upon Defendant's arrest by Spanish police, Defendant's travel companion sent a message to another FIN7 member also traveling in Spain to advise of the arrest.

The parties further agree that the Court may consider additional facts contained in the Presentence Report (subject to standard objections by the parties) and/or that may be presented by the United States or Defendant at the time of sentencing, and that the factual statement contained herein is not intended to limit the facts that the parties may present to the Court at the time of sentencing.

12. **Sentencing Factors**. The parties agree that the following United States Sentencing Guidelines ("USSG") provisions apply to this case:

a. A base offense level of 6, pursuant to USSG § 2B1.1(a)(2).

b. An offense level enhancement of 30 levels (+30), based on a loss amount of more than $550,000,000, pursuant to USSG § 2B1.1(b)(1)(P). For the purposes of this plea agreement, the parties agree to limit the number of stolen payment cards to 20 million, which represents the approximate number of unique card numbers

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

recovered to date. Pursuant to Application Note 3(F)(i), a $500 loss amount is imputed to each payment card, resulting in a total loss amount, for Guidelines purposes, of $10 billion.

c. An offense level enhancement of 2 levels (+2), because the offense involved more than 10 victims, pursuant to USSG § 2B1.1(b)(2)(A).

d. An offense level enhancement of 2 levels (+2), because the offense involved receiving stolen property, and the defendant was a person in the business of receiving and selling stolen property, pursuant to USSG § 2B1.1(b)(4).

e. An offense level enhancement of 2 levels (+2), because a substantial part of the fraudulent scheme was committed from outside the United States and because the offense involved sophisticated means and the defendant intentionally engaged in and caused the conduct constituting sophisticated means, pursuant to USSG § 2B1.1(b)(10).

f. An offense level enhancement of 2 levels (+2), because the offense involved the trafficking in unauthorized access devices and counterfeit access devices and because the offense involved the possession of more than 5 means of identification that were unlawfully obtained, pursuant to USSG § 2B1.1(b)(11).

g. An offense level enhancement of 3 levels (+3), because the defendant was a manager (but not an organizer or leader) and the criminal activity involved more than five participants and was extensive, pursuant to USSG § 3B1.1(b).

h. An offense level reduction for acceptance of responsibility, as set forth in paragraph 12, below, conditioned upon Defendant's fulfillment of the requirements stated at USSG § 3E1.1.

i. Defendant's Guidelines range is 25 years, because the statutory authorized sentence is less than the minimum of the applicable Guidelines range, pursuant to USSG § 5G1.1.

The parties agree they are free to present arguments regarding the applicability of all other provisions of the United States Sentencing Guidelines. Defendant understands, however, that at the time of sentencing, the Court is free to reject these stipulated

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

adjustments, and is further free to apply additional downward or upward adjustments in determining Defendant's Sentencing Guidelines range.

13. **Acceptance of Responsibility.** At sentencing, *if* the district court concludes Defendant qualifies for a downward adjustment for acceptance of responsibility pursuant to USSG § 3E1.1(a) and the defendant's offense level is 16 or greater, the United States will make the motion necessary to permit the district court to decrease the total offense level by three (3) levels pursuant to USSG §§ 3E1.1(a) and (b), because Defendant has assisted the United States by timely notifying the United States of his intention to plead guilty, thereby permitting the United States to avoid preparing for trial and permitting the Court to allocate its resources efficiently.

14. **Non-Prosecution of Additional Offenses**. As part of this Plea Agreement, the United States Attorney's Office for the Western District of Washington and the Computer Crime and Intellectual Property Section of the United States Department of Justice agree to dismiss other pending counts at the time of sentencing and agree not to prosecute Defendant for any additional offenses known to it as of the time of this Agreement that are based upon evidence in its possession at this time, and that arise out of the conduct giving rise to this investigation. In this regard, Defendant recognizes the United States has agreed not to prosecute all of the criminal charges the evidence establishes were committed by Defendant solely because of the promises made by Defendant in this Agreement. Defendant agrees, however, that for purposes of preparing the Presentence Report, the United States Attorney's Office will provide the United States Probation Office with evidence of all conduct committed by Defendant.

Defendant agrees that any charges to be dismissed before or at the time of sentencing were substantially justified in light of the evidence available to the United States, were not vexatious, frivolous or taken in bad faith, and do not provide Defendant with a basis for any future claims under the "Hyde Amendment," Pub. L. No. 105-119 (1997).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

15. **Breach, Waiver, and Post-Plea Conduct.** Defendant agrees that, if Defendant breaches this Plea Agreement, the United States may withdraw from this Plea Agreement and Defendant may be prosecuted for all offenses for which the United States has evidence. Defendant agrees not to oppose any steps taken by the United States to nullify this Plea Agreement, including the filing of a motion to withdraw from the Plea Agreement. Defendant also agrees that, if Defendant is in breach of this Plea Agreement, Defendant has waived any objection to the re-institution of any charges that previously were dismissed or any additional charges that had not been prosecuted.

Defendant further understands that if, after the date of this Agreement, Defendant should engage in illegal conduct, or conduct that violates any conditions of release or the conditions of confinement (examples of which include, but are not limited to, obstruction of justice, failure to appear for a court proceeding, criminal conduct while pending sentencing, and false statements to law enforcement agents, the Pretrial Services Officer, Probation Officer, or Court), the United States is free under this Plea Agreement to file additional charges against Defendant or to seek a sentence that takes such conduct into consideration by requesting the Court to apply additional adjustments or enhancements in its Sentencing Guidelines calculations in order to increase the applicable advisory Guidelines range, and/or by seeking an upward departure or variance from the calculated advisory Guidelines range. Under these circumstances, the United States is free to seek such adjustments, enhancements, departures, and/or variances even if otherwise precluded by the terms of the Plea Agreement.

16. **Waiver of Appellate Rights and Rights to Collateral Attacks.** Defendant acknowledges that, by entering the guilty pleas required by this plea agreement, Defendant waives all rights to appeal from Defendant's conviction and any pretrial rulings of the Court. Defendant further agrees that, provided the Court imposes a custodial sentence that is within or below the Sentencing Guidelines range (or the statutory mandatory minimum, if greater than the Guidelines range) as determined by the Court at the time of sentencing, Defendant waives to the full extent of the law:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Any right conferred by Title 18, United States Code, Section 3742, to challenge, on direct appeal, the sentence imposed by the Court, including any fine, restitution order, probation or supervised release conditions, or forfeiture order (if applicable); and

b. Any right to bring a collateral attack against the conviction and sentence, including any restitution order imposed, except as it may relate to the effectiveness of legal representation.

This waiver does not preclude Defendant from bringing an appropriate motion pursuant to 28 U.S.C. § 2241, to address the conditions of Defendant's confinement or the decisions of the Bureau of Prisons regarding the execution of Defendant's sentence.

If Defendant breaches this Plea Agreement at any time by appealing or collaterally attacking (except as to effectiveness of legal representation) the conviction or sentence in any way, the United States may prosecute Defendant for any counts, including those with mandatory minimum sentences, that were dismissed or not charged pursuant to this Plea Agreement.

17. **Voluntariness of Plea**. Defendant agrees that Defendant has entered into this Plea Agreement freely and voluntarily, and that no threats or promises were made to induce Defendant to enter a plea of guilty other than the promises contained in this Plea Agreement or set forth on the record at the change of plea hearing in this matter.

18. **Statute of Limitations.** In the event this Plea Agreement is not accepted by the Court for any reason, or Defendant breaches any of the terms of this Plea Agreement, the statute of limitations shall be deemed to have been tolled from the date of the Plea Agreement to: (1) thirty (30) days following the date of non-acceptance of the Plea Agreement by the Court; or (2) thirty (30) days following the date on which a breach of the Plea Agreement by Defendant is discovered by the United States Attorney's Office.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. **Completeness of Agreement**. The United States and Defendant acknowledge that these terms constitute the entire Plea Agreement between the parties, except as may be set forth on the record at the change of plea hearing in this matter. This Agreement binds only the United States Attorney's Office for the Western District of Washington and the Computer Crime & Intellectual Property Section of the United States Department of Justice. It does not bind any other United States Attorney's Office or any other office or agency of the United States, or any state or local prosecutor.

Dated this 16TH day of November, 2020.

/s/ Andrii Kolpakov (w/ express permission to attorney)
ANDRII KOLPAKOV
Defendant

Vadim A. Glozman
VADIM A. GLOZMAN
Attorney for Defendant

FOR
ANDREW C. FRIEDMAN
Assistant United States Attorney

FRANCIS FRANZE-NAKAMURA
STEVEN MASADA
Assistant United States Attorneys

FOR
ANTHONY TEELUCKSINGH
Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970