United States District Court
Eastern District of Michigan
Southern Division

United States of America,

Plaintiff,

Hon. Denise Page Hood

v.

Case No. 19-20478

D-3 Aleksandr Skorodumov,

Defendant.
_____/

Plea Agreement

The United States of America (which includes the United States Attorney's Office for the Eastern District of Michigan and the Computer Crime and Intellectual Property Section of the Criminal Division of the United State Department of Justice, hereinafter "prosecuting offices") and the defendant, **ALEKSANDR SKORODUMOV**, have reached a plea agreement under Federal Rule of Criminal Procedure 11. The plea agreement's terms are:

1. Count of Conviction

The defendant will plead guilty to Count 1 of the First Superseding Indictment. Count 1 charges the defendant with

Conspiracy to Engage in a Racketeer Influenced Corrupt Organization (RICO) under 18 U.S.C. § 1962(d).

2. Statutory Minimum and Maximum Penalties

The defendant understands that the count to which he is pleading guilty carries the following maximum statutory penalty:

Count 1	Term of imprisonment:	20 years
	Fine:	$250,000 or twice the gross profits or proceeds from the offense
	Term of supervised release:	Not more than 5 years

3. Agreement to Dismiss Remaining Charges

If the Court accepts this agreement and imposes sentence consistent with its terms, the prosecuting offices will move to dismiss the remaining charge in the First Superseding Indictment against the defendant in this case. Specifically, the prosecuting offices will move to dismiss Count 2, Bank Fraud Conspiracy, 18 U.S.C. § 1349, of the First Superseding Indictment.

4. Elements of Count of Conviction

The elements of Count 1, 18 U.S.C. § 1962(d), Conspiracy to Engage in a Racketeer Influenced Corrupt Organization, are:

A. First, that an enterprise, as alleged in the First Superseding Indictment, existed;

B. The defendant was associated with the enterprise;

C. The defendant knowingly agreed to conduct or participate in the conduct of the affairs of the enterprise;

D. The defendant and at least one other conspirator agreed to conduct or participate in the conduct of the affairs of the enterprise through a pattern of racketeering activity, that is, that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise within a 10-year period; and

E. The enterprise engaged in, or its activities affected, interstate or foreign commerce.

5. Factual Basis

The parties agree that the following facts are true, accurately describe the defendant's role in the offense, and provide a sufficient factual basis for the defendant's guilty plea.

A. From approximately 2009 until approximately the middle of 2015, in the Eastern District of Michigan and elsewhere, defendant **SKORODUMOV** was employed by, associated

with, and a key member of the criminal organization described below (the "Organization"), an enterprise engaged in, and the activities of which affected interstate and foreign commerce, and unlawfully conspired to conduct and participate, directly and indirectly, in the conduct of the affairs of the Organization through a pattern of racketeering activity described below.

B. The Organization was a criminal enterprise, that is, a group of individuals associated in fact, whose members functioned as a continuing unit for a common purpose of achieving the objectives of the enterprise, that existed to enrich its members and associates through acts of identity theft and financial fraud, including, but not limited to: transferring false and stolen identification documents; aiding and abetting the access of computers without authorization; aiding and abetting the possession, trafficking, and use of unauthorized access devices; aiding and abetting bank fraud; and aiding and abetting wire fraud affecting financial institutions. The Organization did so by providing "bulletproof hosting" services (as further described below) to other cybercriminals, and by intentionally using its technological resources and skills to aid others to propagate malicious software ("malware") and to commit bank frauds on victims throughout the world, and with federally insured financial institutions, including in the Eastern District of Michigan. In so doing, the Organization and its members helped their clients to access computers without authorization, steal financial information (including banking credentials), and initiate unauthorized wire transfers from victims' financial accounts using this stolen information. Further, the Organization and its members regularly used stolen and false identity documents and information to avoid detection of its activities by law enforcement and legitimate businesses with which it interacted.

C. As providers of a bulletproof hosting service, Organization members rented Internet Protocol ("IP") addresses and

servers, and registered domain names (hereinafter, "Internet infrastructure") to cyber-criminal clients, in a manner designed to preserve both the Organization and its clients' anonymity, to minimize interruptions in service, and to help the clients evade detection of their criminal activities by law enforcement. That is, **SKORODUMOV** and other Organization members rented Internet infrastructure to clients knowing this infrastructure would be used to commit cybercrimes.

D. Further, as providers of a bulletproof hosting service, **SKORODUMOV** and other Organization members provided various services to the Organization's criminal clientele. One such service included monitoring "abuse notices" and "block lists" issued or maintained by third-party online services, including Spamhaus and Zeus Tracker, which reported malicious activities on particular domains and IP addresses and caused Internet Service Providers ("ISPs") not to route traffic to the affected domains or IP addresses until the "block" was removed or the abuse notice was resolved. **SKORODUMOV** and other Organization members monitored these lists and notices so they could quickly identify "flagged" or blocked domains and IP addresses, transfer their clients' affected infrastructure to new or "clean" domains and IP addresses, and ensure the clients could continue their criminal activities with minimal interruptions in service.

E. Between approximately August 2008 until approximately November 2015, **SKORODUMOV** and other Organization members knowingly facilitated and aided and abetted the distribution over the Internet of "spam" email and malware that were used to gain unauthorized access to victims' computers in the United States and abroad and commit financial frauds. Specifically, **SKORODUMOV** and other Organization members provided bulletproof hosting services for clients they knew to be disseminating banking trojans (i.e., a form of malware designed and used to gain

unauthorized access to victims' computers and steal personal information used to gain access to and control online bank accounts) and exploit kits (i.e., another form of malware used to identify a computer's vulnerabilities and gain access to the computer, often to deploy additional malware, including banking trojans). Malware programs hosted by this Organization included Zeus, SpyEye, Citadel, and the Blackhole Exploit Kit ("Blackhole"). **SKORODUMOV** and other Organization members knew: (1) that these banking trojans and Blackhole were used primarily, if not exclusively, to cause unauthorized damage to computers and gain access to computers without authorization, and steal financial and other personal identifying information; (2) that the Organization's Internet infrastructure and services were used by their clients to further this computer intrusion activity; and (3) that the resulting financial frauds would impact financial institutions and accountholders in the United States. The malware hosted by the Organization rampantly attacked U.S. companies and financial institutions, including entities in the Eastern District of Michigan, causing or attempting to cause millions of dollars in losses to U.S. victims. These losses were reasonably foreseeable to **SKORODUMOV** and other Organization members.

F. The purposes of the Organization included, but were not limited to: providing Internet infrastructure and services for cyber criminals whom the Organization's members knew to be using these services for illegal activities, including bank fraud, wire fraud, identification fraud, computer fraud, and trafficking in unauthorized access devices; promoting the Organization, its services, and the reputation and standing of its members; protecting the enterprise, its members, and its clients from detection, apprehension, and prosecution by law enforcement; and enriching the leaders and members of the enterprise by taking a fee for services rendered for the Organization's clients, which the enterprise members knew furthered the criminal activities of those clients.

G. Members of the Organization had defined roles in the enterprise, including proprietors, system administrators, and client relations/administrative personnel.

   a. The proprietors launched the Organization in approximately August 2008 and were its operational leaders.

   b. The system administrators, including **SKORODUMOV**, registered domains and IP addresses (including with false and/or stolen identity information), set up and configured servers, assigned IP addresses, provided technical assistance to clients, and reconfigured clients' domains and IP addresses in response to abuse notices. **SKORODUMOV** was the lead systems administrator, and at some points the only system administrator, for the Organization. One Organization proprietor believed the Organization would have failed without **SKORODUMOV**.

   c. The client relations and administrative personnel conducted and tracked marketing efforts, screened job applications for new hires, used stolen personally identifiable information and false information to register financial accounts and webhosting accounts with ISPs, and communicated with ISPs about abuse notices relating to the Organization's customers' accounts.

H. **SKORODUMOV** and other Organization members agreed to conduct and participate in the conduct of the affairs of the enterprise as follows:

   a. The Organization's members advertised bulletproof hosting services to known cyber criminals and on known online cybercrime forums between at least 2008 and at least 2013. The forums on which the advertisements were posted could be accessed by forum members from computers located anywhere in

the world, including in the Eastern District of Michigan, and were used by those members to buy, sell, rent, or trade malware kits, botnets, and stolen personally identifiable information, and related services and information.

b. The Organization's members leased domains, servers, and IP addresses from ISPs all over the world, including in the United States, using stolen and fraudulent identity information and a variety of payment methods, all to hide the true owners and users of the accounts.

c. The Organization's members subleased the Internet infrastructure it had rented from ISPs to individuals whom they knew were using this infrastructure to disseminate spam and malware, including banking trojans and exploit kits; to operate botnets; and to steal banking credentials.

d. The Organization's members monitored third-party online services' "block lists," including Spamhaus and Zeus Tracker, notified affected clients when an Organization-administered domain or IP address was "flagged" for abuse, relocated the clients' data to new Internet infrastructure, and provided false information to the ISPs from which the Organization had rented the Internet infrastructure so as to minimize service interruptions.

e. The Organization members used online payment accounts often registered with false information to receive payments from clients and pay staff members' salaries in order to protect the membership's anonymity.

f. The Organization members used a wide range of communication methods, and changed accounts frequently, in order to protect the membership's anonymity and to avoid detection by law

enforcement. Many of these communications accounts were registered using false information or online aliases.

I. As part of the conspiracy, **SKORODUMOV** agreed that he or a co-conspirator would engage in two or more acts of racketeering activity in the conduct of the affairs of the enterprise, including aiding and abetting violations of 18 U.S.C. § 1028 (fraud in connection with identification documents), 18 U.S.C. § 1029 (fraud in connection with access devices), 18 U.S.C. § 1030(a)(5)(A) (computer fraud), 18 U.S.C. § 1343 (wire fraud affecting a financial institution), and 18 U.S.C. § 1344 (bank fraud). In furtherance of the conspiracy, **SKORODUMOV** and his co-conspirators committed the following acts, among others:

a. In February 2010, an Organization proprietor discussed an abuse notice with one of the Organization's systems administrators, which indicated that their IP address had been blocked by Spamhaus because it "was being used for elements of the Zeus Trojan." On March 10, 2010, **SKORODUMOV** redirected a domain used to disseminate Zeus malware from the flagged IP address to a new IP address.

b. Between approximately September 2011 and November 2012, the Organization rented infrastructure to clients for use in hosting the Blackhole Exploit Kit. **SKORODUMOV** serviced many of these clients, helping them to install relevant software and by responding to abuse notices to avoid service interruptions. For example:

i. On or about October 25, 2011, **SKORODUMOV** communicated with "Paunch," whom **SKORODUMOV** knew to be Blackhole's author. They discussed a technical issue that Paunch's administrator, "Blackhole2," was having with one of the

Organization's servers. **SKORODUMOV** agreed to discuss the issue with Blackhole2 directly.

ii. On or about November 9, 2011, **SKORODUMOV** discussed a Spamhaus Block List ("SBL") notice with Organization members. The SBL notice indicated that one of the Organization's IP addresses had been blocked because "Blackhole exploit kit hosted here." An Organization proprietor directed **SKORODUMOV** to "[g]ive [the client] an IP from [another provider] that has not been used before." Shortly thereafter, **SKORODUMOV** reported that he had "passed on the task." The same day, Spamhaus removed the offending IP address from its block list.

iii. On or about December 13, 2011, **SKORODUMOV** again sought an Organization proprietor's guidance on how to handle another Blackhole-related abuse notice. **SKORODUMOV** stated: "Paunch is getting burned. Should we take down the IP or block the domains for now?," and pasted a copy of an SBL notice with the subject line, "Malware botnet controller @[IP address]" into the chat. The proprietor directed **SKORODUMOV** to block "[a]ll the domains for now," so that the offending content could remain on the Organization's IP address. Two weeks later, the proprietor finally directed **SKORODUMOV** to "take down Paunch."

iv. Between February and May 2012, **SKORODUMOV** assisted another client to host Blackhole. On or about February 21, 2012, the client asked **SKORODUMOV** if he could "setup bh for [the client]" and stated that

"Paunch" gave him the Organization's contact information. **SKORODUMOV** coordinated the installation of Blackhole on the Organization's servers and provided continued assistance over several months.

c. In January 2012, **SKORODUMOV** brainstormed with other Organization members about how to respond to abuse complaints impacting the Organization's infrastructure. For example:

   i. On or about January 13, 2012, an Organization proprietor instructed **SKORODUMOV** to prepare for a complaint from an Internet Service Provider after one of the Organization's IP addresses appeared on an SBL. The proprietor noted that it might "be necessary to fight for the server, appealing that we had nothing to do with it" and suggested **SKORODUMOV** "write to them in advance that there was an intrusion." The following day, **SKORODUMOV** forwarded the proprietor a draft of the message, asking: "Will this kind of bullshit work?" As instructed, the message said that the Organization believed its server had been compromised by criminals.

   ii. On or about January 15, 2012, the Organization proprietor instructed **SKORODUMOV** on how to respond to customers whose services were shut down due to abuse complaints, stating: "[r]egarding SPY/Zeus/Blackhole, we change IPs . . . / you can say it this way: your IP was taken down due to SBL and there will be a replacement. / . . . / For everyone that has Blackhole, the replacement is strictly to be paid for / Zeus and SPY can be changed immediately for free."

d. **SKORODUMOV** also helped clients set up SpyEye and Citadel malware-related infrastructure, knowing this infrastructure would be used to set up botnets and steal victims' banking credentials. For example:

i. On or about August 16, 2011, **SKORODUMOV** helped an Organization client troubleshoot issues relating to the installation of a SpyEye control panel on an Organization server.

ii. In or about April 2012, **SKORODUMOV** helped another Organization client set up an administrative control panel for the Citadel banking trojan. **SKORODUMOV** explained that various changes would need to be made, stating: "I am already quite familiar with Zeus itself, and by all indications, this is almost the same. I already found potential problems. Now I'll clean them up…. " After the setup was completed and the client continued to have problems, **SKORODUMOV** suggested he "sign up for our admin subscription" so the client did not "go broke getting [**SKORODUMOV**'s] advice and paying one-time fees."

e. The Organization's crimes continued until at least the middle of 2015. For example, in April 2015, one of the Organization's IP addresses was used to steal or attempt to steal funds from accounts at four U.S. financial institutions. The ISP account associated with this IP address was fraudulently registered using the identity information of "I.P.," a real Lithuanian national. Additionally, it was paid for using a U.S.-based financial account that Organization members fraudulently registered using stolen or fraudulent identity documents belonging to "I.P." Further, Organization members used this fraudulent financial account to rent Internet infrastructure from hundreds

of ISPs, including ISPs in the United States, between at least September 2011 until at least November 2015.

6. Advice of Rights

The defendant has read the First Superseding Indictment, has discussed the charges and possible defenses with his attorney, and understands the crime charged. The defendant understands that, by pleading guilty, he is waiving many important rights, including the following:

A. The right to plead not guilty and to persist in that plea;

B. The right to a speedy and public trial by jury;

C. The right to be represented by counsel—and, if necessary, have the court-appointed counsel at trial;

D. The right to be presumed innocent and to require the government to prove the defendant guilty beyond a reasonable doubt at trial;

E. The right to confront and cross-examine adverse witnesses at trial;

F. The right to testify or not to testify at trial, whichever the defendant chooses;

G. If the defendant chooses not to testify at trial, the right to have the jury informed that it may not treat that choice as evidence of guilt;

H. The right to present evidence or not to present evidence at trial, whichever the defendant chooses; and

I. The right to compel the attendance of witnesses at trial.

7. Collateral Consequences of Conviction

The defendant understands that his conviction here may carry additional consequences under federal or state law. The defendant understands that, if he is not a United States citizen, his conviction here may require him to be removed from the United States, denied citizenship, and denied admission to the United States in the future. The defendant further understands that the additional consequences of his conviction here may include, but are not limited to, adverse effects on the defendant's immigration status, naturalized citizenship, right to vote, right to carry a firearm, right to serve on a jury, and ability to hold certain licenses or to be employed in certain fields. The defendant understands that no one, including the defendant's attorney or the Court, can predict to a certainty what the additional consequences of

the defendant's conviction might be. The defendant nevertheless affirms that the defendant chooses to plead guilty regardless of any immigration or other consequences from his conviction.

A. Waiver of Rights Related to Removal from the United States. Except as provided in section 7.B. below, the defendant agrees to waive the defendant's rights to apply for any and all forms of relief or protection from removal, deportation, or exclusion under the Immigration and Nationality Act (as amended) and related federal regulations. These rights include, but are not limited to, the ability to apply for the following forms of relief or protection from removal:
(a) voluntary departure; (b) asylum; (c) withholding of deportation or removal; (d) cancellation of removal;
(e) suspension of deportation; (f) adjustment of status; and
(g) protection under Article 3 of the Convention Against Torture. As part of this plea agreement, the defendant specifically acknowledges and states that the defendant has not been persecuted in Lithuania, and has no present fear of persecution in Lithuania on account of race, religion,

nationality, membership in a particular social group, or political opinion. Similarly, the defendant further acknowledges and states that the defendant has not been tortured in and has no present fear of torture in Lithuania.

B. Exception for Changed Circumstances Arising After Plea. Nothing in this plea agreement shall prohibit the defendant from applying for asylum, withholding of removal, or protection under Article 3 of the Convention Against Torture, provided the application is based solely on changed circumstances arising after the entry of this plea but before the defendant's removal.

8. Defendant's Guideline Range

A. Court's Determination

The Court will determine the defendant's guideline range at sentencing.

B. Acceptance of Responsibility

The government recommends under Federal Rule of Criminal Procedure 11(c)(1)(B) that the defendant receive a two-level reduction for acceptance of responsibility under USSG § 3E1.1(a) for his guideline

calculation on Count 1. Further, if the defendant's offense level is 16 or greater and the defendant is awarded the two-level reduction under USSG § 3E1.1(a), the government recommends that the defendant receive an additional one-level reduction for acceptance of responsibility under USSG § 3E1.1(b). If, however, the government learns that the defendant has engaged in any conduct inconsistent with acceptance of responsibility—including, but not limited to, making any false statement to, or withholding information from, his probation officer; obstructing justice in any way; denying his guilt on the offense to which he is pleading guilty; committing additional crimes after pleading guilty; or otherwise demonstrating a lack of acceptance of responsibility as defined in USSG § 3E1.1—the government will be released from its obligations under this paragraph, will be free to argue that the defendant not receive *any* reduction for acceptance of responsibility under USSG § 3E1.1, and will be free to argue that the defendant receive an enhancement for obstruction of justice under USSG § 3C1.1.

C. Other Guideline Recommendations

The parties also recommend under Federal Rule of Criminal Procedure 11(c)(1)(B) that the following guideline provisions apply to the defendant's guideline calculation on Count 1:

- Base offense level, § 2B1.1(a)(1) = 7
- Loss greater than $3,500,000, § 2B1.1(b)(1)(J) = 18
- 10 or more victims; mass marketing, § 2B1.1(b)(2)(A)(i), (ii) = 2
- Sophisticated means, § 2B1.1(b)(10)(C) = 2
- Organizer/leader/manager/supervisor, § 3B1.1(c) = 2

The parties have no other recommendations as to the defendant's guideline calculation.

D. Factual Stipulations for Sentencing Purposes

The parties agree that the Organization's racketeering activities caused and attempted to cause at least $3,500,000 in losses to U.S. victims.

E. Parties' Obligations

Both the defendant and the government agree not to take any position or make any statement that is inconsistent with any of the guideline recommendations or factual stipulations in paragraphs 8.B,

8.C, or 8.D. Neither party is otherwise restricted in what it may argue or present to the Court as to the defendant's guideline calculation.

F. Not a Basis to Withdraw

The defendant understands that he will have no right to withdraw from this agreement or withdraw his guilty plea if he disagrees, in any way, with the guideline range determined by the Court, even if that guideline range does not incorporate the parties' recommendations or factual stipulations in paragraphs 8.B, 8.C, or 8.D. The government likewise has no right to withdraw from this agreement if it disagrees with the guideline range determined by the Court.

9. Imposition of Sentence

A. Court's Obligation

The defendant understands that in determining his sentence, the Court must calculate the applicable guideline range at sentencing and must consider that range, any possible departures under the sentencing guidelines, and the sentencing factors listed in 18 U.S.C. § 3553(a), and apply any applicable mandatory minimums.

B. Imprisonment

1. Agreement

Under Federal Rule of Criminal Procedure 11(c)(1)(C), the parties agree that the defendant's sentence of imprisonment on Count 1 may not exceed 97 months.

2. Limited Right to Withdraw

If the Court rejects the agreement by deciding to impose a sentence of imprisonment on Count 1 higher than permitted by paragraph 9.B.1, the defendant will be permitted to withdraw his guilty plea. That is the only reason the defendant may withdraw his guilty plea. If the defendant decides not to withdraw his guilty plea in those circumstances, the defendant agrees that the Court may impose a sentence on Count 1 higher than permitted by paragraph 9.B.1 and that all other provisions in this agreement will remain in effect.

If the Court rejects the plea agreement by rejecting or purporting to reject any other term or terms of this agreement, the government will be permitted to withdraw from this agreement.

C. Supervised Release

1. Recommendation

Because the defendant is likely to be deported after imprisonment, the parties do not recommend a specific term of supervised release.

USSG § 5D1.1(c). The parties agree, however, that if a term of supervised release is ordered, the length of term is two to five years. USSG § 5D1.2(a)(1).

2. No Right to Withdraw

The parties' recommendation is not binding on the Court. The defendant understands that he will have no right to withdraw from this agreement or withdraw his guilty plea if the Court decides not to follow the parties' recommendation.

If the Court decides to impose a term of supervised release, the defendant also understands that the government's recommendation concerning the length of the defendant's sentence of imprisonment, as described above in paragraph 9.B.1, will not apply to or limit any term of imprisonment that results from any later revocation of the defendant's supervised release.

D. Fine

There is no recommendation or agreement as to a fine.

E. Restitution

The Court must order restitution to every identifiable victim of the defendant's offense. There is no recommendation or agreement on

restitution. The Court will determine at sentencing who the victims are and the amounts of restitution they are owed.

The defendant agrees that restitution is due and payable immediately after the judgment is entered and is subject to immediate enforcement, in full, by the prosecuting offices. 18 U.S.C. §§ 3612(c) and 3613. If the Court imposes a schedule of payments, the defendant agrees that the schedule of payments is a schedule of the minimum payment due, and that the payment schedule does not prohibit or limit the methods by which the prosecuting offices may immediately enforce the judgment in full.

The defendant agrees to make a full presentence disclosure of his financial status to the prosecuting offices by completing a Financial Disclosure Form and the accompanying releases for the purpose of determining his ability to pay restitution. The defendant agrees to complete and return the Financial Disclosure Form within three weeks of receiving it from government counsel. The defendant agrees to participate in a presentencing debtor's examination if requested to do so by government counsel.

F. Special Assessment

The defendant understands that he will be required to pay a special assessment of $100, due immediately upon sentencing.

10. Appeal Waiver

The defendant waives any right he may have to appeal his conviction on any grounds. If the defendant's sentence of imprisonment does not exceed 97 months, the defendant also waives any right he may have to appeal his sentence on any grounds.

11. Collateral Review Waiver

The defendant retains the right to raise claims alleging ineffective assistance of counsel or prosecutorial misconduct, as long as the defendant properly raises those claims by collateral review under 28 U.S.C. § 2255. The defendant also retains the right to pursue any relief permitted under 18 U.S.C. § 3582(c), as long as the defendant properly files a motion under that section. The defendant, however, waives any other right he may have to challenge his conviction or sentence by collateral review, including, but not limited to, any right he may have to challenge his conviction or sentence on any grounds under 28 U.S.C. § 2255 (except for properly raised ineffective assistance of counsel or

prosecutorial misconduct claims, as described above), 28 U.S.C. § 2241, or Federal Rule of Civil Procedure 59 or 60.

12. Consequences of Withdrawal of Guilty Plea or Vacation of Judgment

If the defendant is allowed to withdraw his guilty plea, or if the defendant's conviction or sentence under this agreement is vacated, the government may reinstate any charges against the defendant that were dismissed as part of this agreement and may file additional charges against the defendant relating, directly or indirectly, to any of the conduct underlying the defendant's guilty plea or any relevant conduct. If the government reinstates any charges or files any additional charges as permitted by this paragraph, the defendant waives his right to challenge those charges on the ground that they were not filed in a timely manner, including any claim that they were filed after the limitations period expired.

13. Use of Withdrawn Guilty Plea

The defendant agrees that if he is permitted to withdraw his guilty plea for any reason, he waives all of his rights under Federal Rule of Evidence 410, and the government may use his guilty plea, any statement that the defendant made at his guilty plea hearing, and the

factual basis set forth in this agreement, against the defendant in any proceeding.

14. Parties to Plea Agreement

This agreement does not bind any government agency except the prosecuting offices.

15. Scope of Plea Agreement

This plea agreement is the complete agreement between the parties and supersedes any other promises, representations, understandings, or agreements between the parties concerning the subject matter of this agreement that were made at any time before the guilty plea is entered in court. Thus, no oral or written promises made by the government to the defendant or to the attorney for the defendant at any time before the defendant pleads guilty are binding except to the extent they have been explicitly incorporated into this plea agreement. If the parties have entered, or subsequently enter, into a written proffer or cooperation agreement, though, this plea agreement does not supersede or abrogate the terms of that agreement. This plea agreement also does not prevent any civil or administrative actions

against the defendant, or any forfeiture claim against any property, by the prosecuting offices or any other party.

16. Acceptance of Agreement by Defendant

This plea offer expires unless it has been received, fully signed, in the prosecuting offices by 5:00 PM on February 19, 2021.

The government may withdraw from this agreement at any time before the defendant pleads guilty.

JOHN NEAL Digitally signed by JOHN NEAL Date: 2021.02.11 08:26:16 -05'00'

John Neal
Chief, White Collar Crime Unit
Assistant United States Attorney

Saima S. Mohsin
Acting United States Attorney

PATRICK CORBETT Digitally signed by PATRICK CORBETT Date: 2021.02.11 08:44:02 -05'00'

Patrick E. Corbett
Assistant United States Attorney

Nicholas McQuaid
(Acting) Assistant Attorney General
U.S. Department of Justice
Criminal Division

LOUISA MARION Digitally signed by LOUISA MARION Date: 2021.02.11 09:07:24 -05'00'

Louisa Marion
Senior Counsel, Computer Crime and Intellectual Property Section

Dated: 2/10/2021

By signing below, the defendant and his attorney agree that the defendant has read or been read this entire document, has discussed it with his attorney, and has had a full and complete opportunity to confer with his attorney. The defendant further agrees that he understands this entire document, agrees to its terms, has had all of his questions answered by his attorney, and is satisfied with his attorney's advice and representation.

Benton Martin
Attorney for Defendant

Aleksandr Skorodumov
Defendant

Dated: 16.02.21