BRYAN SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant United States Attorney
Federal Building & U.S. Courthouse
222 West 7th Avenue, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: adam.alexander@usdoj.gov

CATHERINE ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Email: Catherine.Pelker@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. KENNETH SCHUCHMAN, Defendant.	No. 3:18-cr-00154-TMB-DMS **PLEA AGREEMENT**

Unless the parties jointly inform the Court in writing of any additional agreements, this document in its entirety contains the terms of the plea agreement between the defendant and the United States. This agreement is limited to the District of Alaska; it does not bind other federal, state, or local prosecuting authorities.

I. SUMMARY OF AGREEMENT, FEDERAL RULE OF CRIMINAL PROCEDURE 11

A. Summary of Agreement

The defendant agrees to plead guilty to the sole count of the Indictment in this case: Count: 1 - Aiding and Abetting Computer Intrusions, in violation of 18 U.S.C. §§ 1030 and 2. The United States agrees to recommend a sentence at the low end of the guideline range as calculated and adopted by the court. The United States agrees not to prosecute the defendant further for any other offense related to the events that resulted in the charge contained in the Indictment.

The defendant will waive all rights to appeal the conviction and sentence imposed under this agreement. The defendant will also waive all rights to collaterally attack the conviction and sentence, except on the grounds of ineffective assistance of counsel or the voluntariness of the plea.

B. Federal Rule of Criminal Procedure 11

Unless the parties otherwise inform the Court in writing, Federal Rule of Criminal Procedure 11(c)(1)(A) and (B) will control this plea agreement. Thus, the defendant may not withdraw from this agreement or the guilty plea if the Court rejects the parties' sentencing recommendations at the sentencing hearing.

II. CHARGES, ELEMENTS, FACTUAL BASIS, STATUTORY PENALTIES AND OTHER MATTERS AFFECTING SENTENCE

A. Charges

1. The defendant agrees to plead guilty to the sole count of the Indictment:

Count 1: Aiding and Abetting Computer Intrusions, a violation of 18 U.S.C. §§ 1030(a)(5)(A) and 2.

B. Elements

The elements of the charge in Count 1 to which the defendant is pleading guilty are as follows:

1. First, the crime of fraud and related activity in connection with a computer was committed in violation of 18 U.S.C. § 1030(a)(5)(A), the elements of which are:

   i) a person knowingly caused the transmission of a program, code, command or information to a computer without authorization; and

   ii) as a result of the transmission, the person intentionally impaired the integrity or availability of data, a program, system, or information; and

   iii) the computer was used in or affected interstate or foreign commerce or communication.

2. Second, the defendant knowingly and intentionally aided, counseled, commanded, induced, or procured a violation of 18 U.S.C. § 1030(a)(5)(A); and

3. Third, the defendant acted before the crime was completed with the knowledge and intention of helping a person commit a violation of 18 U.S.C. § 1030(a)(5)(A).

C. Factual Basis

The defendant admits the truth of the allegations in Count 1 of the Indictment and the truth of the following statement, and the parties stipulate that the Court may rely upon this statement to support the factual basis for the guilty plea and for the imposition of the sentence:

The United States and the defendant, KENNETH CURRIN SCHUCHMAN ("SCHUCHMAN"), agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence.

From at least on or about July 2017, and continuing through October 2018, in the District of Alaska and elsewhere, SCHUCHMAN knowingly and intentionally caused the infection of computer devices for the purposes of establishing Distributed Denial of Service (DDoS) Botnets, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (b), that is, SCHUCHMAN knowingly caused the transmission of a program, information, code, and command, and knowingly aided and abetted others in doing the same and in attempting to do the same, and as a result of such conduct,

intentionally caused damage and attempted to cause damage without authorization to a protected computer, and resulting in a loss of $5,000 or more in damage affecting ten or more protected computers during a one-year period, specifically from August 1, 2017 through July 31, 2018.

1. BACKGROUND

Distributed denial of service ("DDoS") attacks occur when multiple internet-enabled devices act in unison to overwhelm the targeted devices. While there are many different methodologies used to conduct DDoS attacks, the criminal intent is to generate sufficient attack volume to overwhelm the capacity of the target device, rendering the target device inaccessible for the duration of the attack. DDoS attacks of sufficient volume can damage not only the intended target but also upstream internet service providers as well as adjacent servers on the same network.

DDoS attacks are often directed at servers that provide critical services to public and private entities, including those that host websites, with the intent of causing sufficient damage to render the domain or server inaccessible to legitimate users. Individuals developing botnets to conduct DDoS attacks damage at least two different categories of victim devices: victim devices that are hijacked and exploited to comprise the botnet ("nodes") and victim devices that are the targets of the botnets DDoS attacks. Criminals often target so-called Internet of Things (IoT) devices such as home DVRs, internet routers, and smart camera systems. These devices are can be subject to wide-scale credential vulnerabilities that can permit criminal actors to exploit substantial numbers of these devices simultaneously and develop botnets at scale.

2. INSTANT OFFENSE

SCHUCHMAN and co-conspirators located in the United States and abroad entered into a conspiracy spanning at least the period between July 2017 and October 2018 to conduct DDoS attacks using botnets comprised of hijacked IoT devices. In furtherance of this criminal scheme, SCHUCHMAN and his co-conspirators continually developed criminal tools and techniques necessary to effectively deploy botnets for the purposes of conducting DDoS attacks. They gave these botnets names such as "Satori," "Masuta," and "Okiru." Over time, these botnets grew more complex and effective in proportion to the number of compromised devices exploited.

SCHUCHMAN and his co-conspirators did not have consent or permission from the owners of the victim devices compromising the botnet, and instead used an array of complex means to compromise the devices in order to force them to participate in the DDoS attacks against targeted victims. While SCHUCHMAN and his co-conspirators themselves conducted DDoS attacks using the botnets they developed, their primary focus was monetizing their botnets by selling access to other criminal actors in order to generate illicit proceeds. SCHUCHMAN and his co-conspirators received payment from customers who rented access to their botnets to engage in additional criminal activity. Those payments were made in cryptocurrency, such as Bitcoin, and other online platforms such as PayPal.

SCHUCHMAN specialized in researching and identifying vulnerabilities for classes of victim devices for the purpose of compromising those devices at scale. Those vulnerabilities often included default credential pairs such as usernames and passwords,

through which SCHUCHMAN and his co-conspirators were able to compromise not only individual devices, but entire categories of devices sharing the same vulnerability.

From at least on or about July 28, 2017, and continuing through July 27, 2018, SCHUCHMAN and co-conspirators, who are not charged in this indictment, sold access to an evolving series of DDoS botnets. Initially, the botnets were based largely on the source code used for the Mirai botnet, which was the subject of a previous prosecution in the District of Alaska. SCHUCHMAN and co-conspirators, however, added additional features and exploited new vulnerabilities during the course of their criminal conspiracy. SCHUCHMAN'S principal co-conspirators included the individuals using the criminal nicknames "Vamp" and "Drake," whose true identities are known to the United States.

Vamp served as the primary developer and coder for the botnet at this time. Drake took the lead in managing the sales and customer support. SCHUCHMAN developed and acquired exploits used to infect new devices for the botnet and provided development support. All three individuals and other currently uncharged co-conspirators took an active role in aiding and abetting the criminal development and deployment of DDoS botnets during this period for the purpose of hijacking victim devices and targeting victims with DDoS attacks.

In August 2017, SCHUCHMAN and co-conspirators named one of their developmental botnets Satori. This version extended the Mirai DDoS botnet's capabilities, targeted devices with Telnet vulnerabilities, and utilized an improved scanning system borrowed from another DDoS botnet known as Remaiten. Approximately 100,000 devices were compromised by this botnet, including devices

located in the District of Alaska. SCHUCHMAN and his co-conspirators used this version of their Satori botnet to conduct DDoS attacks against victims in the United States, including large internet service providers, popular online gaming services, prominent internet hosting companies, and hosting companies specializing in DDoS mitigation.

During that August 2017 time period, SCHUCHMAN bragged about compromising 32,000 devices belonging to a large Canadian victim ISP, which allowed him in turn to attack targets with bandwidth approximating one Terabit per second. SCHUCHMAN claimed responsibility for a test attack using the compromised Canadian devices among others sufficient to cause a dramatic increase to internet latency on a national level.

By on or about September or October 2017, SCHUCHMAN, Vamp, Drake, and others made improvements to the previously described Satori botnet, which they rechristened as "Okiru." Okiru exploited vulnerable devices including the Goahead family of surveillance cameras.

In or about November 2017, SCHUCHMAN, Vamp, Drake, and others further evolved Satori and Okiru, naming the updated version "Masuta." Masuta targeted vulnerable Huawei and Gigabit Passive Optical Network (GPON) fiber-optic networking devices, infecting up to 700,000 compromised nodes. Logs during the Masuta time period depict a large number of attacks launched at the end of November by SCHUCHMAN, Drake, and others, including paying customers of the criminal botnet scheme. At this time, SCHUCHMAN also operated his own distinct DDoS botnet which

he utilized to attack IP addresses associated with ProxyPipe At the same time, SCHUCHMAN was also actively scanning the internet for vulnerable telnet devices for the purpose of identifying additional devices to incorporate into his active botnets. When SCHUCHMAN received abuse complaints related to the scanning, he responded in his father's identity. SCHUCHMAN frequently used identification devices belonging to his father to further the criminal scheme.

In or about January 2018, SCHUCHMAN, Drake, and others focused on combining elements of both Mirai and Satori to exploit devices largely based in Vietnam in order to expand the size and power of the resulting botnet.

By in or about March 2018, SCHUCHMAN, Drake, Vamp, and others further improved the botnet, which at this time came to be known as both Tsunami and Fbot. Tsunami/Fbot consisted predominantly of vulnerable Goahead camera devices. During the Tsunami/Fbot time period, the botnet infected up to 30,000 devices and was utilized to attack gaming servers as well as servers at Nuclear Fallout. During this development period, SCHUCHMAN and his co-conspirators discovered vulnerabilities in approximately 650,000 High Silicon DVR systems; SCHUCHMAN was able to successfully compromise at least 35,000 of these devices for the purpose of incorporating them into the Tsunami/Fbot botnet. Test attacks conducted by SCHUCHMAN and his co-conspirators using approximately 10,000 of these compromised and hijacked DVR systems resulted in estimated attack bandwidths exceeding 100 Gigabits per second (Gbit/s). At that time, DDoS attacks of that scale could be expected to result in significant damage.

In April 2018, SCHUCHMAN and additional co-conspirators not including Vamp and Drake developed an unnamed Qbot-derived DDoS botnet. To create this unnamed botnet, SCHUCHMAN exploited a number of devices, including high-bandwidth GPON devices at Telemax. At this point, SCHUCHMAN was competing with Vamp to compromise the same universe of botnet nodes utilizing overlapping credentials. Both SCHUCHMAN and Vamp made unauthorized configuration changes to the infected nodes in order to hinder the other's access to the compromised nodes. SCHUCHMAN employed tactics such as using the IPTables tool to kill all open ports on the devices, a technique capable of causing substantial damage to the victim device.

In July 2018, SCHUCHMAN was first interviewed by the FBI. At the time of this interview in July 2018, SCHUCHMAN had reconciled with Vamp and resumed working in earnest to improve their iterative generations of DDoS botnets described above.

The purpose of all of the aforementioned activity was to aid and abet DDoS attacks, which by their nature cause the transmission of code and commands that cause damage to the victim computers by rendering them inaccessible. At all relevant times, SCHUCHMAN knew and understood that these botnets were was designed to be used, and was in fact being used, to commit illegal and unauthorized DDoS attacks against computers in the United States and elsewhere. SCHUCHMAN acted with the intent and goal of aiding, abetting, and furthering these illegal DDoS attacks and causing them to occur. Further, SCHUCHMAN knew that his infection of the underlying devices was conducted without the authorization and consent of the device owners in Alaska and other locations.

SCHUCHMAN predominantly employed the monikers "Nexus" and "Nexus-Zeta" to converse with co-conspirators, solicit customers, and otherwise support the creation of the aforementioned DDoS botnets.

SCHUCHMAN was charged by indictment on August 21, 2018 but his criminal conduct continued past his initial appearance and pretrial status hearing in this case. SCHUCHMAN went so far as to create a new Qbot DDoS botnet variant on or about October 2018 while on supervised release after having been charged by indictment with creating and deploying DDoS botnets. SCHUCHMAN also used information gleaned from discovery in this matter to identify the whereabouts of his co-conspirator Drake for the purpose of facilitating a "swatting" attack that involved a fake 911 call alleging a hostage incident at Drake's residence, triggering a substantial law enforcement response in October 2018.

This Statement of Facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

The actions of the defendant, as recounted above, were in all respects knowing, voluntary, and intentional, and were not committed by mistake, accident or other innocent reason.

D. Statutory Penalties and Other Matters Affecting Sentence

1. Statutory Penalties

The maximum statutory penalties applicable to the charges to which the defendant is pleading guilty, based on the facts to which the defendant will admit in support of the guilty plea(s), are as follows:

Count 1: 18 U.S.C. § 1030 (Aiding and Abetting Computer Intrusions)

1) Imprisonment for not more than 10 years;

2) A fine not exceeding $250,000; and

3) Not more than three years of supervised release.

2. Other Matters Affecting Sentence

a. Conditions Affecting the Defendant's Sentence

The following conditions may also apply and affect the defendant's sentence: 1) pursuant to Comment 7 of U.S.S.G. § 5E1.2, the Court may impose an additional fine to pay the costs to the government of any imprisonment and supervised release term; 2) pursuant to 18 U.S.C.§ 3612(f), unless otherwise ordered, if the Court imposes a fine of more than $2,500, interest will be charged on the balance not paid within 15 days after the judgment date; 3) upon violating any condition of supervised release, a further term of imprisonment equal to the period of the supervised release may be imposed, with no credit for the time already spent on supervised release; 4) the Court may order the defendant to pay restitution pursuant to the 18 U.S.C. § 3663 and U.S.S.G. § 5E1.1, and if 18 U.S.C. § 3663A (mandatory restitution for certain crimes) applies, the Court shall order the defendant to pay restitution.

b. Payment of Special Assessment

The defendant agrees to pay the entire special assessment in this case on the day the Court imposes the sentence. All payments will be by check or money order, and are to be delivered to the Clerk of Court, United States District Court, 222 W. 7th Ave. Box 4, Rm. 229, Anchorage, AK 99513-7564.

c. Consequences of Felony Conviction

Any person convicted of a federal felony offense may lose or be denied federal benefits including any grants, loans, licenses, food stamps, welfare or other forms of public assistance, as well as the right to own or possess any firearms, the right to vote, the right to hold public office, and the right to sit on a jury. If applicable, any defendant who is not a United States citizen may be subject to deportation from the United States following conviction for a criminal offense, be denied citizenship, and not permitted to return to the United States unless the defendant specifically receives the prior approval of the United States Attorney General. In some circumstances, upon conviction for a criminal offense, any defendant who is a naturalized United States citizen may suffer adverse immigration consequences, including but not limited to possible denaturalization.

E. Restitution

The U.S. Government has not presently identified a specific restitution amount owed for the offense of conviction. The Court will have sole discretion ultimately to determine if the defendant has liability for any restitution.

F. Forfeiture

Defendant knowingly and voluntarily waives his rights pursuant to Rule 32.2(a) and admits that Defendant's interest in any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of the offense of conviction, pursuant to 18 U.S.C. § 982(a)(2)(A).

Defendant agrees not to file a claim or withdraw any claim already filed to any of the above-described property in any forfeiture proceeding, administrative or judicial, which has been or may be initiated by the United States. Defendant further waives the right to notice of any forfeiture proceeding involving this property, agrees not to assist others in filing a claim to said property in any forfeiture proceeding, and will take all steps as requested by the United States to pass clear title to the above-described property to the United States, including but not limited to, executing documents and testifying truthfully in any forfeiture proceeding. Defendant further agrees to cooperate to ensure that assets subject to forfeiture are not sold, disbursed, wasted, hidden, or otherwise made unavailable for forfeiture.

Defendant understands and acknowledges that the United States is relying upon the Defendant's truthful asset forfeiture disclosure and cooperation in entering into this plea agreement. If Defendant fails to cooperate or is untruthful in this regard, the United States may declare a material breach of this plea agreement.

III. ADVISORY UNITED STATES SENTENCING GUIDELINES, GUIDELINE APPLICATION AGREEMENTS, SENTENCING RECOMMENDATIONS

A. Advisory United States Sentencing Guidelines

The Court must consult the advisory United States Sentencing Commission Guidelines [U.S.S.G.] as well as the factors set forth in 18 U.S.C. § 3553(a) when considering the sentence to impose. The U.S.S.G. do not establish the statutory maximum or minimum sentence applicable to the offense(s) to which the defendant is pleading guilty. The U.S.S.G. are not mandatory and the Court is not bound to impose a sentence recommended by the U.S.S.G.

B. Guideline Application Agreements

The parties have no agreements on any guideline applications unless set forth below in this section.

1. Acceptance of Responsibility

If the United States concludes that the defendant has satisfied the criteria set out in U.S.S.G. § 3E1.1 and the applicable application notes, the United States agrees to recommend the defendant for a two level downward adjustment for acceptance of responsibility and, if U.S.S.G. § 3E1.1(b) applies, to move for the additional one level adjustment for acceptance of responsibility. If, at any time prior to imposition of the sentence, the United States concludes that the defendant has failed to fully satisfy the criteria set out in U.S.S.G. § 3E1.1, or has acted in a manner inconsistent with acceptance of responsibility, the United States will not make or, if already made, will withdraw this recommendation and motion.

C. Sentencing Recommendations

The United States Probation Office will prepare the defendant's pre-sentence report in which it will include a recommended calculation of the defendant's sentence range under the U.S.S.G. Both the United States and the defendant will have the opportunity to argue in support of or in opposition to the guideline sentence range calculation the U.S.P.O. recommends, as well as present evidence in support of their respective sentencing arguments.

The parties are free to recommend to the Court their respective positions on the appropriate sentence to be imposed in this case based on the stipulated facts set forth in Section II.C, any additional facts established at the imposition of sentence hearing, the applicable statutory penalty sections, the advisory U.S.S.G., and the sentencing factors set forth in 18 U.S.C. § 3553.

IV. ADDITIONAL AGREEMENTS BY UNITED STATES

In exchange for the defendant's guilty plea and the Court's acceptance of the defendant's plea and the terms of this agreement, the United States agrees that it will not prosecute the defendant further for any other offense – now known – arising out of the subject of the investigation related to the charges brought in the Indictment in this case and the defendant's admissions set forth in Section II.C.

Provided, however, if the defendant's guilty plea or sentence is/are rejected, withdrawn, vacated, reversed, set aside, or modified, at any time, in any proceeding, for any reason, the United States will be free to prosecute the defendant on all charges arising out of the investigation of this case including any charges dismissed pursuant to the terms

of this agreement, which charges will be automatically reinstated as well as for perjury and false statements. The defendant hereby agrees that he/she waives any defense that the statute of limitations bars the prosecution of such a reinstated charge.

V. WAIVER OF TRIAL RIGHTS, APPELLATE RIGHTS, COLLATERAL ATTACK RIGHTS, CLAIM FOR ATTORNEY FEES AND COSTS, AND RULE 410

A. Trial Rights

Being aware of the following, the defendant waives these trial rights:

- If pleading to an Information, the right to have the charges presented to the grand jury prior to entering the guilty plea;
- The right to a speedy and public trial by jury on the factual issues establishing guilt or any fact affecting the mandatory minimum and statutory penalties, and any issue affecting any interest in any assets subject to forfeiture;
- The right to object to the composition of the grand or trial jury;
- The right to plead not guilty or to persist in that plea if it has already been made;
- The right to be presumed innocent and not to suffer any criminal penalty unless and until the defendant's guilt is established beyond a reasonable doubt;
- The right to be represented by counsel at trial and if necessary to have a counsel appointed at public expense to represent the defendant at trial –

the defendant is not waiving the right to have counsel continue to represent the defendant during the sentencing phase of this case;

- The right to confront and cross examine witnesses against the defendant, and the right to subpoena witnesses to appear in the defendant's behalf;
- The right to remain silent at trial, with such silence not to be used against the defendant, and the right to testify in the defendant's own behalf; and
- The right to contest the validity of any searches conducted on the defendant's property or person.

B. Appellate Rights

The defendant waives the right to appeal the conviction(s) resulting from the entry of guilty plea(s) to the charges set forth in this agreement. The defendant further agrees that if the Court imposes a sentence that does not exceed the statutory maximum penalties – as set forth in Section II.D above in this agreement, the defendant waives without exception the right to appeal on all grounds contained in 18 U.S.C. § 3742 the sentence the Court imposes. The defendant understands that this waiver includes, but is not limited to, forfeiture (if applicable), terms or conditions of probation (if applicable) or supervised release, any fines or restitution, and any and all constitutional (or legal) challenges to defendant's conviction(s) and guilty plea[s], including arguments that the statute(s) to which defendant is pleading guilty (is/are) unconstitutional, and any and all claims that the statement of facts provided herein is insufficient to support defendant's plea[s] of guilty.

The defendant agrees that the appellate and collateral attack waivers contained within this agreement will apply to any 18 U.S.C. § 3582(c) modifications, as well as the district court's decision to deny any such modification.

Should the defendant file a notice of appeal in violation of this agreement, it will constitute a material breach of the agreement. The government is free to reinstate any dismissed charges, and withdraw any motions for downward departures, or sentences below the mandatory minimum made pursuant to 18 U.S.C. § 3553(e).

C. Collateral Attack Rights

The defendant agrees to waive all rights to collaterally attack the resulting conviction(s) and/or sentence – including forfeiture (if applicable) or terms or conditions of probation (if applicable) or supervised release, and any fines or restitution – the Court imposes. The only exceptions to this collateral attack waiver are as follows: 1) any challenge to the conviction or sentence alleging ineffective assistance of counsel – based on information not now known to the defendant and which, in the exercise of reasonable diligence, could not be known by the defendant at the time the Court imposes sentence; and 2) a challenge to the voluntariness of the defendant's guilty plea(s).

D. Claim for Attorney Fees and Costs

Because this is a negotiated resolution of the case, the parties waive any claim for the award of attorney fees and costs from the other party.

E. Evidence Rule 410 and Fed. R. Crim. P. 11(f)

By signing this agreement, the defendant admits the truth of the facts in the Factual Basis portion of this agreement set forth in Section II.C. The defendant agrees

that the statements made by him in signing this agreement shall be deemed usable and admissible against the defendant as stipulations in any hearing, trial or sentencing that may follow. The foregoing provision acts as a modification, and express waiver, of Federal Rule of Evidence 410 and Federal Rule of Criminal Procedure 11(f), and is effective upon the defendant's in-court admission to the factual basis supporting the plea(s). This provision applies regardless of whether the court accepts this plea agreement.

VI. ADEQUACY OF THE AGREEMENT

Pursuant to Local Criminal Rule 11.2(d)(7) and (8), this plea agreement is appropriate in that it conforms with the sentencing goals that would otherwise be applicable to the defendant's case if the defendant had gone to trial and had been convicted on all counts in the charging instrument.

VII. THE DEFENDANT'S ACCEPTANCE OF THE TERMS OF THIS PLEA AGREEMENT

I, Kenneth Currin Schuchman, the defendant, affirm this document contains all of the agreements made between me – with the assistance of my attorney – and the United States regarding my plea(s). There are no other promises, assurances, or agreements the United States has made or entered into with me that have affected my decision to enter any plea of guilty or to enter into this agreement. If there are any additional promises, assurances, or agreements, United States and I will jointly inform the Court in writing before I enter my guilty plea.

I understand that no one, including my attorney, can guarantee the outcome of my case or what sentence the Court may impose if I plead guilty. If anyone, including my attorney, has done or said anything other than what is contained in this agreement, I will inform the Court when I stand before it to enter my plea.

I enter into this agreement understanding and agreeing that the conditions set forth herein are obligatory and material to this agreement and that any failure on my part to fulfill these obligations will constitute a material breach of this agreement. If I breach this agreement, I agree the United States, in its sole discretion, may withdraw from this agreement and may reinstate prosecution against me on any charges arising out of the investigation in this matter. If my compliance with the terms of this plea agreement becomes an issue, at an appropriate hearing, during which I agree any of my disclosures will be admissible, the Court will determine whether or not I have violated the terms of this agreement. I understand the government's burden to prove a breach will be by a preponderance of the evidence.

I understand the Court will ask me under an oath to answer questions about the offense to which I am pleading guilty and my understanding of this plea agreement. I understand that I may be prosecuted if I make false statements or give false answers and may suffer other consequences set forth in this agreement.

I have read this plea agreement carefully and understand it thoroughly. I know of no reason why the Court should find me incompetent to enter into this agreement or to enter my plea. I enter into this agreement knowingly and voluntarily. I understand that anything that I discuss with my attorney is privileged and confidential, and cannot be

revealed without my permission. Knowing this, I agree that this document will be filed with the Court.

I am fully satisfied with the representation given me by my attorney and am prepared to repeat this statement at the time I stand before the Court and enter my guilty plea. My attorney and I have discussed all possible defenses to the charge to which I am pleading guilty. My attorney has investigated my case and followed up on any information and issues I have raised to my satisfaction. My attorney has taken the time to fully explain the legal and factual issues involved in my case to my satisfaction. We have discussed the statute applicable to my offense and sentence as well as the possible effect the U.S.S.G. may have on my sentence.

Based on my complete understanding of this plea agreement, I therefore admit that I am guilty of Count 1 of the Indictment - Aiding and Abetting Computer Intrusions, in violation of 18 U.S.C. § 1030, and admit the forfeiture allegation of the Indictment in their entirety.

DATED: 09/03/19

KENNETH CURRIN SCHUCHMAN
Defendant

As counsel for the defendant, I have conveyed all formal plea offers. I have discussed the terms of this plea agreement with the defendant, have fully explained the charge(s) to which the defendant is pleading guilty, the necessary elements thereto, all possible defenses, and the consequences of a guilty plea to a felony. Based on these discussions, I have no reason to doubt that the defendant is knowingly and voluntarily entering into this agreement and entering a plea of guilty. I know of no reason to question the defendant's competence to make these decisions. If, prior to the imposition of sentence, I become aware of any reason to question the defendant's competency to enter into this plea agreement or to enter a plea of guilty, I will immediately inform the court.

DATED: 9/3/19

BARRY L. FLEGENHEIMER
Attorney for Kenneth C. Schuchman

On behalf of the United States, the following accepts the defendant's offer to plead guilty under the terms of this plea agreement.

DATED: 9/3/19

BRYAN SCHRODER
United States of America
United States Attorney