ATTACHMENT A
STIPULATION OF FACTS

The undersigned parties stipulate and agree that if this case had proceeded to trial, the Prosecuting Offices would have proven the following facts beyond a reasonable doubt. The undersigned parties also stipulate and agree that the following facts do not encompass all of the evidence that would have been presented had this matter proceeded to trial.

Phobos Ransomware Conspiracy

Beginning no later than in or around November 2020, and continuing through May 2024, in the District of Maryland and elsewhere, the defendant, **EVGENII PTITSYN** ("**PTITSYN**"), did knowingly and unlawfully conspire and agree with others, to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises—to wit, to use access credentials without authorization to remotely access the networks of public and private entities ("Victims") in order to encrypt Victims' files for the purpose of extorting ransom payments—and to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, and sounds in furtherance of such scheme and artifice, in violation of Title 18, United States Code, Sections 1343 and 1349.

The objects of the conspiracy involving **PTITSYN** and co-conspirators were to: (i) distribute the Phobos ransomware to other co-conspirators; (ii) gain unauthorized access to Victims' computers; (iii) copy and steal data from Victims' computers; (iv) install and execute the Phobos ransomware on Victims' computers, resulting in the encryption of data on the computers; (v) extort Victims by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data; (vi) threaten to release stolen data if the ransom was not paid; (vii) collect ransom payments from Victims; (viii) charge other co-conspirators $300 per decryption key to regain access to encrypted files of Victims; and (viii) distribute Phobos ransomware decryption key payments and ransom proceeds to **PTITSYN** and other co-conspirators.

PTITSYN, a Russian national residing outside the United States, and others joined and ultimately administered a cybercrime group using "Phobos ransomware," a sophisticated malware that infected a computer by targeting vulnerabilities in remote desktop protocol and encrypted some or all of the data on the computer using file extensions such as ".devil," ".devos," ".help," ".phobos," and ".eight." In a Phobos ransomware attack, the co-conspirators hacked into the Victims' computer networks, often using stolen or otherwise unauthorized credentials; copied and stole files and programs on the Victims' networks; and encrypted the original versions of the stolen data on the Victims' networks by installing and executing the Phobos ransomware, to prevent the Victims from accessing or using the data on the compromised networks. Once data on a computer was encrypted, distributors of the malware could then extort Victims by demanding a ransom in exchange for the decryption key needed to regain access to the encrypted data on the computer.

To extort victims, the Phobos ransomware co-conspirators left ransom notes on compromised Victim computers in the form of files. In the ransom notes, the co-conspirators typically notified each Victim that all their files had been encrypted and that they must pay a ransom in Bitcoin for decryption. The notes directed each Victim to contact the co-conspirators at specified email addresses to negotiate the ransom payment in exchange for the co-conspirators providing the Victim with the decryption keys needed to restore their access to encrypted data. The co-conspirators often followed up with emails or phone calls to a Victim in which the co-conspirators threatened to sell or otherwise expose the Victim's stolen data if the Victim refused to pay the ransom. The co-conspirators also threatened to expose Victims' stolen files to the public or to the Victims' clients, customers, or constituents if the ransoms were not paid. The Victims also suffered additional losses resulting from Phobos ransomware attacks, including lost business revenue and remediation costs.

The administrators of the Phobos ransomware operated a darknet website to coordinate the sale and distribution of the Phobos ransomware to co-conspirators. The administrators offered the Phobos ransomware for free to co-conspirators acting as "affiliates" of the ransomware. After a successful Phobos ransomware attack, affiliates paid $300 to the Phobos administrators for a decryption key that could be provided to Victims to regain access to the encrypted files. Each deployment of Phobos ransomware was assigned a unique alphanumeric string in order to match it to the corresponding decryption key, and each affiliate was directed to pay the $300 decryption key fee to a cryptocurrency wallet unique to that affiliate.

It was further part of the conspiracy that the co-conspirators collected payments in Bitcoin from Victims that paid ransoms and distributed the proceeds amongst themselves.

PTITSYN's Role in Scheme

PTITSYN's support of the Phobos ransomware conspiracy began at least as early as on or about April 4, 2019, when a message was posted on Zloy, a well-known Russian language cybercriminal forum, titled "PhobosCrypt," that sought to recruit affiliates to the Phobos ransomware group. The post directed interested parties to contact a Jabber account, shipuer@xmpp.jp, that **PTITSYN** controlled. **PTITSYN** then furthered the Phobos ransomware conspiracy by recruiting Phobos ransomware affiliates that operated under multiple identifiers. **PTITSYN** also worked with a prolific Phobos ransomware affiliate that operated under multiple identifiers, including affiliate number 2803. **PTTITSYN** would customize the underlying ransomware code to provide different "builds" for Affiliate 2803, which would then provide information to the victim as to which affiliate to contact for ransom negotiations. **PTITSYN** and others were responsible for dozens of ransomware attacks against U.S. victims, including health care companies, hospitals, educational institutions, and providers of essential services. Among other things, **PTITSYN** facilitated financial transactions for individuals affiliated with Phobos.

From January 2022 to the time of **PTITSYN**'s arrest in South Korea on May 15, 2024, **PTITSYN** assumed a leadership role in the Phobos ransomware conspiracy by acting as an administrator of the Phobos ransomware variant. As an administrator, **PTITSYN** possessed and controlled multiple Phobos administrator cryptocurrency wallets that received thousands of $300 decryption key fees from affiliates who used the Phobos ransomware to exploit victims. **PTITSYN** received 25 percent of the decryption key payment, and at times, **PTITSYN** also received a portion of the ransomware payments made by victims.

PTITSYN also gained control of the primary Jabber accounts—derxan@xmpp.jp and zimmermanx@xmpp.jp—that administrators of the Phobos ransomware variant used to advertise their ransomware on criminal forums and to communicate with potential co-conspirators. **PTITSYN** also used these Jabber accounts to transmit ransomware code for the Phobos affiliates. In addition, in or around February 2024, **PTITSYN**, using Telegram, corresponded with a Phobos ransomware affiliate about a ransomware attack against a U.S. educational institution that reported losses exceeding $4 million. **PTITSYN** and administrators also operated a darknet website to coordinate the sale and distribution of the Phobos ransomware to co-conspirators.

In total, **PTITSYN** and other members of the Phobos ransomware conspiracy launched ransomware attacks against more than 1,000 victims around the world, including at least 890 victims located in the United States. Through these attacks, the co-conspirators have successfully extorted various amounts of Bitcoin from Victims that—measured at the time the ransoms were paid—totaled more than approximately $30 million. Victims have also suffered additional actual losses of at least $9.3 million from Phobos ransomware attacks, including losses associated with responding to the offense, remediation, and costs and losses associated with the disruption of services.

Additional Overt Acts

In furtherance of the conspiracy, and to effect the objects of the conspiracy, **PTITSYN** or one of the co-conspirators performed and caused to be performed the following overt acts in the District of Maryland and elsewhere:

Victim A

In or around November 2020, one or more co-conspirators accessed the computer network of a Maryland-based company that provided accounting and consulting services to federal agencies ("Victim A"), deployed the Phobos ransomware on its computers, including computers located in the District of Maryland, and caused the encryption of Victim A's data, all without Victim A's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim A pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data. In or around February 2021, one or more co-conspirators provided Victim A with decryption keys in exchange for Victim A's payment of a ransom in Bitcoin that was then equivalent to approximately $12,000.

Victim B

In or around December 2021, one or more co-conspirators accessed the computer network of a Maryland-based managed services company ("Victim B"). At or around the same time, one or more co-conspirators deployed the Phobos ransomware on Victim B's computers, including computers located in the District of Maryland, and caused the encryption of Victim B's data, all without Victim B's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim B pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data. At or around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim B's computers if Victim B did not pay the ransom.

Victim C

In or around July 2022, one or more co-conspirators accessed the computer network of a Maryland-based healthcare provider ("Victim C"), deployed the Phobos ransomware on its computers, including computers located in the District of Maryland, and caused the encryption of Victim C's data, all without Victim C's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim C pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data. At or around the same time, one or more co-conspirators provided Victim C with decryption keys in exchange for Victim C's payment of a ransom in Bitcoin that was then equivalent to approximately $25,000.

Victim D

In or around August 2022, one or more co-conspirators accessed the computer network of another Maryland-based healthcare provider ("Victim D"), deployed the Phobos ransomware on its computers, including computers in the District of Maryland, and caused the encryption of Victim D's data, all without Victim D's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim D pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data. At or around the same time, one or more co-conspirators transmitted a threat to publicly publish or otherwise expose data stolen from Victim D's computers if Victim D did not pay the ransom. At or around the same time, one or more co-conspirators provided Victim D with decryption keys in exchange for Victim D's payment of a ransom in Bitcoin that was then equivalent to approximately $37,000.

Victim E

In or around October 2023, one or more co-conspirators accessed the computer network of another Maryland-based healthcare provider ("Victim E"), deployed the Phobos ransomware on its computers, including computers in the District of Maryland, and caused the encryption of Victim E's data, all without Victim E's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim E pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data. At or around the same time, one or more co-conspirators provided Victim E with decryption keys in exchange for Victim E's payment of a ransom in Bitcoin that was then equivalent to approximately $2,300.

Victim F

In or around January 2024, one or more co-conspirators accessed the computer network of a Maryland-based educational institution, deployed ransomware on its computers, and caused the encryption of Victim F's data, all without Victim F's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim F pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

Victim G

In or around April 2022, one or more co-conspirators accessed the computer network of a Pennsylvania-based healthcare company ("Victim G"), deployed ransomware on its computers, and caused the encryption of Victim G's data, all without Victim G's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim G pay a ransom in Bitcoin worth $70,000 in exchange for decryption keys for the encrypted data. At or around the same time, one or more co-conspirators provided Victim G with decryption keys in exchange for Victim G's payment of a ransom in Bitcoin that was then equivalent to approximately $20,000.

Victim H

In or around May 2022, one or more co-conspirators accessed the computer network of an Arizona-based marketing and data analytics firm ("Victim H"), deployed ransomware on its computers, and caused the encryption of Victim H's data, all without Victim H's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim H pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data. At or around the same time, one or more co-conspirators provided Victim H with decryption keys in exchange for Victim H's payment of a ransom in Bitcoin that was then equivalent to approximately $40,000.

Victim I

In or around July 2022, one or more co-conspirators accessed the computer network of a New York–based law enforcement union ("Victim I"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim I's data, all without Victim I's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim I pay a ransom in Bitcoin worth $25,000 in exchange for decryption keys for the encrypted data, and transmitted a threat to publish or otherwise expose data stolen from Victim I's computers if Victim I did not pay the ransom.

Victim J

In or around July 2022, one or more co-conspirators accessed the computer network of a federally recognized tribe ("Victim J"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim J's data, all without Victim J's permission. Victim J reported that the attack affected dozens of computer servers, and approximately 2.6 million files. One or more coconspirators transmitted a demand that Victim J pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

Victim K

In or around July 2023, one or more co-conspirators accessed the computer network of a Connecticut-based public school system ("Victim K"), deployed ransomware on its computers, and caused the encryption of Victim K's data, all without Victim K's permission.

At or around the same time, one or more co-conspirators transmitted at demand that Victim K pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data, and transmitted a threat to publish or otherwise expose data stolen from Victim K's computers if Victim K did not pay the ransom.

Victim L

In or around August 2022, one or more co-conspirators accessed the computer network of an Illinois-based contractor for the U.S. Department of Defense and the U.S. Department of Energy ("Victim L"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim L's data, all without Victim L's permission, and transmitted a demand that Victim L pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

Victim M

In or around May 2023, one or more co-conspirators accessed the computer network of an Ohio-based automotive company ("Victim M"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim M's data, all without Victim M's permission. In or around May and June 2023, one or more co-conspirators transmitted a demand that Victim M pay a ransom in Bitcoin worth $800,000 in exchange for decryption keys for the encrypted data, and transmitted a threat to publish or otherwise expose data stolen from Victim M's computers if Victim M did not pay the ransom.

Victim N

In or around June 2023, one or more co-conspirators accessed the computer network of a California-based public school system ("Victim N"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim N's data, all without Victim N's permission. One or more co-conspirators transmitted a demand that Victim N pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data, and did transmit a threat to publish or otherwise expose data stolen from Victim N's computers if Victim N did not pay the ransom. To obtain a decryption key, Victim N paid a ransom in Bitcoin that was then equivalent to approximately $300,000.

Victim O

In or around September 2023, one or more co-conspirators accessed the computer network of a North Carolina-based children's hospital ("Victim O"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim O's data, all without Victim O's permission. At or around the same time, one or more co-conspirators transmitted a demand that Victim O pay a ransom worth $300,000 in Bitcoin in exchange for decryption keys for the encrypted data. One or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from

Victim O's computers if Victim O did not pay the ransom. To obtain a decryption key, Victim O paid a ransom in Bitcoin that was then equivalent to approximately $100,000.

SO STIPULATED:

Digitally signed by
THOMAS SULLIVAN
Date: 2026.02.10
13:00:03 -05'00'

2/10/26
Dated

Thomas M. Sullivan
Assistant United States Attorney

Frank Lin, Senior Counsel
Computer Crime and Intellectual Property
Section, Department of Justice

2/11/2026
Dated

Evgenii Ptitsyn
Defendant

3/4/26
Dated

Paul W. Verner, Esquire
Counsel for Defendant

3/4/26
Dated

Artie McConnell, Esquire
Counsel for Defendant