AF Approval SN Chief Approval CAB

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

UNITED STATES OF AMERICA

v. CASE NO. 6:25-cr- 00005-JSS-DCI

MICHAEL SCHEUER

PLEA AGREEMENT

Pursuant to Fed. R. Crim. P. 11(c), the United States of America, by Roger B. Handberg, United States Attorney for the Middle District of Florida, and the defendant, Michael Scheuer, and the attorney for the defendant, David Haas, Esq., mutually agree as follows:

A. Particularized Terms

1. Count(s) Pleading To

The defendant shall enter a plea of guilty to Counts One and Two of the Information. Count One charges the defendant with knowingly transmitting a program, information, code, and command and intentionally causing damage without authorization to a protected computer, and the defendant's course of conduct resulting in an aggregate loss to persons of at least $5,000 in a one-year period, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B). Count Two charges the defendant with aggravated identity theft, in violation of 18 U.S.C. § 1028A.

2. Minimum and Maximum Penalties

Count One carries a maximum sentence of ten years' imprisonment; a maximum fine of $250,000, or twice the gross gain caused by the offense, or twice the gross loss caused by the offense, whichever is greater; a term of supervised release of not more than three years; and a special assessment of $100. Count Two carries a mandatory sentence of two years' imprisonment to be served consecutively to any term of imprisonment for Count One; a fine of $250,000, or twice the gross gain caused by the offense, or twice the gross loss caused by the offense, whichever is greater; a term of supervised release of not more than one year; and a special assessment of $100. With respect to certain offenses, the Court shall order the defendant to make restitution to any victim of the offense(s), and with respect to other offenses, the Court may order the defendant to make restitution to any victim of the offense(s), or to the community, as set forth below.

3. *Apprendi v. New Jersey*

Under *Apprendi v. New Jersey*, 530 U.S. 466 (2000), a maximum sentence of ten years may be imposed for Count One because the following facts have been admitted by the defendant and are established by this plea of guilty: the defendant caused loss to one or more persons during any one-year period aggregating at least $5,000 in value. Namely, between the months of June, through September 2024, the defendant caused losses to Company A and Company B, which exceeded $5,000 in value.

Defendant's Initials MJ

4. Elements of the Offense(s)

The defendant acknowledges understanding the nature and elements of the offense with which defendant has been charged and to which defendant is pleading guilty. The elements of Count One are:

First: the defendant knowingly transmitted a program, information, code, or command to a protected computer;

Second: in doing so, the defendant intentionally caused damage without authorization to a protected computer; and

Third: the damage resulted in losses of more than $5,000 during a one-year period.

The elements of Count Two are:

First: the defendant knowingly transferred, possessed, or used another person's means of identification;

Second: the defendant did so without lawful authority;

Third: the defendant did so during and in relation to the crime of knowingly transmitting a program, information, code, and command and intentionally causing damage without authorization to a protected computer, and resulting in an aggregate loss of at least $5,000 in a one-year period, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B); and

Fourth: the defendant did so despite knowing that the individual whose means of information the defendant transferred, possessed, or used was an actual person.

5. Indictment Waiver

Defendant will waive the right to be charged by way of indictment before a federal grand jury.

6. No Further Charges

If the Court accepts this plea agreement, the United States Attorney's Office for the Middle District of Florida agrees not to charge defendant with committing any other federal criminal offenses known to the United States Attorney's Office at the time of the execution of this agreement, related to the conduct giving rise to this plea agreement.

7. Mandatory Restitution to Victim of Offense of Conviction

Pursuant to 18 U.S.C. § 3663A(a) and (b), defendant agrees to make full restitution to the victims of his offenses of conviction.

8. Guidelines Sentence

Pursuant to Fed. R. Crim. P. 11(c)(1)(B), the United States will recommend to the Court that the defendant be sentenced within the defendant's applicable guidelines range as determined by the Court pursuant to the United States Sentencing Guidelines, as adjusted by any departure the United States has agreed to recommend in this plea agreement. The parties understand that such a recommendation is not binding on the Court and that, if it is not accepted by this Court, neither the United States nor the defendant will be allowed to withdraw from the plea agreement, and the defendant will not be allowed to withdraw from the plea of guilty.

9. Acceptance of Responsibility - Three Levels

At the time of sentencing, and in the event that no adverse information is received suggesting such a recommendation to be unwarranted, the United States will

recommend to the Court that the defendant receive a two-level downward adjustment for acceptance of responsibility, pursuant to USSG § 3E1.1(a). The defendant understands that this recommendation or request is not binding on the Court, and if not accepted by the Court, the defendant will not be allowed to withdraw from the plea.

Further, at the time of sentencing, if the defendant's offense level prior to operation of subsection (a) is level 16 or greater, and if the defendant complies with the provisions of USSG § 3E1.1(b) and all terms of this Plea Agreement, including but not limited to, the timely submission of the financial affidavit referenced in Paragraph B.5., the United States agrees to move pursuant to USSG § 3E1.1(b) for a downward adjustment of one additional level. The defendant understands that the determination as to whether the defendant has qualified for a downward adjustment of a third level for acceptance of responsibility rests solely with the United States Attorney for the Middle District of Florida, and the defendant agrees that the defendant cannot and will not challenge that determination, whether by appeal, collateral attack, or otherwise.

10. Forfeiture of Assets

The defendant agrees to forfeit to the United States immediately and voluntarily any and all assets and property, or portions thereof, subject to forfeiture, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), whether in the possession or control of the United States, the defendant or defendant's nominees.

The assets to be forfeited specifically include, but are not limited to, the following: Corsair desktop computer tower, Serial No. 030422135716, which was seized from the defendant's residence on September 23, 2024, which asset was used to commit or to facilitate the commission of the offense.

The defendant agrees and consents to the forfeiture of these assets pursuant to any federal criminal, civil judicial, or administrative forfeiture action. The defendant also agrees to waive all constitutional, statutory, and procedural challenges (including direct appeal, habeas corpus, or any other means) to any forfeiture carried out in accordance with this Plea Agreement on any grounds, including that the forfeiture described herein constitutes an excessive fine, was not properly noticed in the charging instrument, addressed by the Court at the time of the guilty plea, announced at sentencing, or incorporated into the judgment.

The defendant admits and agrees that the conduct described in the Factual Basis below provides a sufficient factual and statutory basis for the forfeiture of the property sought by the government. Pursuant to Rule 32.2(b)(4), the defendant agrees that the preliminary order of forfeiture will satisfy the notice requirement and will be final as to the defendant at the time it is entered. In the event the forfeiture is omitted from the judgment, the defendant agrees that the forfeiture order may be incorporated into the written judgment at any time pursuant to Rule 36.

The defendant agrees to take all steps necessary to identify and locate all property subject to forfeiture and to transfer custody of such property to the United

States before the defendant's sentencing. The defendant agrees to be interviewed by the government, prior to and after sentencing, regarding such assets and their connection to criminal conduct. The defendant further agrees to be polygraphed on the issue of assets, if it is deemed necessary by the United States. The defendant agrees that Federal Rule of Criminal Procedure 11 and USSG § 1B1.8 will not protect from forfeiture assets disclosed by the defendant as part of the defendant's cooperation.

The defendant agrees to take all steps necessary to assist the government in obtaining clear title to the forfeitable assets before the defendant's sentencing. In addition to providing full and complete information about forfeitable assets, these steps include, but are not limited to, the surrender of title, the signing of a consent decree of forfeiture, and signing of any other documents necessary to effectuate such transfers. To that end, the defendant agrees to make a full and complete disclosure of all assets over which defendant exercises control directly or indirectly, including all assets held by nominees, to execute any documents requested by the United States to obtain from any other parties by lawful means any records of assets owned by the defendant, and to consent to the release of the defendant's tax returns for the previous five years. The defendant agrees to be interviewed by the government, prior to and after sentencing, regarding such assets and their connection to criminal conduct.

The defendant agrees that the United States is not limited to forfeiture of the property specifically identified for forfeiture in this Plea Agreement. If the United States determines that property of the defendant identified for forfeiture cannot be

located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty; then the United States shall, at its option, be entitled to forfeiture of any other property (substitute assets) of the defendant up to the value of any property described above. The Defendant expressly consents to the forfeiture of any substitute assets sought by the Government. The defendant agrees that forfeiture of substitute assets as authorized herein shall not be deemed an alteration of the defendant's sentence.

Forfeiture of the defendant's assets shall not be treated as satisfaction of any fine, restitution, cost of imprisonment, or any other penalty the Court may impose upon the defendant in addition to forfeiture.

The defendant agrees that, in the event the Court determines that the defendant has breached this section of the Plea Agreement, the defendant may be found ineligible for a reduction in the Guidelines calculation for acceptance of responsibility and substantial assistance, and may be eligible for an obstruction of justice enhancement.

The defendant agrees that the forfeiture provisions of this plea agreement are intended to, and will, survive the defendant, notwithstanding the abatement of any underlying criminal conviction after the execution of this agreement. The forfeitability of any particular property pursuant to this agreement shall be determined as if the defendant had survived, and that determination shall be binding upon defendant's

heirs, successors and assigns until the agreed forfeiture, including satisfaction of any preliminary order of forfeiture for proceeds.

B. Standard Terms and Conditions

1. Restitution, Special Assessment and Fine

The defendant understands and agrees that the Court, in addition to or in lieu of any other penalty, shall order the defendant to make restitution to any victim of the offense(s), pursuant to 18 U.S.C. § 3663A, for all offenses described in 18 U.S.C. § 3663A(c)(1); and the Court may order the defendant to make restitution to any victim of the offense(s), pursuant to 18 U.S.C. § 3663, including restitution as to all counts charged, whether or not the defendant enters a plea of guilty to such counts, and whether or not such counts are dismissed pursuant to this agreement. The defendant further understands that compliance with any restitution payment plan imposed by the Court in no way precludes the United States from simultaneously pursuing other statutory remedies for collecting restitution (28 U.S.C. § 3003(b)(2)), including, but not limited to, garnishment and execution, pursuant to the Mandatory Victims Restitution Act, in order to ensure that the defendant's restitution obligation is satisfied.

On each count to which a plea of guilty is entered, the Court shall impose a special assessment pursuant to 18 U.S.C. § 3013. This special assessment is due on the date of sentencing. The defendant understands that this agreement imposes no limitation as to fine.

Defendant's Initials _____

2. Supervised Release

The defendant understands that the offenses to which the defendant is pleading provide for imposition of a term of supervised release upon release from imprisonment, and that, if the defendant should violate the conditions of release, the defendant would be subject to a further term of imprisonment.

3. Immigration Consequences of Pleading Guilty

The defendant has been advised and understands that, upon conviction, a defendant who is not a United States citizen may be removed from the United States, denied citizenship, and denied admission to the United States in the future.

4. Sentencing Information

The United States reserves its right and obligation to report to the Court and the United States Probation Office all information concerning the background, character, and conduct of the defendant, to provide relevant factual information, including the totality of the defendant's criminal activities, if any, not limited to the counts to which the defendant pleads, to respond to comments made by the defendant or the defendant's counsel, and to correct any misstatements or inaccuracies. The United States further reserves its right to make any recommendations it deems appropriate regarding the disposition of this case, subject to any limitations set forth herein, if any.

5. Financial Disclosures

Pursuant to 18 U.S.C. § 3664(d)(3) and Fed. R. Crim. P. 32(d)(2)(A)(ii), the defendant agrees to complete and submit to the United States Attorney's Office within

30 days of execution of this agreement an affidavit reflecting the defendant's financial condition. The defendant promises that his financial statement and disclosures will be complete, accurate, and truthful and will include all assets in which he has any interest or over which the defendant exercises control, directly or indirectly, including those held by a spouse, dependent, nominee, or other third party. The defendant further agrees to execute any documents requested by the United States needed to obtain from any third parties any records of assets owned by the defendant, directly or through a nominee, and, by the execution of this Plea Agreement, consents to the release of the defendant's tax returns for the previous five years. The defendant similarly agrees and authorizes the United States Attorney's Office to provide to, and obtain from, the United States Probation Office, the financial affidavit, any of the defendant's federal, state, and local tax returns, bank records, and any other financial information concerning the defendant, for the purpose of making any recommendations to the Court and for collecting any assessments, fines, restitution, or forfeiture ordered by the Court. The defendant expressly authorizes the United States Attorney's Office to obtain current credit reports in order to evaluate the defendant's ability to satisfy any financial obligation imposed by the Court.

6. Sentencing Recommendations

It is understood by the parties that the Court is neither a party to nor bound by this agreement. The Court may accept or reject the agreement, or defer a decision until it has had an opportunity to consider the presentence report prepared by the United

States Probation Office. The defendant understands and acknowledges that, although the parties are permitted to make recommendations and present arguments to the Court, the sentence will be determined solely by the Court, with the assistance of the United States Probation Office. The defendant further understands and acknowledges that any discussions between the defendant or the defendant's attorney and the attorney or other agents for the government regarding any recommendations by the government are not binding on the Court and that, should any recommendations be rejected, the defendant will not be permitted to withdraw the defendant's plea pursuant to this plea agreement. The government expressly reserves the right to support and defend any decision that the Court may make with regard to the defendant's sentence, whether or not such decision is consistent with the government's recommendations contained herein.

7. Defendant's Waiver of Right to Appeal the Sentence

The defendant agrees that this Court has jurisdiction and authority to impose any sentence up to the statutory maximum and expressly waives the right to appeal the defendant's sentence on any ground, including the ground that the Court erred in determining the applicable guidelines range pursuant to the United States Sentencing Guidelines, except (a) the ground that the sentence exceeds the defendant's applicable guidelines range as determined by the Court pursuant to the United States Sentencing Guidelines; (b) the ground that the sentence exceeds the statutory maximum penalty; or (c) the ground that the sentence violates the Eighth Amendment to the Constitution;

Defendant's Initials MJ

provided, however, that if the government exercises its right to appeal the sentence imposed, as authorized by 18 U.S.C. § 3742(b), then the defendant is released from his waiver and may appeal the sentence as authorized by 18 U.S.C. § 3742(a).

8. Middle District of Florida Agreement

It is further understood that this agreement is limited to the Office of the United States Attorney for the Middle District of Florida and cannot bind other federal, state, or local prosecuting authorities, although this office will bring the defendant's cooperation, if any, to the attention of other prosecuting officers or others, if requested.

9. Filing of Agreement

This agreement shall be presented to the Court, in open court or in camera, in whole or in part, upon a showing of good cause, and filed in this cause, at the time of defendant's entry of a plea of guilty pursuant hereto.

10. Voluntariness

The defendant acknowledges that defendant is entering into this agreement and is pleading guilty freely and voluntarily without reliance upon any discussions between the attorney for the government and the defendant and the defendant's attorney and without promise of benefit of any kind (other than the concessions contained herein), and without threats, force, intimidation, or coercion of any kind. The defendant further acknowledges the defendant's understanding of the nature of the offense or offenses to which the defendant is pleading guilty and the elements thereof, including the penalties provided by law, and the defendant's complete satisfaction with the

representation and advice received from the defendant's undersigned counsel (if any). The defendant also understands that the defendant has the right to plead not guilty or to persist in that plea if it has already been made, and that the defendant has the right to be tried by a jury with the assistance of counsel, the right to confront and cross-examine the witnesses against the defendant, the right against compulsory self-incrimination, and the right to compulsory process for the attendance of witnesses to testify in the defendant's defense; but, by pleading guilty, the defendant waives or gives up those rights, and there will be no trial. The defendant further understands that if the defendant pleads guilty, the Court may ask the defendant questions about the offense or offenses to which the defendant pleaded, and if the defendant answers those questions under oath, on the record, and in the presence of counsel (if any), the defendant's answers may later be used against the defendant in a prosecution for perjury or false statement. The defendant also understands that the defendant will be adjudicated guilty of the offenses to which the defendant has pleaded and, if any of such offenses are felonies, may thereby be deprived of certain rights, such as the right to vote, to hold public office, to serve on a jury, or to have possession of firearms.

11. Factual Basis

The defendant is pleading guilty because defendant is in fact guilty. The defendant certifies that the defendant does hereby admit that the facts set forth in the attached "Factual Basis," which is incorporated herein by reference, are true, and were

this case to go to trial, the United States would be able to prove those specific facts and others beyond a reasonable doubt.

12. Entire Agreement

This plea agreement constitutes the entire agreement between the government and the defendant with respect to the aforementioned guilty plea and no other promises, agreements, or representations exist or have been made to the defendant or the defendant's attorney with regard to such guilty plea.

13. Certification

The defendant and defendant's counsel certify that this plea agreement has been read in its entirety by (or has been read to) the defendant and that the defendant fully understands its terms.

DATED this 9 day of January, 2025.

ROGER B. HANDBERG
United States Attorney

Michael Scheuer
Defendant

Robert D. Sowell
Assistant United States Attorney

David Haas
Attorney for Defendant

Chauncey A. Bratt
Assistant United States Attorney
Deputy Chief, Orlando Division

Defendant's Initials MS

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

UNITED STATES OF AMERICA

v. CASE NO. 6:25-cr-

MICHAEL SCHEUER

PERSONALIZATION OF ELEMENTS

I. Count One

First: Did you knowingly transmit a program, information, code, or command to a protected computer?

Second: In doing so, did you intentionally cause damage without authorization to a protected computer?

Third: Did the damage result in losses of more than $5,000 during a one-year period?

II. Count Two

First: Did you knowingly transfer, possess, or use another person's means of identification, specifically victim A.G.'s email address or username?

Second: Did you do so without lawful authority?

Third: Did you do so during and in relation to the crime of knowingly transmitting a program, information, code, and command, and intentionally causing damage without authorization, to a protected computer?

Fourth: Did you do so despite knowing that A.G. was an actual person?

Defendant's Initials MS

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

UNITED STATES OF AMERICA

v. CASE NO. 6:25-cr-

MICHAEL SCHEUER

FACTUAL BASIS

From on or about June 12, 2024, through on or about September 23, 2024, the defendant Michael Scheuer ("SCHEUER") conducted a series of computer intrusions or attacks directed at a media and entertainment company operating in the Middle District of Florida ("Company A"). These intrusions are described below.

SCHEUER was previously an employee of Company A. His title was "Menu Production Manager," and his responsibilities included the creation and publishing of menus for Company A's portfolio of restaurants. He was thus substantially familiar with the online program used by Company A to create and manage its menus (hereinafter referred to as "Menu Creator"), the system architecture, and potential vulnerabilities within the system. SCHEUER was terminated from Company A on or about June 13, 2024.

A. Intrusion 1 - Menu Creator

In early July 2024, Company A was made aware of issues with Menu Creator. The Menu Creator program is from a third-party vendor, Company B, based out of Minnesota but with an office in the Middle District of Florida.

Upon investigation, it was determined that SCHEUER had accessed, and made several unauthorized changes to, Menu Creator that impacted the integrity of the system. These changes included replacing fonts in the application. The fonts were replaced with a different font appearance but retained the original font name. When launched, Menu Creator reached out to the configuration files to retrieve what it believed to be the correct font; instead, it retrieved the altered font files. These font changes propagated throughout the database resulting in each menu displaying the same generic font as opposed to the themed fonts applied to each menu. Further, this change caused the Menu Creator system to become inoperable while the font changes were pushed to all of the menus.

In addition to the font-related changes, SCHEUER also made changes to the menu images and backgrounds. These changes made it so that several of the menus were loading as blank white pages. Specifically, SCHEUER replaced the correct backgrounds and images with plain white backgrounds and images. As a result, the affected menus appeared as blank white screens because the Menu Creator system was pulling the new files.

Company A was forced to take the Menu Creator application offline while they reverted to backups to regain the ability to operate and restore to the last known good version of the system. The Menu Creator system was impacted for a period of 1-2 weeks and is no longer in use by Company A. As a result, Company A has moved to a manual menu approval and distribution process while a new system is developed.

Defendant's Initials MS

The investigation revealed that on July 3, 2024, SCHEUER utilized an administrator account within Menu Creator to create a new user account from IP address 146.70.187.158, which contained a fictitious name, Emily P. Beaman ("EPB"). This IP address resolved to Mullvad, a virtual private network ("VPN"). The credentials used in Intrusions 1 (as well as Intrusions 2 and 3, discussed below) were not specific to a user, rather, they were made for a specific job role and were available to multiple users. While SCHEUER knew these credentials as a result of his job responsibilities, upon his termination, he no longer had authorization to access the systems.

On July 4, 2024, one day after the creation of the EPB account, SCHEUER accessed Menu Creator through the EPB account and other accounts all from the same IP address. He then uploaded the altered font and background files. In total, there were approximately 70 uploads completed from this IP address. Each upload, in turn, contained multiple files. These altered files ultimately rendered the menus useless, forcing Company A to move to backups.

Shortly thereafter, Company A limited account access and implemented password resets, which ended SCHEUER's ability to enter Menu Creator. The IP address used in this attack was from the same IP range that SCHEUER used to logon to his Company A email account in the past, which was also a Mullvad IP address.

Further, to conduct this attack, SCHEUER utilized a URL to access the Menu Creator system. Typically, employees of Company A would authenticate their session

through a portal called [redacted] and were generally not familiar with the URL option. In this intrusion, SCHEUER accessed the system via URL, which was an option available to allow contractors (who were not employees of Company A and thus did not have [redacted] accounts) to access Menu Creator.

B. Intrusion 2 – SFTP Server 1 and Manipulation of Allergen Information

The next step in the menu workflow process was for approved menus to be transferred to 1 of 3 secure file transfer protocol servers ("SFTP servers"), all maintained by Company B. The SFTP servers each had their own specific purpose, but the overall functionality was to act as a print queue for menus ready to be printed and/or displayed on virtual menu screens.

SFTP Server 1 was the server utilized as a print queue for handheld menus. Importantly, menus cannot move directly from Menu Creator to Company B's printing process without being added to, and passing through, SFTP Server 1. Additionally, while files are typically routed to the SFTP server via the Menu Creator system, it is also possible for files to be uploaded to or downloaded directly from the SFTP server. In order to access SFTP Server 1, the user would need to enter a valid username and password combination in order to be authenticated on the server.

Upon investigation, it was determined that SCHEUER had committed an unauthorized intrusion into SFTP Server 1 after the forced password change on the Menu Creator application following Intrusion 1. As part of this intrusion, SCHEUER utilized a valid set of administrator credentials to gain access to SFTP Server 1. He

then downloaded a set of approved menus, which had been legitimately submitted by employees of Company A through Menu Creator and were waiting to be printed. Next, SCHEUER uploaded altered versions of those menus to the SFTP server. After these altered versions were uploaded, they entered the print queue.

Among the changes made by SCHEUER to the menus were changes to allergen information and pricing. As to the former, SCHEUER added notations to menu items indicating they were safe for people with specific allergies, which change could have had fatal consequences depending on the type and severity of a customer's allergy. The allergen alterations focused on peanut, tree nut, shellfish, and milk allergens.

Other changes were to wine lists within menus. Namely, SCHEUER altered information regarding wine regions and, for certain wines, changed their region to that of recent mass shootings. SCHEUER also imbedded or added images to one or more menus, including in one instance a swastika.

Some numbers of these altered menus were ultimately printed, though it is believed that all altered menus were identified and isolated prior to being shipped out to Company A restaurants and not otherwise distributed.

C. Intrusion 3 – SFTP Server 2

SFTP Server 2 was used by Company A itself for printing projects (i.e., it was not for printing by Company B). This server was specifically used by Company A to print menus that would be displayed on large boards outside of the respective restaurant. As with SFTP Server 1, menus cannot move directly from Menu Creator

to Company A's printing process without passing through SFTP Server 2. To be authenticated on SFTP Server 2, the user would have needed to enter a valid username and password combination, different from that of SFTP Server 1.

Upon investigation, it was determined that SCHEUER had committed a separate, unauthorized intrusion into SFTP Server 2. Specifically, SCHEUER downloaded menus from SFTP Server 2, altered them locally, and them uploaded them back to SFTP Server 2.

Among the changes made by SCHEUER to the menus were changes to QR codes, which direct users to a digital version of the menu. SCHEUER altered the QR codes so that users were directed to a website, boycott-israel.org, instead of the digital menus. The altered files were later printed by Company A but after learning of the intrusion, the printed menus were identified and isolated prior to being shipped out to restaurants and were not distributed further.

D. Denial-of-Service Attacks

Beginning on or about August 29, 2024, SCHEUER engaged in a cyberattack designed to continually lock employees of Company A out of their enterprise accounts. Namely, SCHEUER would enter on the login screen the respective victim's username or company email address along with an incorrect password and then launch repeated logon attempts. Initially, SCHEUER performed manual logon attempts but later shifted to a more sophisticated attack after developing a script to perform automated logon attempts.

These attacks were a form of a denial-of-service ("DoS") attacks. Specifically, the multiple incorrect logon attempts would cause an account to lockdown and thus render the account unusable until the attacks subsided and the passwords reset.

In total, SCHEUER attacked 14 employees of Company A as part of his DoS attacks. The victims of these attacks are identified by their initials as: DP, AG, DH, TS, MB, JV, PW, PT, AM, CS, JK, GH, MS, and SP. Many of these victims had previously had some type of interaction with SCHEUER while he was an employee of Company A.

As one example, on or about August 29, 2024, the defendant conducted a DoS attack with respect to Victim AG by entering AG's username/company email address into the login screen, coupled with an incorrect password, and launched multiple login attempts designed to, and ultimately succeeding in, locking down Victim AG's account.

As of September 23, 2024, SCHEUER had attempted over 100,000 logons to the victim accounts. As an example of the volume, on a single day, September 1, 2024, SCHEUER launched approximately 7,934 logon attempts across 4 different victim accounts.

FBI agents executed a search warrant of SCHEUER's residence on September 23, 2024, and the DoS attacks ceased minutes before the agents first made contact with SCHEUER and have not restarted following the seizure of his computer.

E. Intrusion Impacts

As a result of SCHEUER's actions within Menu Creator, nearly every menu in the system was impacted. The entire repository of menus had to be reverted to older versions and brought up to date manually. Additionally, as a result of SCHEUER's intrusion into the SFTP servers, numerous Company A restaurants and menu variations were impacted.

The losses to both Company A and Company B resulting from SCHEUER's conduct have included, but are not limited to, costs related to reprinting of menus that had been altered, investigating and responding to the intrusions, remediating the intrusions and damage to the systems, and other consequential damages. The parties agree that the losses to Company A and Company B are each, independently in excess of $5,000 in value and that such losses were incurred in less than a one-year period.

F. SCHEUER's Computer Setup

As a result of the September 23, 2024, execution of a search warrant of SCHEUER's residence, federal agents seized a total of 4 personal computers, which were imaged for further analysis.

One of the computers was a desktop computer, specifically a Corsair desktop computer tower, Serial No. 030422135716, located in SCHEUER's office space. An analysis of this computer showed that it had the "Mullvad" application installed. As noted, Mullvad was the VPN used in one or more of the intrusions. A VPN conceals

user information by encrypting their data and is thus often used by threat actors to obfuscate illegal activity.

The analysis also revealed several "virtual machines" on this computer. A virtual machine ("VM") is an image of an operating system, which can be virtually launched within an application on a physical computer; it is designed to create a layer of separation between the physical computer and the virtual environment. Specifically, the virtual machine software, combined with the image of an operating system, allows a user to operate another computer from within their physical computer.

In total, there were 4 relevant virtual environments located on the desktop computer. Encryption was present on each of the VMs, and SCHEUER used multiple layers of encryption to protect or mask evidence of his activities.

These VMs were specifically used to conduct the intrusions directed at Company A, and evidence of the intrusions was readily available on the VMs. For example, SCHEUER maintained "snapshots" of the VMs—an image of the VM at a particular point in time. One snapshot shows SCHEUER using the 146.70.187.158 IP address, which is the same address used in Intrusion 1, a login to Menu Creator from the EPB account, and a text file showing the file trees for the font list, background list, and images.

Another snapshot shows four Company A login screens, which in turn show login attempts to Victims AG, DP, DH, and MB, and a "Your account has been locked out" banner above each login screen.

Yet another snapshot shows a Google Chrome bookmark for the Company A login portal. Another bookmark was titled "sniipet," and linked to a piece of JavaScript code used in the DoS attack. Also shown was an application (login8.exe) that was used in the DoS attack.

The analysis of the VMs also showed a desktop folder titled, "dox." In this folder were 5 files, containing the personally identifiable information ("PII") of 4 of the DoS victims: DP, AG, TS, and DH. This PII was within reports that SCHEUER had purchased from a third-party website. There was also a report for a fifth individual (whose initials are DPR), determined to be the mother of Victim DP.

Separate from these reports, SCHEUER also maintained a document with the filename "dox.txt." This document contained personal details for Victim DP and DPR. This personal information included address information for DPR, links to parcel and tax information for DPR's property, and information related to email addresses and accounts created by SCHEUER using derivations of DPR's personal information.

G. October 22, 2024

On October 22, 2024, SCHEUER traveled to the residence of one of the DoS victims—Victim AG. In security camera footage from Victim AG's house, SCHEUER is seen arriving in his vehicle and parking in front of the house at approximately 10:45pm. SCHEUER is then seen exiting his vehicle, approaching the front door of the house, inspecting the label of a package by the front door, giving a thumbs up to the camera, and then walking back to his vehicle. SCHEUER then leaves in his

vehicle. This incident followed SCHEUER having received notice earlier in the day of a search warrant previously executed by federal agents on his Google account.

As a result of this incident, Company A provided security to Victim AG, including removing him from the home and placing him in a hotel.

H. Data Leak

In addition to the above, SCHEUER also leaked on the dark web the Menu Creator URL he used to commit Intrusion 1 and Menu Creator login information for numerous accounts.

The above is merely a summary of some of the events, some of the persons involved, and other information relating to this case. It does not include, nor is it intended to include, all the events, persons involved, or other information relating to this case.