United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED

Jun 01 2021

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

[redacted] and
SERAZHUDIN TAMIRLANOVICH AKTULAEV,

CR 21-0229 JD

DEFENDANT(S).

INDICTMENT

18 U.S.C. § 371 – Conspiracy; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud; 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B) – Obtaining Information from a Protected Computer; 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer to Obtain Value;
18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(A)(i)(I) – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer; 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft;
18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c) – Forfeiture Allegations

A true bill.

/s/ Foreperson of the Grand Jury
Foreman

Filed in open court this 1st day of

June 2021.

Clerk

Bail, $ ___No Bail _____

STEPHANIE M. HINDS (CABN 154284)
Acting United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. [redacted] and SERAZHUDIN TAMIRLANOVICH AKTULAEV, Defendants.	CASE NO. CR 21-0229 JD VIOLATIONS: 18 U.S.C. § 371 – Conspiracy; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud; 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B) – Obtaining Information from a Protected Computer; 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer to Obtain Value; 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(A)(i)(I) – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer; 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft; 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c) – Forfeiture Allegations SAN FRANCISCO VENUE

INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

1. [redacted] was a resident of the Russian Federation.

//

//

2. SERAZHUDIN TAMIRLANOVICH AKTULAEV was a resident of the Russian Federation.

3. Company A was a technology company that provided an online platform for freelance employment based in Santa Clara, California. Among other services, this company provided a means of posting job listings. As discussed below, the defendants and their co-conspirators created large numbers of fake user accounts to obtain access to Company A's platform and used those accounts to then send fictitious job invites to numerous legitimate Company A users. The job invites contained Microsoft Excel spreadsheets that contained malware which, upon opening, facilitated the harvesting of financial credentials of the conspirators' victims. The computer servers used by Company A in operating their platform, as well as many of the computers of the victim users of Company A, were located in the Northern District of California. The computer servers of Company A and the computers of the victim users were used to facilitate interstate and foreign commerce and communication, including by interstate and foreign electronic signals, and constituted "protected computers" as defined in Title 18, United States Code, Section 1030(e)(2)(B).

4. A "spear-phishing" message is a tailored and personalized email or other electronic communication designed to appear legitimate in order to induce the targeted recipient(s) to take a certain action—such as clicking on a link, or downloading or opening a file—to cause a victim's computer to be compromised by a hacker. Spear-phishing messages often include information that the hacker knows about the recipient(s) based on research or other sources of information about the intended victim.

5. Command and control (C2) domains are computers with which malware communicates to send and receive data and commands.

6. An SQL (Structured Query Language) managed database is a domain-specific language used in programming and designed for managing data held in a relational database management system.

7. Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

8. TVRAT (TeamViewer Remote Access Trojan) malware was designed to exploit a vulnerability in the popular remote administration tool TeamViewer to provide those distributing the TVRAT malware with remote control over the infected computer. Like other variants of malware,

TVRAT malware is used to send stolen data from a victim computer to a C2 domain, from which the stolen data can be collected and used by criminals to commit fraud or other criminal activity.

9. DarkVNC malware was different malware that was similar in functionality to TVRAT, except that instead of exploiting TeamViewer, it exploited the remote administration tool VNC Viewer to provide those distributing the DarkVNC malware with remote control over the infected computer.

10. A Virtual Private Server (VPS) runs on a physical server, but with its own copy of an operating system. A VPS is created by taking one massive server and partitioning it into several independent servers. Virtualization layers are then created to ensure each virtual environment appears as a standalone server. Each "virtual" server has the ability to run its own operating system, applications, and software.

COUNT ONE: (18 U.S.C. § 371 – Conspiracy)

11. Paragraphs 1 through 10 of this Indictment are re-alleged and incorporated as if fully set forth here.

12. Beginning at a time unknown to the Grand Jury, but no later than on or about at least May 2016, and continuing through to and including a date unknown, but at least through on or about November 2017, in the Northern District of California and elsewhere, the defendants,

[redacted] and
SERAZHUDIN TAMIRLANOVICH AKTULAEV,

did knowingly and willfully conspire and agree with each other and with others, to commit computer fraud and abuse, namely, (1) caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(I) and (c)(4)(A)(i)(VI); (2) with intent to defraud, accessed a protected computer used in interstate and foreign commerce without authorization and exceeding authorized access, and by means of such conduct furthered the below-described fraud and obtained something of value, in violation of 18 U.S.C. §§§ 1030(a)(4) and (c)(3)(A); and (3) intentionally accessed a protected computer without authorization, and thereby obtained information from a protected computer, and committed the offense for purposes of commercial advantage and private financial gain, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(i).

The Conspiracy and Scheme to Defraud

13. As part of the conspiracy and scheme to defraud, the defendants used the Internet to launch a sophisticated spear-phishing campaign targeting users of Company A, and others.

14. With respect to Company A, the defendants and their co-conspirators created large numbers of fake Company A user accounts to obtain access to Company A's platform.

15. They then used those accounts to send fictitious job invites to numerous legitimate users of Company A's platform to deceive the victims into opening the invites. The job invites all contained variously named Microsoft Excel spreadsheets that contained hidden malicious macros using the TVRAT malware. The malware was not apparent to users when they received and opened the spreadsheets.

16. When the spreadsheets were opened by the receiving users, the macros downloaded malware to the users' systems. The malware was programmed to automatically call out to a C2 server controlled by the defendants to harvest sensitive information of their victims. Through this process, the defendants collected the sensitive information, including means of identification and financial credentials, from the victim users that opened the malware.

17. The defendants stored and shared the information collected on an SQL database, that they created to manage the information. The defendant then used the stolen means of identification and financial information collected from the victims during the intrusions to initiate and complete fraudulent financial transactions using financial accounts of victims, obtaining funds from those victims.

18. In addition to the use of the TVRAT malware described above, the defendants used the Internet to spread a different malware variant, DarkVNC, to victims' computers. It appears these victims did not have a connection to Company A. As with the TVRAT malware, the DarkVNC malware was programmed to automatically call out to a different C2 server controlled by the defendants to harvest sensitive information, including means of identification and financial credentials, from the victim users that opened the malware. The defendants shared this information on shared documents and used the stolen means of identification and financial information collected from the victims to initiate and complete fraudulent financial transactions using financial accounts of victims, obtaining funds from those victims.

The Victims

19. Approximately 80,000 of Company A's users received the fake job invites. Additionally, at least 2,169 computers infected with the TVRAT malware were identified to have called back to the C2 server. Of that number, approximately 1,000 of those victim computers were in the United States, 46 of which were in the Northern District of California. In addition, at least 1,584 computers infected with the DarkVNC malware were identified to have called back to a separate C2 server with at least one victim residing in the Northern District of California.

The Manner and Means of Accomplishing the Conspiracy

20. In furtherance of the conspiracy, the defendants used the following manner and means to accomplish the object and purpose of the conspiracy:

a. Creating fake accounts on Company A's platform to gain the ability to send spear-phishing emails to the users of that platform;

b. Using malware, including TVRAT and DarkVNC, that could be transmitted to potential victims in order to gain unauthorized access to the computer(s) of the victims;

c. Concealing the TVRAT malware within seemingly legitimate emails with Microsoft Excel spreadsheets that contained macros, which when opened downloaded the malware on to the victim's computer;

d. Using VPSs to distribute the DarkVNC malware to additional victim computers;

e. Registering, creating, and administering C2 domains for the victim computers to call back to, allowing for the harvesting of the means of identification and financial credential of their victims; and

f. Using an SQL database, as well as shared documents, to store, manage, and share the means of identification and financial credentials of their victims, and then using those means of identification and financial credentials to initiate fraudulent transactions for financial gain and to fraudulent obtain things of value.

//

//

//

The Overt Acts

21. In furtherance of the conspiracy and to effect its objects, on or about the dates listed below, in the Northern District of California and elsewhere, AKTULAEV and [redacted] and others, committed the following overt acts, among others:

Fraud Scheme Involving TVRAT Malware and the Victim Users of Company A

a. On May 26, 2016, the defendants registered the C2 domain "pushatone.net" through a domain registrar, headquartered in Milwaukee, Wisconsin.

b. On June 6, 2016, the defendants registered the C2 domain "pushatone.net" with network service provider utilizing servers located in the United States, in Utah;

c. Between at least June 2016 and at least August 2016, the defendants registered and created at least 225 fake accounts to use Company A's platform and, in doing so, transmitted an interstate wire communication from outside the state of California to the servers of Company A, located in the Northern District of California;

d. Between at least June 2016 and at least February 2017, the defendants caused to be sent thousands of emails to users of Company A's platform that fraudulently contained a job invite that had a Microsoft Excel spreadsheet attached with a macro that enabled the TVRAT malware to be installed on victim computers, and caused victim users of Company A, many of whom resided in the Northern District of California, to click on the attachment, and unwittingly allow the malware to be installed on their computers. In one such instance, on or about November 29, 2016, a victim user of Company A, Victim 1, clicked on the fake job invite and attached spreadsheet;

e. Between at least June 2016 and at least February 2017, the defendants controlled and administered the C2 domain to call to computers infected by the malware they distributed through their fraudulent emails. For example, Victim 1's computer beaconed back to the C2 domain between November 29 and December 25, 2016;

f. Between at least June 2016 and February 2017, through the above-described fraud scheme, the defendants controlled and administered the C2 domain to collect and harvest the means of identification and financial credentials of thousands of victims, many of whom resided in the Northern District of California;

g. Between at least June 2016 and February 2017, the defendant created, managed, and shared an SQL database to log the harvested financial credentials and means of identification of their victims.

Fraud Scheme Involving DarkVNC Malware and Additional Victims

h. On or about July 25, 2016, the defendant leased several VPSs through a VPS hosting company, using servers in New York.

i. On or about May 9, 2017, the defendants registered the C2 domain with a cloud computing and web services company, with servers located in the Netherlands.

j. The defendants used the virtual VPSs to distribute a file named "apivn.exe," determined to be the malware variant DarkVNC, to a number of victim computers.

k. Between May 2017 and at least November 2017, through the above-described fraud scheme, the defendants controlled and administered the C2 domain to collect and harvest the means of identification and financial credentials of thousands of victims, at least one of whom resided in the Northern District of California;

l. In or about August 2017, the defendants created a shared document to log and share the harvested financial credentials and means of identification of their victims. One such victim, Victim 2 (L.G.), resided in the Northern District of California;

m. In September 2017, Victim 2's (L.G.'s) fraudulently obtained financial accounts were used to make fraudulent purchases by the defendants or others. Victim 2 (L.G.) reported financial losses as a result.

COUNT TWO: (18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud)

22. Paragraphs 1 through 21 of this Indictment are re-alleged and incorporated as if fully set forth here.

23. Beginning at a time unknown to the Grand Jury, but no later than on or, about at least May 2016, and continuing through to and including a date unknown, but at least through on or about November 2017, in the Northern District of California and elsewhere, the defendants

[redacted] and SERAZHUDIN TAMIRLANOVICH AKTULAEV,

and others, did knowingly conspire to devise and intend to devise a scheme and artifice to defraud as to a material matter and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and by concealment of material facts, and, for the purpose of executing such scheme or artifice and attempting to do so, did transmit, and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343.

All in violation of Title 18, United States Code, Section 1349.

COUNT THREE: (18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i) – Obtaining Information from a Protected Computer for Financial Gain)

24. Paragraphs 1 through 21 of this Indictment are re-alleged and incorporated as if fully set forth here.

25. Beginning on or about at least June 2016, and continuing through to and including a date unknown, but at least through at least on or about November 2017, in the Northern District of California and elsewhere, the defendants,

[redacted] and
SERAZHUDIN TAMIRLANOVICH AKTULAEV,

intentionally accessed a protected computer without authorization, and thereby obtained information from a protected computer, and committed the offense for purposes of commercial advantage and private financial gain; specifically, defendants distributed malware to victim computer users, which when downloaded to their computer, would automatically call out to a C2 domain controlled by the defendants to harvest financial credentials of their victims, all in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i).

COUNT FOUR: (18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer to Obtain Value)

26. Paragraphs 1 through 21 of this Indictment are re-alleged and incorporated as if fully set forth here.

//

//

27. Beginning on or about at least June 2016, and continuing through to and including a date unknown, but at least through at least on or about November 2017, within the Northern District of California and elsewhere, the defendants,

[redacted] and
SERAZHUDIN TAMIRLANOVICH AKTULAEV,

knowingly and with intent to defraud accessed a protected computer used in interstate and foreign commerce without authorization and exceeding authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, the means of identification and financial credentials of thousands of victims, including victims in the Norther District of California.

All in violation of 18 U.S.C. Sections 1030(a)(4) and (c)(3)(A).

COUNT FIVE: (18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(A)(i)(VI) – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer)

28. Paragraphs 1 through 21 of this Indictment are re-alleged and incorporated as if fully set forth here.

29. Beginning on or about June 2016 and continuing through on or about November 2017, in the Northern District of California, and elsewhere, the defendants,

[redacted] and
SERAZHUDIN TAMIRLANOVICH AKTULAEV,

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit, the defendant caused the transmission of malware to protected computers used in interstate and foreign commerce and communication, and, by such conduct, caused damage to 10 or more protected computers during any one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(A)(i)(VI).

COUNT SIX: (18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft)

30. Paragraphs 1 through 21, 23, 25, 27, and 29 of this Indictment are re-alleged and incorporated as if fully set forth here.

31. Between at least June 2016 and continuing through on or about November 2017, in the Northern District of California and elsewhere, the defendants,

[redacted] and SERAZHUDIN TAMIRLANOVICH AKTULAEV,

during and in relation to felony violations of Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section1349, as described in Count Two of this Indictment: Obtaining Information from a Protected Computer for Financial Gain, in violation of Title 18, United States Code, Section 1030(a)(2), as described in Count Three of this Indictment; Unauthorized Access to a Protected Computer to Obtain Value, in violation of Title 18, United States Code, Section 1030(a)(4), as described in Count Four of this Indictment; and Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer, in violation of Title 18, United States Code, Section 1030(a)(4), did knowingly transfer, possess, and use, without lawful authority, the means of identification of another person, to wit, the usernames and passwords of L.G.'s PayPal and Amazon accounts.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j))

32. The allegations contained in this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and 1030(i) and (j).

33. Upon conviction for the offenses set forth in Counts One, Three, Four, and Five, in violation of Title 18, United States Code, Section 1030(a), set forth in this Indictment, the defendants,

[redacted] and SERAZHUDIN TAMIRLANOVICH AKTULAEV,

shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and 1030(i) and (j), any personal property used or intended to be used to commit or to facilitate the commission of said violation or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not limited to, a sum of money equal to the total amount of proceeds defendant obtained or derived, directly

or indirectly, from the violation, or the value of the property used to commit or to facilitate the commission of said violation.

34. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030, and Federal Rule of Criminal Procedure 32.2.

WIRE FRAUD FORFEITURE ALLEGATION: (18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))

35. The allegations contained in this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

36. Upon conviction for the offense set forth in Count Two of this Indictment, the defendants,

[redacted] and SERAZHUDIN TAMIRLANOVICH AKTULAEV,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), all property, real or personal, constituting, or derived from proceeds the defendant obtained directly and indirectly, as the result of those violations; including but not limited to:

37. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code, Section 2461(c), and Federal Rule of Criminal Procedure 32.2.

DATED: June 1, 2021

A TRUE BILL.

/S/
FOREPERSON

STEPHANIE M. HINDS
Acting United States Attorney

Cynthia Frey
CYNTHIA FREY
Assistant United States Attorney

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CRIMINAL COVER SHEET

Instructions: *Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case.*

CASE NAME: **CASE NUMBER: CR 21-0229 JD**

USA v. [redacted] and SERAZHUDIN AKTULAEV **CR**

Is This Case Under Seal?	**Yes** ✓	**No**	
Total Number of Defendants:	**1**	**2-7** ✓	**8 or more**
Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?	**Yes**	**No** ✓	
Venue (Per Crim. L.R. 18-1):	**SF** ✓	**OAK**	**SJ**
Is this a potential high-cost case?	**Yes**	**No** ✓	
Is any defendant charged with a death-penalty-eligible crime?	**Yes**	**No** ✓	
Is this a RICO Act gang case?	**Yes**	**No** ✓	

Assigned AUSA (Lead Attorney): AUSA Cynthia Frey **Date Submitted:** 6/1/2021

Comments:

RESET FORM SAVE PDF

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT ☐ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

OFFENSE CHARGED

PLEASE SEE ATTACHMENT

☐ Petty ☐ Minor ☐ Misde-meanor ☒ Felony

PENALTY: SEE ATTACHMENT

DEFENDANT - U.S

SERAZHUDIN TAMIRLANOVICH AKTULAEV

DISTRICT COURT NUMBER

CR 21-0229 JD

FILED
Jun 01 2021
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)

FBI

☐ person is awaiting trial in another Federal or State Court, give name of court

_____

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

_____

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of: ☐ U.S. ATTORNEY ☐ DEFENSE } SHOW DOCKET NO. _____

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under } MAGISTRATE CASE NO. _____

Name and Office of Person Furnishing Information on this form STEPHANIE M. HINDS

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) CYNTHIA FREY

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges _____

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

_____

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

_____

Has detainer been filed? ☐ Yes ☒ No } If "Yes" give date filed _____

DATE OF ARREST Month/Day/Year _____

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year _____

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount: No Bail

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Defendant Address:

_____

Date/Time: _____ Before Judge: _____

Comments:

PENALTY SHEET ATTACHMENT

Count 1: 18 U.S.C. § 371 – Conspiracy to Commit Computer Fraud to Defraud and Obtain Value and to Cause Damage to a Protected Computer

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 2: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

Maximum Penalties: (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 3: 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i) – Unauthorized Access to Obtain Information for the Purpose of Financial Gain

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 4: 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 5: (18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i) (referencing (c)(4)(A)(i)(VI)) - Transmission of a Program, Information, Code, and Command to Cause Damage Affecting 10 or More Protected Computers During any 1-year Period

Maximum Penalties: (1) 10 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 6: 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

Maximum Penalties: (1) 2 years imprisonment (to run consecutive to any other term imposed); (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Forfeiture Allegations: 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT ☐ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

OFFENSE CHARGED

PLEASE SEE ATTACHMENT

☐ Petty ☐ Minor ☐ Misde-meanor ☒ Felony

PENALTY: SEE ATTACHMENT

DEFENDANT - U.S

[redacted]

DISTRICT COURT NUMBER

CR 21-0229 JD

FILED
Jun 01 2021
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)

FBI

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of: ☐ U.S. ATTORNEY ☐ DEFENSE } SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under } MAGISTRATE CASE NO.

Name and Office of Person Furnishing Information on this form STEPHANIE M. HINDS

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) CYNTHIA FREY

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☒ No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount: No Bail

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Defendant Address:

Date/Time: Before Judge:

Comments:

PENALTY SHEET ATTACHMENT

Count 1: 18 U.S.C. § 371 – Conspiracy to Commit Computer Fraud to Defraud and Obtain Value and to Cause Damage to a Protected Computer

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 2: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

Maximum Penalties: (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 3: 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i) – Unauthorized Access to Obtain Information for the Purpose of Financial Gain

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 4: 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;

Maximum Penalties: (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 5: (18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i) (referencing (c)(4)(A)(i)(VI)) - Transmission of a Program, Information, Code, and Command to Cause Damage Affecting 10 or More Protected Computers During any 1-year Period

Maximum Penalties: (1) 10 years imprisonment; (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Count 6: 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

Maximum Penalties: (1) 2 years imprisonment (to run consecutive to any other term imposed); (2) Maximum of 3 years of supervised release; (3) $250,000 fine or twice the gross gain or twice the gross loss; (4) $100 Special Assessment

Forfeiture Allegations: 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c)