ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

OHND No. 1:24 MJ 4023

CR23-00471 WHO

UNITED STATES OF AMERICA, Plaintiff, v. NOAH ROSKIN-FRAZEE and KEITH LATTERI, Defendants.	CASE NO. VIOLATIONS: 18 U.S.C. § 371 – Conspiracy to Commit Computer Fraud and Abuse; 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), and (c)(4)(A)(i)(I), and 2 – Intentional Damage to a Protected Computer, Aiding and Abetting; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud and Mail Fraud; 18 U.S.C. § 1343 – Wire Fraud; 18 U.S.C. § 1341 – Mail Fraud; 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j) – Forfeiture Allegation SAN FRANCISCO

INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

1. NOAH ROSKIN-FRAZEE ("ROSKIN-FRAZEE") was a resident of San Francisco, California.

2. KEITH LATTERI ("LATTERI") was a resident of New Jersey and Ohio.

3. Company A was a corporation headquartered in Cupertino, California, which developed, manufactured, licensed, supported and sold computer software, consumer electronics, personal computers, and services. 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. Company B was a corporation headquartered in Fremont, California, which provided customer experience solutions and services to other companies. The computer servers of Company B 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).

5. A Virtual Private Network ("VPN") is a technology that creates a secure network connection over a public network such as the Internet or private network owned by an Internet Service Provider. The user of a VPN can conceal his true Internet Protocol ("IP") address from those with whom he is communicating.

6. A Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

COUNT ONE: (18 U.S.C. § 371 – Conspiracy to Commit Computer Fraud and Abuse)

7. Paragraphs 1 through 6 of this Indictment are re-alleged and incorporated as if fully set forth here.

8. Beginning on a date unknown to the Grand Jury, but no later than on or about December 21, 2018, and continuing through a date unknown, but at least through on or about March 1, 2019, in the Northern District of California and elsewhere, the defendant,

NOAH ROSKIN-FRAZEE,

and others known and unknown to the Grand Jury, did knowingly and willfully conspire and agree with each other to commit computer fraud and abuse, namely, (a) 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 (b) intentionally accessed a protected computer without authorization, and thereby obtained information from a protected computer, and committed the offense for purposes of private financial gain, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(i).

Background

9. Company A offered "Customer Service" contracts which provided customers with extended warranty and technical support options for Company A's products. Company A maintained a "Log Program" which allowed its Customer Service staff and contractors to view important information about Company A products, search products by serial number, and order Customer Replacement Units (CRUs) for customers whose products had broken or otherwise warranted replacement. Company A also maintained a "Toolbox" program that allowed Customer Service staff to edit orders for a limited time after they were placed. Company A utilized SAP software to manage its product order and merchandise distribution systems in a "SAP Database." The computer servers used by Company A in operating the SAP Database were located in the Northern District of California.

10. Company B contracted with Company A to provide customer experience solutions and services to Company A's customers as part of Company A's Customer Service program. Company B employees assigned to the Company A account had limited access to Company A's computer system and certain databases within that system in order to perform their customer service responsibilities. During the normal course of business, Company B employees logged into Company B's VPN server network using valid Company B credentials. Company B employees assigned to the Company A account had additional credentials that granted them access to Company A's computer system via Company A's Connect application, an authentication system that allowed users access to certain applications inside Company A's network. Once in Company A's system, Company B employees were able to access Company A's Log Program to place CRU orders and Company A's Toolbox and SAP Database to view and edit customer orders. Company B also had a Remote Desktop application used internally by IT staff for resolving technical issues. The Remote Desktop application allowed certain Company B employees to gain full control of another Company B employee computer remotely. Company B's VPN servers were located in South Carolina and Arizona.

11. Company B also maintained a JAMF Mobile Device Management platform, which was a device management tool used to configure Company A devices. The JAMF platform allowed access across Company B's network. The JAMF platform resided on a server located in Ontario, Canada.

The Conspiracy and Scheme to Defraud

12. The essence of the conspiracy and scheme to defraud was for the defendant and others to obtain unauthorized access to Company B's computer system and thereby obtain unauthorized access to Company A's computer system. It was further part of the conspiracy and scheme to utilize access to Company A's computer system to place fraudulent orders and fraudulently manipulate orders for Company A products and services to obtain such products and services for private financial gain.

13. During the course of the scheme, the defendant and co-conspirators attempted to fraudulently obtain over $3 million in Company A products and services through more than two dozen fraudulent orders. Of the orders that were completed, the defendant and co-conspirators obtained approximately $2.5 million in Company A electronic gift cards and over $100,000 in Company A products and services. Much of the gift cards and products were resold to third parties. As a result of the scheme, Company A and Company B sustained losses, including over $3 million in losses to Company B.

The Manner and Means of Accomplishing the Conspiracy

14. It was part of the scheme and artifice that the defendant and co-conspirators used the Internet and a password reset tool to gain access to a Company B employee account, and thereby gained unauthorized access to Company B's computer system and protected computers.

15. It was part of the scheme and artifice that the defendant and co-conspirators used Company B's computer system and protected computers to gain access to additional employee credentials which they used to access Company B's VPN servers.

16. It was part of the scheme and artifice that the defendant and co-conspirators used Company B's computers and VPN servers to access Company B's Remote Desktop application and Company A's Connect application, which they used to gain unauthorized access to Company A's computer system and protected computers.

17. It was part of the scheme and artifice that the defendant and co-conspirators used

Company A's computer system to access Company A's Log System and place fraudulent orders for CRUs for the defendant and his co-conspirators' private financial gain;

18. It was part of the scheme and artifice that the defendant and co-conspirators used Company A's computer system to access Company A's Toolbox program. Company A customarily placed product orders on hold for a limited time, during which time the orders could be edited in Company A's Toolbox program. The defendant and his co-conspirators utilized their unauthorized access to Company A's Toolbox to fraudulently manipulate product orders that the defendant and his co-conspirators had placed by editing the orders in Toolbox during the hold time for the defendant and his co-conspirators' private financial gain.

19. It was part of the scheme and artifice that the defendant and co-conspirators used Company B's computer system, employee credentials, and fraudulent user accounts to access Company B's JAMF platform and run scripts to exfiltrate sensitive data.

20. It was part of the scheme and artifice that the defendant and co-conspirators used the JAMF platform to access Company B employee computers located in India and Costa Rica and log those computers into join.me remote desktop sharing sessions.

21. It was part of the scheme and artifice that the defendant and co-conspirators logged into the join.me sessions on the computers in India and Costa Rica in order to remotely operate the computers. Company A customarily placed product orders on hold for a limited time, during which time the orders could be edited in Company A's SAP Database. It was part of the scheme and artifice that the defendant and co-conspirators remotely operated Company B's computers in India and Costa Rica to fraudulently manipulate product orders that the defendant, his family, and his co-conspirators had placed by editing the orders in Company A's SAP Database during the hold time. The defendant and co-conspirators made edits to these product orders to further the fraud and obtain something of value, including by fraudulently extending existing service contracts, adding products to existing orders without cost, and changing order monetary values to zero, all for private financial gain.

22. It was part of the scheme and artifice that the defendant and co-conspirators deleted their JAMF scripts and fraudulent order data to conceal the defendant's and co-conspirators' conduct during the intrusion.

23. It was part of the scheme and artifice that the defendant and co-conspirators used a VPN to conceal their real IP addresses, and that they used false names, disposable email addresses, false statements, and other false representations in placing and manipulating the fraudulent orders.

24. It was part of the scheme and artifice that the defendant and co-conspirators used transshipment companies Shipito LLC and Amboy Technologies LLC as shipping destinations for fraudulent orders to conceal their identity and location, and that they used false names, false statements and other false representations in connection with transshipment company accounts.

25. It was part of the scheme and artifice that the defendant and co-conspirators sold some of the fraudulently obtained products to third parties such as SellShark.

The Overt Acts

26. 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, the defendant and co-conspirators committed and caused to be committed the following overt acts, among others:

a. Beginning on a date unknown, but no later than on or about January 3, 2019, and continuing through at least on or about March 1, 2019, the defendant and co-conspirators used Company B employee credentials and VPN certificates to access Company B's VPN server and protected computers without authorization on multiple occasions.

b. The defendant and Individual 1, a co-conspirator, along with other co-conspirators, conspired to create an account with transshipment company Amboy Technologies LLC ("Amboy") to facilitate the fraud scheme. On or about January 3, 2019, the defendant and co-conspirators created an account in the name of "Jamie Baker" ("Baker Account"). The account payment record listed Individual 1, Individual 1's physical address, and Individual 1's email address.

c. The defendant and co-conspirators used the Baker Account as a recipient and shipping address for fraudulent product orders from Company A. On or about January 5, 2019, Individual 1 placed order number W619135858 with Company A for products valued at approximately $19,359. This order was fraudulent and directed shipments to the Baker Account at an Amboy address in Oregon.

d. On or about January 9, 2019, the defendant logged into the Baker Account four times. Between on or about January 8, 2019, and January 10, 2019, the defendant and co-conspirators, using the name Jamie Baker, contacted Amboy and requested that Amboy direct an incoming package for the Baker Account to "Noah Kai" at the defendant's address in San Francisco, California. Amboy terminated the Baker Account due to fraud concerns.

e. Around the time Amboy terminated the Baker Account, the defendant and co-conspirators conspired to create an account with transshipment company Shipito LLC to facilitate the fraud scheme. On or around January 9, 2019, the defendant and co-conspirators created an account in the name of Individual 1 ("Shipito Account"), with Individual 1's physical address, and email address genjislap@gmail.com. The defendant logged into the Shipito Account multiple times between January 9, 2019, and February 5, 2019.

f. Between on or around January 9, 2019, and January 20, 2019, at least seven fraudulent orders were shipped to the Shipito Account. On January 9, 2019, the defendant placed order number W780617561 in the name of Individual 1 at a Shipito address in Oregon. Order W780617561 included six laptops, all of which were activated by Individual 1 at or near Individual 1's physical address.

g. Between on or about January 8, 2019, and January 17, 2019, six laptops with serial numbers matching the laptops in order W780617561 were shipped from the Shipito Account to SellShark.com, a third party electronics reseller, by the defendant and co-conspirators. In exchange, SellShark issued a check for $8,025 made out to Individual 2, a co-conspirator.

h. From on or about January 16, 2019, and continuing until at least February 16, 2019, the defendant and co-conspirators accessed a Company B JAMF server without authorization and used it to push malicious script to Company B's protected computers. The defendant and co-conspirators used the script, which contained username "b00mX0r," to create a reverse Secure Shell tunnel between Company B and a Microsoft Azure account which allowed the defendant and co-conspirators to continue to access the Company A/Company B environment.

i. On or about January 26, 2019, the defendant and co-conspirators manipulated a Company A Customer Service contract, SAP Order 6283214163 for private financial gain. The defendant and co-conspirators identified an existing Customer Service contract associated with the defendant and his family. The defendant and co-conspirators used Company B employee credentials to access the SAP Database without authorization and extended the Customer Service contract expiration date from August 14, 2020, to August 14, 2022, without payment.

j. On or about January 31, 2019, the defendant and co-conspirators placed order W563839416 for an inexpensive device cable to be shipped to the defendant at the defendant's physical address. While the order was on the customary temporary hold, the defendant and co-conspirators added a laptop and smartphone to the order without payment. The laptop was shipped via mail from Rialto, California to the defendant's physical address in San Francisco, California.

k. On or about February 9, 2019, defendant and co-conspirators placed order number W5122912 with Company A for products valued at approximately $7,924, including one laptop and two smartphones. The order shipping name was the first name and last initial of Individual 1 and the shipping address was Individual 1's physical address. While the order was on the customary temporary hold, the defendant and co-conspirators used the credentials of a Company B employee to access Company A's SAP database without authorization and changed the value of the ordered products to zero. After the changes were made and the hold expired, the products were shipped. The products shipped in this order included a smartphone with serial number C39XW05AKPFX. This smartphone was activated by the defendant in California.

l. From on or about February 10, 2019, and continuing until a date unknown, but at least on or about February 14, 2019, the defendant and co-conspirators conspired to fraudulently obtain over $2.5 million in electronic gift cards from Company A. The defendant and co-conspirators directed the gift cards to disposable email addresses, including bigboy@yopmail.com, jpeacocker@yopmail.com, and jonamagicy@yopmail.com. Between on or about February 10, 2019, and on or about February 12, 2019, the defendant and co-conspirators logged into the three Yopmail email accounts.

m. On or about February 11, 2019, the defendant redeemed two of the gift cards for about $100 each. On or about February 13, 2019, the defendant redeemed a third gift card for about $100. On or around February 26, 2019, the defendant used the $300 in funds obtained from these gift cards to purchase FinalCut Pro on Company A's app store for about $299.99 using the defendant's own Company A account.

n. On or around February 22, 2019, the defendant and co-conspirators created a Bittrex account in the name of Julian Randall, with email address julrandalli@yopmail.com, and used this account to facilitate the transfer of proceeds from the fraud scheme. On or about February 22, 2019, the defendant and co-conspirators logged into the julrandalli@yopmail.com email account.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO: (18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), and (c)(4)(A)(i)(I), and 2 – Intentional Damage to a Protected Computer, Aiding and Abetting)

27. Paragraphs 1 through 6, 9 through 11, and 14, 15, and 18 of this Indictment are re-alleged and incorporated as if fully set forth here.

28. Beginning on a date unknown to the Grand Jury, but no later than on or about December 21, 2018, and continuing through a date unknown, but at least through on or about March 1, 2019, in the Northern District of California and elsewhere, the defendants,

NOAH ROSKIN-FRAZEE and KEITH LATTERI,

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 of Company B, a computer used in interstate and foreign commerce and communication, and, by such conduct, caused loss to one or more persons during a one-year period aggregating at least $5,000 in value, to wit: defendants intentionally transmitted programs, codes, information, and commands to Company B computers to manipulate employee accounts and passwords and access Company B servers and computer systems without authorization, thereby intentionally causing damage to protected computers of Company B, including at least one protected computer in the Northern District of California.

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

(c)(4)(A)(i)(I), and 2.

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

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

30. Beginning on a date unknown to the Grand Jury, but no later than on or about December 21, 2018, and continuing through a date unknown, but at least through on or about March 1, 2019, in the Northern District of California and elsewhere, the defendant,

NOAH ROSKIN-FRAZEE,

and others known and unknown to the Grand Jury, 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, and did use, and cause to be used, the mails to carry out an essential part of the scheme, in violation of Title 18, United States Code, Section 1341.

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

COUNTS FOUR THROUGH NINE: (18 U.S.C. § 1343 – Wire Fraud)

31. Paragraphs 1 through 25 and 28 through 29 and of this Indictment are re-alleged and incorporated as if fully set forth here.

32. Beginning on a date unknown to the Grand Jury, but no later than on or about December 21, 2018, and continuing through a date unknown, but at least through on or about March 1, 2019, in the Northern District of California and elsewhere, the defendant,

NOAH ROSKIN-FRAZEE,

knowingly and with the intent to defraud participated in, devised, and intended 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 means of omission and concealment of material facts.

33. Beginning on or about the dates set forth below, in the Northern District of California and elsewhere, for the purpose of executing the aforementioned scheme and artifice to defraud, the defendant,

NOAH ROSKIN-FRAZEE,

did knowingly transmit and cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain writings, signs, signals, pictures, and sounds, to wit: computer transmissions that accessed protected computers of Company A and Company B without authorization, in furtherance of the aforementioned fraud, as set forth below.

Count	Date	Description	Server A	Server B
Four	1/5/2019	IP address 67.160.208.7 logged into Company B VPN via Company B account for employee L.R.	California	South Carolina
Five	1/7/2019	IP address 67.160.208.7 logged into Company B JAMF server with account/username jss_computerinfo_scriptID_312	California	Canada
Six	1/15/2019	IP address 104.152.45.154 logged into Company B VPN via Company B account for employee S.C.	California	Arizona
Seven	1/21/2019	IP address 67.160.208.7 submitted a request for /JSSResource/policies from https://JAMFadmin-1.concentrix.com	California	Canada
Eight	1/31/2019	IP address 104.152.45.154 logged into Company B JAMF server with account/username adminbackup	California	Canada
Nine	2/10/2019	IP address 104.152.45.154 logged into Company B JAMF server with account/username - jss_computerinfo_scriptid_osv	California	Canada

All in violation of Title 18, United States Code, Section 1343.

COUNT TEN: (18 U.S.C. § 1341 – Mail Fraud)

34. Paragraphs 1 through 25 and 28 through 32 of this Indictment are re-alleged and incorporated as if fully set forth here.

35. On or around January 31, 2019, in the Northern District of California and elsewhere, the defendant,

NOAH ROSKIN-FRAZEE,

knowingly and with the intent to defraud participated in, devised, and intended 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 means of omission and concealment of material facts.

36. On or about January 31, 2019, in the Northern District of California and elsewhere, for the purpose of executing the aforementioned scheme and artifice to defraud, the defendant,

NOAH ROSKIN-FRAZEE,

did knowingly use, and cause to be used, the mails to carry out an essential part of the scheme, to wit: the defendant knowingly and with the intent to defraud caused a fraudulent order, order number W563839416 containing a Company A product, to be mailed from Company A's logistics provider in Rialto, California, to the defendant's physical address in San Francisco, California.

All in violation of Title 18, United States Code, Section 1341.

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

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).

Upon conviction for one or more of the offenses set forth in Count Two in this Indictment, the defendants,

NOAH ROSKIN-FRAZEE and KEITH LATTERI,

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.

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.

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

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).

Upon conviction for one or more of the offenses set forth in Counts One and Three through Ten in this Indictment, the defendant,

NOAH ROSKIN-FRAZEE,

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.

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: December 12, 2023

A TRUE BILL.

/s/ Foreperson
FOREPERSON
San Francisco, California

ISMAIL J. RAMSEY
United States Attorney

Maia Perez
MAIA PEREZ
Assistant United States Attorney