1546

FILED

MAY 20 2020

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

JUSTIN SEAN JOHNSON
a/k/a TDS
a/k/a DS

20-94

Criminal No.
(18 U.S.C. §§ 2, 371, 1028A(a)(1), and 1343)
UNDER SEAL

INDICTMENT

INTRODUCTION AND BACKGROUND

1. At all times material to this Indictment, the University of Pittsburgh Medical Center (hereafter, "UPMC") headquartered in Pittsburgh, Pennsylvania, was a $10 billion integrated global nonprofit health care enterprise with more than 65,000 employees, 21 hospitals, and 400 clinical locations. It operates outpatient sites and doctors' offices, a 2.3 million-member health insurance division, as well as commercial and international ventures in Europe and China.

2. At all times material to this Indictment, UPMC maintained an electronic human resource database (hereafter, "HR database") of employee information on the content server in its computer network, which contained highly sensitive, personally-identifiable information (hereafter, "PII") of present and former employees, including names, dates of birth, social security numbers, marriage statuses, salaries, employment statuses, and federal Form W-2 data which also contained income and tax withholding information.

3. At all times material to this Indictment, the HR database was managed by "PeopleSoft" data and human resource management software, and was accessible only via password by authorized UPMC personnel. The HR database contained the PII of approximately 65,000 UPMC employees.

4. On or about December 1, 2013, an unauthorized infiltration occurred to the HR database network, and a 'test query' for PII belonging to approximately 23,500 employees was performed by the intruder.

5. Beginning on or about January 21, 2014, through February 24, 2014, frequent remote infiltrations of the HR database occurred, often multiple times daily, during which time the infiltrator (hereafter, "hacker"), was able to view and to exfiltrate PII belonging to tens of thousands of UPMC employees.

6. Within a few days, UPMC investigators determined that PII belonging to tens of thousands of UPMC employees was likely viewed and stolen by the hacker.

7. Between January 31, 2014, and March 6, 2014, approximately 1,327 unauthorized, fraudulently-filed year 2013 Form 1040, 1040A, and 1040EZ federal income tax returns (hereafter, "Returns") were fraudulently prepared, electronically transmitted and filed with the IRS which contained the PII of UPMC employees.

8. The Returns were falsified to claim excessive withholdings due, and included other materially false statements, which caused the IRS to issue $1.7 million in unauthorized federal tax refunds.

9. The filers directed that the tax refunds be issued onto Amazon.com gift cards, which the tax filers applied towards the purchase of electronic merchandise at Amazon.com.

10. Between February 27, 2014, and March 14, 2014, approximately $885,578.00 in electronic merchandise purchased at Amazon.com, such as Samsung and Apple cell phones, gaming devices, and other electronics, was ordered using the fraudulently obtained Amazon.com gift cards, with instructions for delivery of the merchandise to Venezuela, through reshipping services located in Miami, Florida.

11. Individuals residing in Maracay and Maracaibo, Venezuela, received the Amazon shipments, including persons known to the grand jury as Y.L., M.N., and J.M., among others both known and unknown to the grand jury.

12. The unlawfully obtained merchandise was later trafficked and sold on online marketplace websites in South America.

COUNT ONE

The grand jury charges:

13. The United States incorporates by reference herein the allegations set forth in paragraphs 1-12, as though set forth at length more fully herein.

THE CONSPIRACY AND ITS OBJECTS

14. Beginning in and around November, 2013, and continuing thereafter until in and around May, 2014, in the Western District of Pennsylvania and elsewhere, the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS, conspired with persons known to the grand jury as Y.L., M.S.N., M.A., and M.N., and with other persons both known and unknown to the grand jury (collectively hereafter, "conspirators"), who all knowingly and willfully did conspire, combine, confederate, and agree together to defraud the United States of America, by impairing, impeding, obstructing, and defeating the lawful government functions of the IRS in the ascertainment, computation, assessment, and collection of the revenue, to wit, the filing of false Form 1040 federal income tax returns.

MANNER AND MEANS

15. It was a part of the conspiracy that the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS (hereafter, "JOHNSON"), determined to unlawfully infiltrate the HR database content servers located at the University of Pittsburgh Medical Center, which contained personally identifiable information of employees of UPMC, to exfiltrate and to steal bulk amounts of PII including names, dates of birth, social security numbers, marriage statuses, incomes, and other information contained in employee W-2 forms, and to solicit the sale of the data to buyers on darkweb marketplaces who schemed to file false federal income tax returns.

16. It was further a part of the conspiracy that in and around November, 2013, in a Facebook chat, JOHNSON stated that he wanted "*to play with Peoplesoft,*" "*which is basically HR*

in a box," that he was "*conspiring,*" and that he would be willing to tell the other person about it "*on torchat.*"

17. It was further a part of the conspiracy that JOHNSON became self-taught and proficient in PeopleSoft management software and performed over 1,000 Google searches for the word "PeopleSoft," in order to uncover any vulnerability in the software.

18. It was further a part of the conspiracy that to familiarize himself with PeopleSoft, JOHNSON stored information on his Google Drive titled "PEOPLESOFT PERMISSIONS" and "Super User."

19. It was further a part of the conspiracy that in Facebook chats in November, 2013, JOHNSON stated to others that he would be "*rich by end of year ...if you had what i have,*" that he was looking for a "*tor messaging service,*" and that "*the onion world is a very wonderful place.*"

20. It was further a part of the conspiracy that JOHNSON conspired with others about how to obtain bitcoin for a "*seller qualification fee*" in order to "*acquire, sell,* (and to) *profit,*" from stolen PII.

21. It was further a part of the conspiracy that JOHNSON and conspirators discussed obtaining unlawful access through PeopleSoft-managed databases in order to gain illegal access to company HR databases, for example, the database of a prominent national retailer.

22. It was further a part of the conspiracy that JOHNSON frequently chatted with others about his familiarity with the IRS, the process of filing electronic tax returns, the duties of "Case Advocates," and how to obtain a preparer tax identification number (hereafter, "PTIN").

23. It was further a part of the conspiracy that on or about December 1, 2013, JOHNSON infiltrated the content server of the HR database at UPMC by use of the TOR network and queried the PII, including Form W-2 data, of approximately 23,500 UPMC employees.

24. It was further a part of the conspiracy that on or about January 20, 2014, JOHNSON again intruded into the HR database and queried Form W-2 data of UPMC employees.

25. It was further a part of the conspiracy that between January 21, 2014, and February 24, 2014, JOHNSON infiltrated, queried, and exfiltrated to his control, PII belonging to thousands of UPMC employees.

26. It was further a part of the conspiracy that JOHNSON, using the moniker, "TDS," then solicited the sale of the stolen UPMC employee PII on a darkweb trading forum known as "Evolution."

27. It was further a part of the conspiracy that in January, 2014, TDS solicited the sale of UPMC employee PII on Evolution, stating as follows:

> *"US Identity Fullz + 2013 W-2 [Pack of 10]"*
> *Description*
> *$3 each Name Address City State Zip SSN DOB Federal State/City W-2 Information (includes employer EIN and address)*
> *Provided but unverified data: Marital Status*
> *!!! The majority of this listing will originate from Pennsylvania!!!*

28. It was further a part of the conspiracy that between January and February, 2014, buyers of the stolen UPMC PII acknowledged their purchases of the UPMC employee PII, stated that TDS was a good seller, and said that they would do business with him again.

29. It was further a part of the conspiracy that TDS sold or consigned UPMC employee PII to a person known to the grand jury as M.N. (an unindicted conspirator), and directed that M.N. send a percentage of profits from the use of the data to TDS in bitcoin cryptocurrency.

30. It was further a part of the conspiracy that M.N. digitally preserved records from his acquisition of the UPMC PII from TDS in a folder titled "*new HR profiles from DS.*"

31. It was further a part of the conspiracy that on or about October 31, 2013, JOHNSON registered an account at cryptocurrency exchange provider Coinbase for the purpose of depositing proceeds from the sale of the UPMC employee PII.

32. It was further a part of the conspiracy that JOHNSON deposited approximately $8,258.97 in cryptocurrency into his Bitcoin wallet from the sale of the UPMC employee PII.

33. It was further a part of the conspiracy that beginning in January, 2014, through March, 2014, conspirators who purchased the stolen UPMC employee PII from TDS prepared, electronically transmitted, and filed approximately 1,327 false Form 1040 federal income tax returns from locations in Venezuela or elsewhere, which contained the UPMC employee PII.

34. It was further a part of the conspiracy that, for the purpose of electronically transmitting the false federal income tax returns, conspirators registered fictitious email addresses through anonymizing foreign email service providers known as "Hushmail.com" and "Safe-mail.net."

35. It was further a part of the conspiracy that conspirators requested tax refunds in the form of Amazon.com gift cards, which they redeemed for Amazon.com electronic merchandise.

36. It was further a part of the conspiracy that conspirators then, using the previously registered Hushmail or Safe-mail email accounts and the Amazon.com gift cards, purchased hundreds of thousands of dollars in electronics and merchandise at Amazon.com, such as Samsung Galaxy cell phones, Apple iPhones, HP laptop computers, tablets, and gaming devices.

37. It was further a part of the conspiracy that conspirators registered shipping accounts at reshipping service companies in Miami, Florida, for the purpose of reshipping the fraudulently purchased merchandise from the United States to Venezuela.

38. It was further a part of the conspiracy that the conspirators caused the fraudulently obtained merchandise to be sent by reshipping services located in Miami, Florida, by air freight to Maracay and Maracaibo, Venezuela.

39. It was further a part of the conspiracy that conspirators then trafficked-in and sold the electronic merchandise through online auction websites in South America.

OVERT ACTS

40. In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendant, JUSTIN SEAN JOHSON, a/k/a TDS, a/k/a DS, and conspirators both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

(a) On or about October 31, 2013, JOHNSON created an account at cryptocurrency exchange Coinbase;

(b) On December 1, 2013, JOHNSON infiltrated the UPMC HR database and queried PII belonging to thousands of UPMC employees;

(c) Between January 21, 2014, and February 24, 2014, JOHNSON regularly infiltrated the content servers of the UPMC HR database and queried and exfiltrated PII belonging to thousands of UPMC employees;

(d) Between December 11, 2013, and April 12, 2014, JOHNSON made deposits of cryptocurrency into his Coinbase account from the sale of UPMC employee PII, which totaled approximately $8,258.97;

(e) In January, 2014, JOHNSON advertised the sale of UPMC employee PII to buyers on the darkweb forum Evolution and to a person known to the grand jury as M.N.;

(f) Between January 31, 2014, and March 6, 2014, conspirators electronically transmitted and filed approximately 1,327 false Form 1040 year 2013 federal income tax returns, which contained the PII of UPMC employees;

(g) Between February 27, 2014, and March 10, 2014, conspirators registered Amazon.com email user accounts with Hushmail.com or Safe-mail.net, and placed orders of electronic merchandise with gift card codes fraudulently obtained and funded with the unauthorized tax refunds;

(h) On or about March 12, 2014, conspirators placed three separate orders for electronic merchandise with Amazon.com through a user account "tecnomax266@gmail.com," which shipments were directed to Venezuela through reshipping services in Miami, Florida;

(i) On or about March 12, 2014, a user account was registered at Amazon.com styled as "tecnobioservicios@gmail.com," for the purpose of trafficking the electronic merchandise to purchasers on websites in South America;

(j) On or about March 19, 2014, March 21, 2014, April 4, 2014, and April 9, 2014, a conspirator signing as "Manuel," accepted delivery of electronic merchandise purchased at Amazon.com at a location in Venezuela; and

(k) On or about April 1, 2014, other conspirators personally signed for and accepted deliveries of electronic merchandise ordered for delivery to Venezuela;

(l) On or about May 7, 2014, conspirators received communications from online South America merchant "MercadoLibre" (not a conspirator herein) regarding the unlawfully obtained merchandise conspirators advertised for sale.

In violation of Title 18, United States Code, Section 371.

COUNTS TWO THROUGH ELEVEN

The grand jury further charges:

41. The United States incorporates by reference herein the allegations set forth in paragraphs 1-12, as though set forth at length more fully herein.

42. Beginning in and around November, 2013, and continuing thereafter until in and around March, 2017, the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS, devised, and intended to devise, a scheme and artifice to defraud UPMC, and its employees, of their personally identifiable information, as well as other individuals' personally identifiable information, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, well knowing at the time that the pretenses, representations, and promises were false and fraudulent when made, and which scheme to defraud placed financial institutions at a risk of financial loss.

43. It was part of the scheme and artifice to defraud that JOHNSON deceitfully infiltrated institutional HR databases controlled by PeopleSoft management software, queried for and exfiltrated sensitive employee PII and bank account information, and then solicited the sale of the PII on darkweb marketplaces.

44. It was further a part of the scheme and artifice to defraud that JOHNSON became proficient in PeopleSoft management software, learned its vulnerabilities, and even promoted himself on his résumé as having "*installed PeopleSoft systems with Oracle WebLogic...*"

45. It was further a part of the scheme and artifice to defraud that in October, 2013, JOHNSON registered an account at cryptocurrency exchange provider Coinbase.

46. It was further a part of the scheme and artifice to defraud that between January 21, 2014, through February 24, 2014, JOHNSON regularly and deceitfully infiltrated the content

servers of the UPMC HR database network and queried for and exfiltrated sensitive PII belonging to thousands of UPMC employees.

47. It was further a part of the scheme and artifice to defraud that JOHNSON then solicited the sale of the stolen UPMC PII to buyers on the darkweb marketplaces such as Evolution, which PII was purchased by fraudsters and used to fraudulently prepare, electronically transmit, and to file hundreds of false Form 1040 year 2013 federal income tax returns, which caused the IRS to unwittingly issue $1.7 million in false tax refunds to the false tax return filers.

48. It was further a part of the scheme and artifice to defraud that in and around August, 2015, TDS appeared on the illicit darkweb trading forum known as AlphaBay Marketplace (ABM), and posted the following solicitation for the sale of PII he exfiltrated from institutional HR databases, stating:

> *"In case anyone remembers me from TCF or evo: I'm back."*
>
> *"It's another year and once again I'm sitting on tens of thousands of fresh names, SSN, DOB, bank routing/account numbers and payroll data..."*
>
> *"600 employees is not huge in my book when I can spend time swiping the payroll of a company with 10,000+ employees or raiding the HR system of an institution with tens to hundreds of thousands of names."*
>
> *"Never said it was legitimate access. Just access. But for avoidance of doubt: Not my companies. Not employed by these companies...."*

49. It was further a part of the scheme and artifice to defraud that on or about August 25, 2015, JOHNSON registered a "Jabber" communication account and used it to solicit the sale of the stolen PII to prospective buyers.

50. It was further a part of the scheme and artifice to defraud that in October, 2016, JOHNSON changed his dark web pseudonym to "DS" and used it to communicate with buyers and to solicit the sale of PII.

51. It was further a part of the scheme and artifice to defraud that throughout 2016 and 2017, DS frequently solicited the sale of PII that he surreptitiously obtained in institutional database infiltrations on the darkweb marketplace ABM, stating, for example:

> "*And as for me being new...I've been doing this off and on since Evo and I'll be selling my own database of W-2 info as they're ready.*"
>
> "*I've got 45,000 fresh names/address/DOB/SSN and the source for the info that I'd like to get rid of in bulk.*"
>
> "*Still have most of these. Selling the lot for $7,500 or best non-ridiculous offer.*"
> "*12,500 rows of direct deposit information (yes, that includes account and routing numbers) retrieved yesterday from an active payroll system (no invalid shit). No logins. No credit cards. No companies. Just people...*"
>
> "*I've found not one but THREE colleges in the past few years that have had their entire academic student information system accessible because of shitty/default passwords...*"
>
> "*Profiles with IRS verified 2015 AGI or unverified 2015 non-filers...I have many profiles of college students and prospective college students (and sometimes their parents) with an IRS verified 2015 AGI from their financial aid paperwork...Interested? Let me know.*"

52. It was further a part of the scheme and artifice to defraud that in 2016, on ABM, DS solicited the sale of sensitive bank account information and PII to buyers, stating: "*Bulk SSN;*" "*Have a need for bank info?;*" "*I have some business for you;*" or "*Any buyers of bank account profiles?*"

53. It was further a part of the scheme and artifice to defraud that in October, 2016, DS stated to a buyer that the stolen PII came from a large healthcare provider in Georgia and Florida.

54. It was further a part of the scheme and artifice to defraud that DS solicited the sale of account holder information belonging to a TD Bank account customer and directed the buyer to deposit the sale proceeds in JOHNSON'S cryptocurrency wallet.

55. It was further a part of the scheme and artifice to defraud that in March, 2017, DS communicated with a buyer known to the grand jury as "C.L." and revealed the vulnerability and source of DS' stolen PII, stating in the following exchange with C.L.:

C.L.: "*hey bro, was on AB and seen a post you made about direct access to the database...that still available I am still working on turning $ into BTC...*"

DS: "*can check and see if I still have access, dunno if i do*"

C.L.: "*cool...like i said i got the $....feel like that's the best way to go...*"

DS: "*not unless you know how to use the software lol*"

C.L.: "*what software is it?*"

DS: "*peoplesoft*"

56. It was further a part of the scheme and artifice to defraud that on or about February 7, 2017, February 14, 2017, and March 21, 2017, DS sold multiple sets of PII to C.L. on the darkweb ABM, which C.L. paid for in cryptocurrency totaling $1,850.00, and which proceeds DS concealed through virtual currency "mixers."

THE WIRE COMMUNICATIONS

On or about the following dates set forth below, in the Western District of Pennsylvania, the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS, for the purpose of executing and attempting to execute the scheme and artifice to defraud, did transmit and cause to be transmitted in interstate commerce by means of a wire communication, certain signs, signals, sounds, and any appropriate combination of the three, that is, the defendant, by use of the internet, deceitfully infiltrated the content servers of the human resource database located at the University of Pittsburgh Medical Center in Pittsburgh, Pennsylvania, queried for, and exfiltrated employee PII to his control, placing financial institutions at a risk of loss, each such exfiltration of data being a separate count herein:

Count	Date
2	December 1, 2013
3	December 2, 2013
4	December 28, 2013
5	January 22, 2014
6	January 24, 2014

7	January 28, 2014
8	February 12, 2014
9	February 13, 2014
10	February 14, 2014
11	February 24, 2014

In violation of Title 18, United States Code, Section 1343.

COUNTS TWELVE THROUGH FOURTEEN

The grand jury further charges:

The United States incorporates by reference herein the allegations set forth in paragraphs 41 through 56, as though set forth at length more fully herein.

On or about the following dates set forth below, in the Western District of Pennsylvania, the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS, for the purpose of executing and attempting to execute the scheme and artifice to defraud, did transmit and cause to be transmitted in interstate commerce by means of a wire communication, certain signs, signals, sounds, and any appropriate combination of the three, that is, the defendant, by use of the internet, fraudulently solicited and sold PII which contained the names, dates of birth, social security numbers, and adjusted gross incomes for real persons, which the defendant transmitted to a person known to the grand jury as C.L., each such transmission of data being a separate count herein:

Count	Date
12	February 7, 2017
13	February 14, 2017
14	March 21, 2017

In violation of Title 18, United States Code, Section 1343.

COUNTS FIFTEEN THROUGH THIRTY-EIGHT

The grand jury further charges:

The United States incorporates by reference herein the allegations set forth in paragraphs 41 through 56, as though set forth at length more fully herein.

On or about the following dates set forth below, in the Western District of Pennsylvania, the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS, for the purpose of executing and attempting to execute the scheme and artifice to defraud, did transmit and cause to be transmitted in interstate commerce by means of a wire communication, certain signs, signals, sounds, and any appropriate combination of the three, that is, JOHNSON, by use of the internet, caused the preparation, electronic transmittal and filing of false Form 1040 year 2013 federal income tax returns which contained the PII of UPMC employees identified by their initials below, from Western Pennsylvania to an IRS Service Center located in Memphis Tennessee, each such electronic transmittal being a separate count herein:

Count	Date	UPMC Employee
15	January 31, 2014	D.S.
16	February 1, 2014	G.B.
17	February 2, 2014	M.W.
18	February 12, 2014	M.P.
19	February 12, 2014	S.Z.
20	February 16, 2014	D.R.
21	February 16, 2014	Y.P.
22	February 18, 2014	M.W.
23	February 18, 2014	C.B.
24	February 18, 2014	C.H.
25	February 20, 2014	K.S.
26	February 20, 2014	J.B.
27	February 21, 2014	L.D.
28	February 22, 2014	C.B.
29	February 23, 2014	G.S.
30	February 25, 2014	L.W.
31	February 27, 2014	C.S.
32	March 4, 2014	R.W.
33	March 4, 2014	S.W.

34	March 4, 2014	R.B.
35	March 5, 2014	L.S.
36	March 5, 2014	R.B.
37	March 5, 2014	J.L.
38	March 5, 2014	B.S.

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS THIRTY-NINE THROUGH FORTY-THREE

The grand jury further charges:

On or about March 21, 2017, in the Western District of Pennsylvania, the defendant, JUSTIN SEAN JOHNSON, a/k/a TDS, a/k/a DS, during and in relation to the felony violations of Wire Fraud, in violation of Title 18, United States Code, Section 1343, as alleged in Counts 12 through 14, did knowingly and without lawful authority, transfer, possess, and use a means of identification of another person, specifically, the defendant, by use of the internet, transferred, possessed, and used, the names, social security numbers, and dates of birth of the real persons identified by initials below during the sale of their PII to a person known to the grand jury as C.L., each such transfer, possession, and use being a separate count herein below:

Count	Initials
39	C.J.
40	C.C.
41	M.A.
42	A.G.
43	T.K.

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

A True Bill,

Foreperson

SCOTT W. BRADY
United States Attorney
PA ID No. 88352