

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FILED IN CHAMBERS
U.S.D.C. - Atlanta

JAN 28 2020

By: James N. Hatten, Clerk
Deputy Clerk

UNITED STATES OF AMERICA

v.

WU ZHIYONG,
WANG QIAN,
XU KE,
LIU LEI

Criminal Indictment

No. 19-0000 - CR046

Under Seal

THE GRAND JURY CHARGES THAT:

INTRODUCTION

1. Equifax Inc. is a consumer credit reporting agency headquartered in Atlanta, Georgia ("Equifax"). In its ordinary course of business, Equifax compiles and stores a vast collection of consumer information, which it sells to other businesses and organizations seeking to use the information to assess creditworthiness or verify identity. Equifax thus holds a colossal repository of sensitive personally identifiable information, including full names, addresses, social security numbers, birth dates, and driver's license numbers, belonging to hundreds of millions of individuals in the United States and abroad. This data compilation was confidential, proprietary business information for Equifax, and the company stored the information on restricted, nonpublic servers located in Alpharetta, Georgia and elsewhere.

2. Beginning on an unknown date, but at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, members of the People's Liberation Army ("PLA"), the armed forces of the People's Republic of China ("China"), conspired with each other to hack into the protected computers of Equifax located in the Northern District of Georgia, to maintain unauthorized access to those computers, and to steal sensitive personally identifiable information of 145 million Americans.

3. The PLA hackers obtained names, birth dates, and social security numbers for the 145 million American victims, in addition to driver's license numbers for at least 10 million Americans stored on Equifax's databases. The hackers also collected credit card numbers and other personally identifiable information belonging to approximately 200,000 American consumers. Accordingly, in a single breach, the PLA obtained sensitive personally identifiable information for nearly half of all American citizens.

4. In addition, the PLA hackers obtained personally identifiable information belonging to nearly a million citizens of the United Kingdom and Canada.

BACKGROUND

5. At all times relevant to this Indictment:

a. Equifax hosted an online dispute portal that permitted users to research and dispute potential inaccuracies in their Equifax credit reports on servers located in Alpharetta, Georgia. The online dispute portal used the Apache Struts Web Framework, an open-source software package for developing web-based applications.

b. In connection with the management and protection of its databases, Equifax developed and maintained proprietary compilations, designs, processes, and codes that constituted trade secrets, for which it had taken reasonable measures to keep secret and which derived independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person who could obtain economic value from the disclosure and use of the information. This trade secret information included the above-described personally identifiable information Equifax had acquired at great effort and expense and that enabled it to operate its business and compete in the marketplace – that is, its data compilations – as well as the means by which Equifax accessed and analyzed that information, that is, its database schemas.

c. On or about March 7, 2017, Apache announced a vulnerability in certain versions of Apache Struts software that permitted unauthorized users to access the Apache Struts Web Framework and perform a remote code execution attack on a target web application. The United States Computer Emergency Readiness Team issued a threat warning notice about the vulnerability on or about the following day. The vulnerability was not patched on Equifax's online dispute portal.

d. Defendants WU ZHIYONG, whose photograph is attached as Exhibit A; WANG QIAN, whose photograph is attached as Exhibit B; XU KE, whose photograph is attached as Exhibit C; and LIU LEI were

residents of Beijing, China and members of the 54th Research Institute, which was a component of the PLA.

e. A web shell was a script that can be uploaded to a web server to enable remote administration of the server. A web shell can be used by an attacker to gain access to functions on the server and to maintain persistent access to a compromised server.

COUNT ONE

(Computer Fraud Conspiracy)

6. Beginning on an unknown date, but at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, the exact dates being unknown to the Grand Jury, in the Northern District of Georgia and elsewhere, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, did knowingly and willfully combine, conspire, confederate, agree, and have a tacit understanding with each other and other persons known and unknown to the Grand Jury, to commit offenses against the United States, namely:

- a. to intentionally access protected computers without authorization and thereby obtain information from protected computers in furtherance of the criminal act of economic espionage in violation of Title 18, United States Code, Section 1831(a)(2), with the value of such information exceeding \$5,000, all in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii)-(iii); and

- b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause loss aggregating at least \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

MANNER AND MEANS OF THE CONSPIRACY

7. It was part of the conspiracy that the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and others hacked into Equifax's computer networks, maintained unauthorized access to those networks, and stole login credentials and sensitive personally identifiable information that were stored on databases within those networks, as well as protected trade secrets.

8. The conspirators exploited the Apache Struts vulnerability to upload to an Equifax web server multiple unauthorized web shells and began reconnaissance of Equifax's online dispute portal. After gaining access to the web server, the conspirators interacted with Equifax's back-end databases by installing web shells created through Apache Struts and issuing commands using Structured Query Language ("SQL"), a database management language commonly used to query and manipulate data. The

conspirators also located and used Equifax database service credentials and thereby falsely represented that they were authorized users of Equifax's network, which permitted them to access additional back-end databases.

9. The conspirators ran a series of queries to search for sensitive personally identifiable information within Equifax's databases. After locating a repository of names, addresses, social security numbers, and birth dates, the conspirators ran additional queries to extract this data. In total, the attackers ran approximately 9,000 queries on Equifax's system while masking this activity through encrypted communication channels. The majority of these queries were issued by conspirators using two China-based IP addresses that connected directly to Equifax's network.

10. The conspirators stored the stolen information in temporary files, compressed and divided the large data files into more manageable file sizes for transmission, and executed Hypertext Transfer Protocol ("HTTP") commands to download the data files.

11. The conspirators attempted to hide the origin and location of their internet traffic and reduce the likelihood of detection by using approximately thirty-four servers located in nearly twenty countries to infiltrate Equifax's network. The conspirators also employed a variety of encrypted login protocols, including Remote Desktop Protocol and Secure Shell software, which permitted them to connect to servers over network connections from other servers they controlled. To further disguise their infrastructure, the conspirators obtained access to the servers located

outside of China from reseller hosting services, who purchase remote computing services from other providers and then lease those remote computing services to others.

12. Additionally, the conspirators attempted to disguise their unauthorized access to Equifax's online dispute portal by using existing encrypted communication channels within Equifax's network to send queries and commands, which allowed them to blend in with normal network activity. By compressing and dividing the data files, the conspirators also disguised the exfiltration of sensitive personally identifiable information.

13. To further conceal their activity, the conspirators deleted the compressed files after exfiltrating the sensitive data. In addition, the conspirators configured settings on at least one of their leased servers that wiped log files on a daily basis in an effort to eliminate records of their activity.

OVERT ACTS

14. In furtherance of the conspiracy, and to effect the purpose and objects thereof, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and others committed various overt acts in the Northern District of Georgia and elsewhere, including, but not limited to, the following:

a. On or about May 13, 2017, a conspirator began exploiting the Apache Struts vulnerability within Equifax's online dispute portal and created a web shell to grant back door access to the portal. Through this

initial access, the conspirators obtained database service login credentials that could be used to navigate to databases within Equifax's network.

b. After exploiting the vulnerability, the conspirators conducted reconnaissance on Equifax's online dispute portal over several weeks by running a series of queries to identify Equifax's database structure and the number of records within it. The conspirators reviewed database records in small segments through a combination of Apache Struts commands, malicious web shells created through Apache Struts, and SQL commands.

c. For example, on or about May 13, 2017, a conspirator ran SQL commands to identify table names and column names for an Equifax database table. The conspirator then sampled a select number of records from the database.

d. Between on or about May 13, 2017, and on or about July 24, 2017, the conspirators accessed a file containing sensitive personally identifiable information. After querying database tables, the conspirators stored results in output files, which were then split into smaller segments to facilitate a quicker download while attempting to lessen the risk of detection.

e. On or about June 16, 2017, a conspirator using a China-based IP address ("China Server #1"), which was repeatedly accessed during the intrusion by WANG QIAN, logged into a Taiwanese IP address ("the Taiwan Server") via Remote Desktop Protocol software and copied the malicious file "jndi.txt." A substantively identical web shell, "jQuery-1.3.2.min.jsp," was then uploaded to the Equifax network.

f. On or about July 5, 2017, a conspirator who was using a Swiss IP address ("the Swiss Server") connected to the Equifax network and accessed a database by using the username and password for one of the compromised database service accounts. After gaining access to the database, the conspirator queried the database table for social security numbers.

g. On or about July 6, 2017, a conspirator who was logged into the Swiss Server connected to the Equifax network and queried a database for social security numbers, full names, and address information and placed the results in output files. After creating the output files, the conspirators created a compressed file archive of the results and copied it to a different directory prior to downloading the archive. Following the download of the personally identifiable information, the conspirators deleted the archive in an effort to conceal their activity.

h. On or about the same day, a conspirator who was logged into the Swiss Server connected to the Equifax network, accessed a different back-end database by using the username and password for another compromised database service account, and queried the database.

i. On or about July 7, 2017, a conspirator who was logged into the Swiss Server connected to the Equifax network, accessed a third back-end database by using the username and password for yet another compromised database service account, and queried the database.

j. On or about the same day, another China-based IP address ("China Server #2"), which was also repeatedly accessed during the

intrusion by WANG QIAN, exploited the Apache Struts vulnerability on Equifax's online dispute portal.

k. On or about the same day and July 9, 2017, XU KE used a different China-based IP address ("China Server #3") to conduct reconnaissance on Equifax's online dispute portal.

l. On or about July 10, 2017, a conspirator using another China-based IP address ("China Server #4") logged into the Taiwan Server and copied the malicious file "abc.txt" to the Taiwan Server. A conspirator using another China-based IP address ("China Server #5") then utilized the malicious web shell "css.jsp," which was previously installed on Equifax's network, to issue a command to download the "abc.txt" file from the Taiwan Server. Minutes later, a conspirator using China Server #5 uploaded a substantively identical web shell, "ss.jsp," to the Equifax network.

m. On or about the same day, a conspirator logged into the Swiss Server, connected to the Equifax network, and issued a command to create an archive containing 49 directories. Once the archive was created, a conspirator split it into 600 megabyte segments, which were then downloaded from the Equifax network to a Dutch server via HTTP commands.

n. On or about the same day, a conspirator who was logged into another China-based IP address ("China Server #6") utilized the malicious web shell "boxover.jsp" to query an Equifax database table and store the results in output files. Using China Server #6, the conspirator then

compressed the output file into an archive file and downloaded the archive using HTTP commands. Following the download, the conspirator then used the "css.jsp" web shell to delete the archive from Equifax's network in an effort to conceal the theft.

o. On or about July 20, 2017 through on or about July 22, 2017, WANG QIAN, using China Server #2, remotely accessed the malicious web shell "six.jsp" on an Equifax server, which permitted WANG to issue unauthorized SQL commands to one of Equifax's back-end databases. On or about July 22, 2017, a Singapore-based IP address ("the Singapore Server") connected to an Equifax server and accessed the same "six.jsp" web shell to run additional queries on Equifax's databases.

p. The conspirators continued to perform queries to compress, download, and delete output files containing personally identifiable information stolen from Equifax's back-end databases until on or about July 30, 2017.

q. On or about July 30, 2017, LIU LEI, using the Singapore Server, remotely accessed the malicious web shell "ss.jsp" on an Equifax server.

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

COUNT TWO

(Computer Fraud and Abuse: Intentional Damage)

15. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 5 and 7 through 14 of this Indictment as if fully set forth herein.

16. From on or about May 13, 2017, through on or about July 30, 2017, in the Northern District of Georgia and elsewhere, the defendants, WU

ZHIYONG, WANG QIAN, XU KE, and LIU LEI, aided and abetted by each other and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, namely, malicious web shells and SQL and HTTP commands, and as a result of such conduct, intentionally caused damage without authorization to a protected computer with the offense loss aggregating at least \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B) and Section 2.

COUNT THREE

(Computer Fraud and Abuse: Unauthorized Access)

17. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 5 and 7 through 14 of this Indictment as if fully set forth herein.

18. From on or about May 13, 2017, through on or about July 30, 2017, in the Northern District of Georgia and elsewhere, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, aided and abetted by each other and others known and unknown to the Grand Jury, did intentionally access a computer, namely the private, internal networks of Equifax, without authorization and thereby obtained and attempted to obtain information from a protected computer in furtherance of the criminal act of economic espionage in violation of Title 18, United States Code, Section 1831(a)(2), with the value of such information exceeding

\$5,000, all in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii)-(iii) and Section 2.

COUNT FOUR

(Conspiracy to Commit Economic Espionage)

19. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 5 and 7 through 14 of this Indictment as if fully set forth herein.

20. Beginning on an unknown date, but at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, in the Northern District of Georgia and elsewhere, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, knowingly and willfully combined, conspired, confederated, agreed, and had a tacit understanding, with each other and others known and unknown to the Grand Jury, to:

- a. knowingly steal and without authorization appropriate, take, and by fraud, artifice, and deception obtain trade secrets belonging to Equifax;
- b. knowingly and without authorization copy, duplicate, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey trade secrets belonging to Equifax; and
- c. knowingly receive, buy, and possess trade secrets belonging to Equifax, knowing the same to have been stolen, appropriated, obtained, and converted without authorization;

with said trade secrets including the compilation of confidential, personally identifiable data collected from a variety of sources at

significant effort and expense and the proprietary database schema designed to store and manipulate that data, intending and knowing that the offense would benefit a foreign government, instrumentality, and agent, namely China and the People's Liberation Army, in violation of Title 18, United States Code, Sections 1831(a)(1), (a)(2), and (a)(3).

OVERT ACTS

21. In furtherance of the conspiracy, and to effect the purpose and objects thereof, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and others committed various overt acts in the Northern District of Georgia and elsewhere, including, but not limited to, the overt acts identified in paragraph 14 of the Indictment.

All in violation of Title 18, United States Code, Section 1831(a)(5).

COUNT FIVE

(Economic Espionage)

22. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 5 and 7 through 14 of this Indictment as if fully set forth herein.

23. Beginning on an unknown date, but at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, in the Northern District of Georgia and elsewhere, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, aided and abetted by each other and others known and unknown to the Grand Jury, intending and knowing that the offense would benefit a foreign government, instrumentality, and agent, namely China and the People's Liberation Army, did knowingly and

without authorization copy, duplicate, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey a trade secret, and did attempt to do so, specifically database schemas and the compilation of data within those databases owned by Equifax, in violation of Title 18, United States Code, Sections 1831(a)(2) and 1831(a)(4) and Section 2.

COUNT SIX

(Conspiracy to Commit Wire Fraud)

24. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 5 and 7 through 14 of this Indictment as if fully set forth herein.

25. Beginning on an unknown date, but at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, in the Northern District of Georgia and elsewhere, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, knowingly and willfully combined, conspired, confederated, agreed, and had a tacit understanding, with each other and others known and unknown to the Grand Jury, to devise and intend to devise a scheme and artifice to defraud Equifax, and to obtain money and property from Equifax by means of materially false and fraudulent pretenses, representations, and promises, as well as by omissions of material facts, and for the purpose of executing such scheme and artifice and to obtain money and property, and attempting to do so, did knowingly transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, namely malicious computer code and

misappropriated user credentials, in violation of Title 18, United States Code, Section 1343.

MANNER AND MEANS OF THE CONSPIRACY

26. It was part of the conspiracy that the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and others known and unknown employed the manner and means set forth in paragraphs 7 through 13 of the Indictment to gain unauthorized access to the computer networks of Equifax and steal confidential, sensitive personally identifiable information from Equifax's databases.

27. After infiltrating Equifax's network, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and their co-conspirators gained unauthorized access to an Equifax data repository containing database service credentials and stole the credentials.

28. WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and their co-conspirators then logged into additional Equifax databases using those credentials, thereby misrepresenting that they were authorized users of those databases.

29. After gaining access to these additional databases with stolen credentials, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, and their co-conspirators searched for and stole sensitive and proprietary personally identifiable information stored in the databases.

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

COUNTS SEVEN THROUGH NINE

(Wire Fraud)

30. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 5, 7 through 14, and 26 through 29 of this Indictment as if fully set forth herein.

31. On or about the dates listed in Column A of the table below, in the Northern District of Georgia and elsewhere, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, aided and abetted by each other and others known and unknown to the Grand Jury, having knowingly devised and intending to devise the aforementioned scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises as set forth in Count Six of this Indictment, did with intent to defraud cause the transmission by means of wire communication in interstate and foreign commerce of certain writings, signs, signals, pictures, and sounds, that is, the commands specified in Column B issued from the Swiss Server to an Equifax server located in the Northern District of Georgia, after accessing an Equifax database through the use of misappropriated login credentials, for the purpose of executing such scheme and artifice:

	A	B
Count	Date	Computer Command
7	7/5/2017	Select SSN from [REDACTED] where rownum<1000
8	7/6/2017	Select 1 from [REDACTED]
9	7/7/2017	Select * from [REDACTED]

All in violation of Title 18, United States Code, Section 1343 and Section 2.

FORFEITURE PROVISION

32. Upon conviction of the offense alleged in Count One of this Indictment, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, 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, the defendants' interest in any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations.

33. Upon conviction of one or more of the offenses alleged in Counts Two and Three of this Indictment, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), the defendants' interest in any and all personal property that was used or intended to be used to commit or to facilitate the commission of such violations, as well as any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations.

34. Upon conviction of one or more of the offenses alleged in Counts Four and Five of this Indictment, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 1834 and 2323(b), any and all property that was used or intended to be used to commit or to facilitate the commission of such violations, as well as any and all property constituting,

or derived from, proceeds obtained directly or indirectly as a result of said violations.

35. Upon conviction of one or more of the offenses alleged in Counts Six through Nine of this Indictment, the defendants, WU ZHIYONG, WANG QIAN, XU KE, and LIU LEI, 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), any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations.

36. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property described above; all pursuant to

Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(A) & (B),
and Title 28, United States Code, Section 2461(c).

A BILL

✓ FOREPERSON

BYUNG J. PAK

United States Attorney



NATHAN P. KITCHENS

Assistant United States Attorney

Georgia Bar No. 263930



SAMIR KAUSHAL

Assistant United States Attorney

Georgia Bar No. 935285



THOMAS J. KREPP

Assistant United States Attorney

Georgia Bar No. 346781

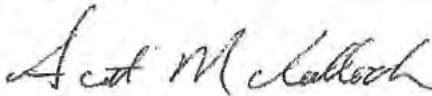


BENJAMIN FITZPATRICK

Senior Counsel

Computer Crime and Intellectual Property Section

DC Bar No. 501806



SCOTT MCCULLOCH

Trial Attorney

Counterintelligence and Export Control Section

DC Bar No. 1020608

600 U.S. Courthouse
75 Ted Turner Drive SW
Atlanta, GA 30303
404-581-6000; Fax: 404-581-6185

Exhibit A



Wu Zhiyong (吴志勇)

Exhibit B



Wang Qian (王乾)

Exhibit C



Xu Ke (许可)
