DENNIS J. HERRERA, State Bar #139669
City Attorney
RONALD P. FLYNN, State Bar #184186
Chief Deputy City Attorney
YVONNE R. MERÉ, State Bar #173594
Chief of Complex and Affirmative Litigation
KRISTINE POPLAWSKI, State Bar #160758
KENNETH WALCZAK, State Bar #247389
Deputy City Attorneys
1390 Market Street, 7th Floor
San Francisco, California 94102-5408
Telephone: (415) 554-3878
Facsimile: (415) 437-4644
E-Mail: kristine.poplawski@sfgov.org

Attorneys for Plaintiff
PEOPLE OF THE STATE OF CALIFORNIA,
by and through DENNIS J. HERRERA AS
CITY ATTORNEY OF SAN FRANCISCO

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN FRANCISCO

UNLIMITED JURISDICTION

PEOPLE OF THE STATE OF CALIFORNIA, by and through DENNIS J. HERRERA AS CITY ATTORNEY OF SAN FRANCISCO,

Plaintiff,

vs.

EQUIFAX, INC., and DOES 1-20, inclusive,

Defendants.

Case No. CGC-17-561529

COMPLAINT FOR EQUITABLE AND INJUNCTIVE RELIEF AND CIVIL PENALTIES FOR VIOLATIONS OF BUSINESS AND PROFESSIONS CODE SECTION 17200 ET SEQ.

Plaintiff, the People of the State of California (the "People"), acting by and through San Francisco City Attorney Dennis Herrera, hereby alleges as follows:

INTRODUCTION

1. Defendant Equifax, Inc. ("Equifax") is one of the three major companies providing national credit-reporting services in the United States. Equifax collects and maintains data regarding more than 820 million consumers worldwide, including more than 15 million consumers who reside in California. The data Equifax collects includes consumer names; addresses; social security numbers; dates of birth; bank, credit, and other financial account numbers; and the status of consumer, bank, and credit accounts (as open, delinquent, closed, etc.).

2. The personal data that Equifax maintains is crucial to consumers' ability to obtain credit, open bank accounts, purchase homes and lease apartments. Lenders and other businesses throughout the United States rely upon Equifax's consumer credit reports to make decisions regarding a consumer's creditworthiness and eligibility for many services and products, including cellphone service, insurance and premium rates, and leasing of automobiles and apartments.

3. According to its 2016 Annual Report, Equifax "develop[s], maintain[s] and enhances secured proprietary information databases through the compilation of consumer specific data, including credit, income, employment, asset, liquidity, net worth and spending activity, and business data, including credit and business demographics, that [it] obtain[s] from a variety of sources, such as credit granting institutions, income and tax information primarily from large to mid-sized companies in the U.S., and survey-based marketing information." Businesses such as banks and other financial institutions regularly furnish to Equifax electronic data files containing information regarding their customers. The consumers have no reasonable ability to prevent the entities with which they do business from disclosing their personal information to Equifax, nor any reasonable way to prevent or limit Equifax from processing or using that information. Consumers must rely on Equifax to protect their personal information and to prevent it from being accessed inappropriately.

4. On September 7, 2017, Equifax posted a notice on its website announcing that it had discovered "a cybersecurity incident potentially impacting approximately 143 million U.S. consumers," and that "[c]riminals exploited a U.S. website application vulnerability to gain access to

certain files" that contained consumers' names, social security numbers, birth dates, addresses, and driver's license numbers, and credit card numbers for approximately 209,000 consumers. Equifax stated that it had discovered the Data Breach on July 29, 2017, and that unauthorized access to its consumer database occurred from approximately May 13, 2017 through July 30, 2017.

5. Equifax has since identified the means by which criminals gained access to its consumer data as a "vulnerability" in an open-source software called "Apache Struts" that Equifax uses on its website. The existence of this vulnerability was detected and publicly announced as early as March 7, 2017 by various organizations, including the creator of Apache Struts software, Apache Software Foundation, which at the same time also provided a "patch" to cure the vulnerability.

6. Although Equifax knew about the Apache Struts vulnerability (the "March Security Vulnerability") and the patches and fixes for that vulnerability by March 2017, Equifax failed to take measures sufficient to protect the personal data it maintains, thereby exposing such sensitive and personal consumer data to unauthorized access. Equifax could have prevented the Data Breach by implementing the patches and fixes provided by the Apache Software Foundation in March 2017, and by implementing other reasonable security measures such as encryption of customer data, imposition of layers of security, and segregating different types of data into different files or systems, that would have limited the amount of data that the Data Breach intruders could access simply by taking advantage of the Apache Struts vulnerability. Equifax failed to apply the available patches or to take other action such as encryption or adding multiple layers of security. Equifax's failure to timely install the patch to fix the Apache Struts vulnerability and to implement other reasonable security measures violated industry standards for data security and the California Customer Records Act ("CRA"), at Civil Code sections 1798.81.5(a) and (b).

7. As a result, criminals accessed the consumer data maintained by Equifax, and did so from at least May 13, 2017 through July 30, 2017 (the "Data Breach") and likely stole sensitive and personal information of 143 million United States consumers, approximately 44% of the United States population. Among the affected consumers are more than 15 million California residents.

8. By failing to secure consumer information from unauthorized access, Equifax exposed 44% of the United States population to risks of identity theft and financial fraud, including

fraudulently filed tax returns and theft from consumers' bank accounts, health identity fraud, and other potential harms.

9. Impacted consumers have expended, and will continue to expend, money, time and resources to protect against the increased risk of identity theft and fraud posed by the Data Breach, including by (a) paying to place fraud flags and security freezes on their credit data maintained by Equifax and the other major credit reporting services, (b) paying for credit monitoring services, and (c) closely monitoring their credit card and bank statements, other financial accounts, health benefit accounts, driver's license records, and any other accounts for which a name, date of birth, and social security number may provide access.

10. The injury to consumers will not be short-lived. Because of the extent of the personal information that was accessible to unauthorized individuals, and the immutability of a consumer's social security number and date of birth, the Data Breach will subject California residents to increased risk of identity theft and fraud for many years to come.

11. Moreover, Equifax exacerbated the risk of identity theft and fraud faced by California consumers by unreasonably delaying announcement of the Data Breach until six weeks after it had discovered the breach. This delay prevented consumers from acting swiftly to mitigate the adverse effects of the Data Breach by placing fraud flags and security freezes on their credit data and taking other action to avoid becoming victims of identity theft and fraud. Equifax's unreasonable delay in notifying California residents of the Data Breach violated Civil Code sections 1798.82 (a) and (b).

12. The People bring this action to hold Equifax accountable for its gross failure to secure the personal and sensitive data of California residents, and to require Equifax to take all necessary action to ensure the security of California residents' personal information in the future. The People seek civil penalties, restitution, and injunctive relief under the California Business & Professions Code section 17200 *et seq.*

PARTIES

13. Plaintiff the People of the State of California, by and through San Francisco City Attorney Dennis Herrera, prosecute this action pursuant to Business and Professions Code sections 17204 and 17206.

14. Defendant Equifax, Inc. is a publicly-traded Georgia corporation with its principal place of business at 1550 Peachtree Street N.E., Atlanta, Georgia.

15. The true names and capacities of Defendants sued herein under the fictitious names Does 1 through 20, inclusive, are unknown to Plaintiff. Defendants Does 1 through 20 engaged in the same conduct and omissions as are alleged with respect to Defendant Equifax, Inc., and are subject to the same legal obligations and liabilities as Defendant Equifax. Plaintiff will seek leave of court to amend this Complaint to allege such names and capacities as soon as they are ascertained.

16. Plaintiff is informed and believes that all of the acts and omissions described in this Complaint by any Defendant were duly performed by, and attributable to, all Defendants, each acting as agent, employee, alter ego, and/or under the direction and control of the others, and such acts and omissions were within the scope of such agency, employment, alter ego, direction, and/or control. Additionally or in the alternative, each Defendant has aided and abetted all other Defendants in violating the letter of and the public policy embodied in the laws set forth in this Complaint.

JURISDICTION AND VENUE

17. The Superior Court has jurisdiction over this action. Defendant is conducting unlawful, unfair, and fraudulent business practices in San Francisco, and the City Attorney has standing and authority to prosecute this case on behalf of the People. (Business and Professions Code sections 17204 and 17206.)

18. Venue is proper in this Court because Defendants transact business in the City and County of San Francisco and some of the acts complained of occurred in this venue. Venue is also proper in this Court because the People's cause of action and Defendant's liability for its unlawful actions and omissions arose in the City and County of San Francisco. (Code of Civil Procedure sections 393 and 395.5.) Further, venue is proper in this Court because Defendant is a Georgia corporation with no residence in any county of California, rendering venue proper in any county designated by Plaintiff, the People. (*Id.* at section 395(a).)

//

//

//

FACTUAL BACKGROUND

Equifax's Business Model

19. Equifax's core business is the collection, processing, and sale of information about people and businesses. According to its website, Equifax is a "global information solutions company" that "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers." According to Equifax's 2016 Annual Report, U.S. Information Solutions, the Equifax unit that handles consumer information services such as credit information and credit scoring, had an operating revenue for 2016 of more than $1.2 billion.

20. As part of its business, Equifax creates, maintains, and sells credit reports and "credit scores" regarding individual consumers. Credit reports may contain an individual's full social security number, date of birth, current and prior residential addresses, employment history, balance and payment information for financial accounts, as well as status of accounts as open or closed, and information regarding bankruptcies, judgments, liens, and other sensitive information. A credit score is a number, derived pursuant to a proprietary formula and based on information in an individual's credit report, that is intended to indicate whether an individual is likely to repay debts.

21. Third parties use credit reports and credit scores to make highly consequential decisions affecting California consumers, including regarding qualification for mortgages, car loans, student loans, credit cards, and other forms of credit, as well as checking accounts, insurance and rate of insurance premiums, cellular phone service, and qualifications to rent an apartment.

22. Equifax is one of the three major credit reporting agencies that virtually all banks and other financial entities, businesses, insurance companies, and landlords use to assess the credit-worthiness of individuals seeking credit, insurance, goods and services, and rental housing. A consumer has no ability to dictate which of the three major credit reporting agencies these entities use to assess the consumer's credit-worthiness.

23. Equifax also sells to consumers credit monitoring services, "identity theft assistance" and identity theft insurance, which Equifax advertises as services that provide the consumer a "greater

//

sense of comfort" with respect to the security of their personal information – personal information that Equifax collects, maintains as computerized data in its systems, and uses for its business purposes.

The Data Breach

24. At all relevant times, Equifax maintained a publicly available website at www.equifax.com.

25. This website includes publicly available web pages directed to consumers, including California residents. Among these web pages is one through which Equifax invites consumers to submit information to initiate and support a formal dispute regarding the accuracy of information in their credit reports (the "Dispute Portal").

26. Equifax maintained computerized databases containing personal information, including names, addresses, full social security numbers, dates of birth, and for some consumers, driver's license numbers and credit card numbers, belonging to at least 143 million United States consumers, including more than 15 million California residents. Equifax's computerized databases of consumer personal information were, and continue to be, accessible directly or indirectly through the Dispute Portal (the "Exposed Information"). The Exposed Information was not limited to information of those consumers who had used the Dispute Portal, but included sensitive and personal information that Equifax maintained for a larger group of consumers.

27. Although the Exposed Information was accessible through a publicly available website, Equifax did not encrypt this information in its databases and systems. Nor did Equifax impose multiple and varying layers of security for some of the more sensitive consumer information, such as full social security numbers, driver's license numbers, and credit card numbers.

28. Beginning on or about May 13, 2017, and continuing through July 30, 2017, unauthorized third parties infiltrated Equifax's computer system via the Dispute Portal. Having gained access to consumer data in Equifax's databases, these unauthorized persons accessed and obtained the Exposed Information from Equifax's network. There have been unconfirmed reports that hackers claiming to have credit-card data from Equifax attempted in August 2017, to sell the data in online forums.

//

Equifax Ignored Threats By Hackers To Its Databases Despite Warnings Of Its System's Vulnerability

29. On or about September 13, 2017, Equifax published a statement on its website, https://www.equifaxsecurity2017.com, stating that the Data Breach resulted when "criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638."

30. Apache Struts is open-source computer code available free on the internet and used to create web applications, *i.e.*, computer programs that run in a web browser.

31. At all relevant times, Equifax used Apache Struts, in whole or in part, to create, support, and/or operate its Dispute Portal.

32. As "open-source" code, Apache Struts is free and available for anyone to download, install, or integrate into their computer system. Apache Struts, like most open-source code, comes with no warranties of any kind, including warranties about its security. Accordingly, it is incumbent on companies that use Apache Struts – like Equifax – to determine whether the open-source code is appropriate and sufficiently secure for the company's purposes and to ensure that the code is kept up-to-date with available security patches and protected from known vulnerabilities.

33. There are, and at all relevant times have been, multiple well-known resources available to support companies relying on open-source code, including Apache Struts. These resources publicly announce security vulnerabilities discovered in open-source code, including Apache Struts, and compare the associated risks of such vulnerabilities and propose fixes.

34. At least four separate organizations published warnings about the vulnerability of Apache Struts to hackers months before the Data Breach.

35. One such organization, the MITRE Corporation, a "not-for-profit organization that operates research and development centers sponsored by the federal government," identifies computer code security vulnerabilities, including vulnerabilities in Apache Struts, using a Common Vulnerabilities and Exposures ("CVE") Identifier. On its website, MITRE states the CVE Identifier is the industry standard for identifying publicly known cyber security vulnerabilities. MITRE maintains a database of CVE identifiers and the vulnerabilities to which they correspond, available publicly and without cost at https://cve.mitre.org.

36. MITRE included the March Security Vulnerability in the vulnerability database it maintains, and documented various external website references to the vulnerability.[1]

37. A second resource, the Apache Software Foundation ("ASF"), is a non-profit corporation that created the Apache Struts code and regularly releases updated versions of Apache Struts that contain revised code to "patch" it against verified security vulnerabilities. ASF also releases Security Bulletins on its website regarding security flaws in Apache Struts, explaining the nature of the vulnerability and ways to resolve it. Since 2007, ASF has posted at least 53 such security bulletins for Apache Struts.

38. On March 7, 2017, ASF published notice in its online Security Bulletins S2-045 and S2-046 of the existence of the March Security Vulnerability in certain versions of Apache Struts.[2]

39. The ASF Security Bulletins were directed to "All Struts2 developers and users," and warned that the software was vulnerable to "Remote Code Execution," or "RCE." RCE refers to a method of hacking a public website whereby a hacker can send to the website computer code that allows the hacker to gain access to, and run commands on, the computer that stores the information supporting the website.

40. The ASF Security Bulletins assigned the March Security Vulnerability a "maximum security rating" of "critical." ASF recommended that users update the affected versions of Apache Struts to fix the vulnerability, or to implement other specific workarounds to avoid the vulnerability. See Exhibits 1 and 2.

41. A third public resource on data security vulnerability is the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST"), which maintains a free and publicly available National Vulnerability Database ("NVD") at http://nvd.nist.gov. The NVD

---

[1] Exhibit 5 is a copy of this MITRE bulletin (available at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638, last visited September 25, 2017).

[2] Attached to this Complaint as Exhibit 1 is the ASF Security Bulletin S2-045 (available at https://cwiki.apache.org/confluence/display/WW/S2-045, last visited September 25, 2017). Attached as Exhibit 2 is the ASF Security Bulletin S2-046 (available at https://cwiki.apache.org/confluence/display/WW/S2-046, last visited September 25, 2017. The vulnerability was assigned the CVE identifier "CVE-2017-5638" (the "March Security Vulnerability").

identifies security vulnerabilities, including open-source code, the risks such vulnerabilities pose, and ways to fix them.

42. On or about March 10, 2017, NIST published notice of the March Security vulnerability in its NVD.[3] This NIST notice states that the severity of the March Security Vulnerability had an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System ("CVSS"). A score of 10.0 is the highest possible severity score on either scale. The NIST notice also stated that an attack based on the March Security Vulnerability "[a]llows unauthorized disclosure of information," would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password) to exploit the vulnerability. The NIST notice also documented over twenty other website resources for advisories, solutions, and tools related to the March Security Vulnerability and how to fix it.

43. A fourth public resource of information regarding data security vulnerability, the United States Computer Emergency Readiness Team ("U.S. CERT"), is part of the United States Department of Homeland Security. U.S. CERT's responsibilities include provision of cyber security advice to Federal civil executive branch agencies and analysis of and response to violations of or threats to computer security. U.S. CERT analyzes data security incidents, and publishes weekly Vulnerability Bulletins that summarize new computer data vulnerability that was documented in NIST's U.S. National Vulnerability Database the previous week. The weekly Vulnerability Bulletins also contain patch information when available. U.S. CERT also posts Technical Alerts, providing "information about vulnerabilities, incidents, and trends that pose a significant risk, as well as mitigations to minimize loss of information and disruption of services." U.S. CERT's Vulnerability Bulletins and Technical Alerts are publicly available, at no cost, on its website. Members of the public, including data security personnel at entities such as Equifax, also may sign up to receive the

//

//

//

[3] Exhibit 3 is the NIST notice of the March Security vulnerability, available at https://nvd.nist.gov/vuln/detail/CVE-2017-5638, last visited on September 25, 2017.

weekly Vulnerability Bulletins and Technical Alerts in their email inboxes or may subscribe to U.S. CERT's RSS feed.[4]

44. On March 20, 2017, U.S. CERT issued a Vulnerability Bulletin (Bulletin SB17-079), identifying the March Security Vulnerability as a "High" severity vulnerability.[5]

45. Equifax admitted on or about September 13, 2017, that the Data Breach occurred as a result of intruders exploiting the March Security Vulnerability. On September 15, 2017, Equifax stated on its website that "[t]he particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017."

46. By March 7, 2017, or soon after, Equifax knew or should have known, by virtue of the publicly available ASF Security Bulletins, the NIST notice, the US CERT alert, and the MITRE vulnerability database, that the March Security Vulnerability existed in its Apache Struts code. In fact, in a notice posted on Equifax's website https://www.equifaxsecurity 2017.com, Equifax stated that "Equifax's Security organization was aware of this vulnerability" in Apache Struts in early March 2017.

47. By March 7, 2017, or soon after, Equifax knew or should have known, by virtue of the publicly available ASF Security Bulletins, the NIST notice, the US CERT alert, and the MITRE vulnerability database, that its websites, including the Dispute Portal, was susceptible to the March Security Vulnerability and vulnerable to unauthorized access to the sensitive and person consumer information Equifax maintained.

48. From March 2017 to at least July 30, 2017, Equifax continued to use an Apache Struts-based web application that was subject to the March Security Vulnerability, without effectively employing recommended patches, fixes or workarounds, and without otherwise hardening its systems or implementing any controls sufficient to avoid the March Security Vulnerability, safeguard the Exposed Information, or prevent the Data Breach.

---

[4] RSS (Rich Site Summary) is a format for delivering regularly changing web content directly to a user's device (computer, cellphone, etc.), without the need for the user to sign up for emails or newsletters.

[5] Exhibit 4 to this Complaint is an excerpt from U.S. CERT Bulletin SB17-079 (available at https://www.us-cert.gov/ncas/bulletins/SB17-079, last visited on September 25, 2017) (relevant entry highlighted).

49. Until at least July 29, 2017, Equifax did not detect or appropriately respond to evidence that unauthorized parties were accessing its computer systems and had access to the Exposed Information, and/or did not detect or appropriately respond to evidence that those parties were stealing the Exposed Information out of Equifax's computer system.

50. As a result of Equifax's actions and omissions, the Data Breach occurred, and criminals were able to access and likely steal the sensitive and personal data of 143 million consumers, including more than 15 million California residents.

Equifax's Failure To Timely And Fully Disclose The Data Breach

51. The Exposed Information constitutes "personal information" as defined by Civil Code section 1798.82(h) and (i). The CRA requires persons or businesses that maintain computerized data that includes personal information to notify the owner of that personal information of any "breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person." (Civil Code section 1798.82(b).) The CRA requires businesses that own or license the personal information of the business' customers to disclose "in the most expedient time possible and without unreasonable delay" any breach in the security of the business' data if the customer is a California resident "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (*Id.* at section 1798.82(a).) In either case, notification may be delayed "if a law enforcement agency determines that the notification will impede a criminal investigation." (*Id.* at section 1798.82(c).)

52. Equifax owns or licenses personal information of the customers to whom it has sold credit monitoring services and identity theft protection services. Equifax also maintains personal information of California residents who are not Equifax customers, but are customers of banks and other business entities that have furnished the consumer's personal information to Equifax.

53. The Data Breach experienced by Equifax was a "breach of the security of the system" of Equifax's computerized data bases, as defined by Civil Code section 1798.82(g).

54. By July 29, 2017, or soon thereafter, Equifax knew or should have known that the "personal information" of California residents maintained in Equifax's data bases was accessed and

likely acquired by an unauthorized person, and thus had a duty under Civil Code section 1798.82(b) to immediately provide notice to the owners of that information. But Equifax did not announce or otherwise provide notice of the Data Breach until September 7, 2017, at which time Equifax posted notice of the Data Breach on its website[6] and issued press releases.

55. Beginning on September 7, 2017, Equifax has issued statements explaining its actions following its detection of suspicious network traffic on its site on July 29, 2017. In none of Equifax's public statements has it stated that notification of the breach was delayed as a result of a law enforcement investigation, even though the CRA, Civil Code section 1798.82(d)(2)(D) requires that such information be included in any notification of the breach.

56. As a result of Equifax's delay in notifying the owners of the personal information that was accessed in the Data Breach, millions of California consumers were prevented from acting quickly to protect against identify theft and financial fraud.

FIRST CAUSE OF ACTION

AGAINST EQUIFAX, INC. AND DOES 1 THROUGH 20 FOR VIOLATION OF BUSINESS AND PROFESSIONS CODE §§ 17200, *et seq.*

57. The People incorporate by reference the allegations set forth in paragraphs 1 through 56 above, as if those allegations were fully set forth herein.

58. California Business and Professions Code section 17200 prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."

59. From at least March 7, 2017 to the present, Defendant Equifax and Does 1 through 20, have engaged in and continue to engage in, unlawful, unfair and/or fraudulent business acts and practices in violation of Business and Professions Code section 17200 *et seq.*, including but not limited to the following:

//

---

[6] Attached as Exhibit 6 to this Complaint is a true and correct copy of the notice posted by Equifax on its website on September 7, 2017 (available at: https://web.archive.org/web/20170907233841/https://www.equifaxsecurity2017.com/consumer-notice, and at https://web.archive.org/web/20170907233843/https://www.equifaxsecurity2017.com/frequently-asked-questions, both pages last visited September 25, 2017).

a. Defendant has violated and continues to violate the Civil Code section 1798.81.5(b) by failing to "implement and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect the personal information [of California residents] from unauthorized access, destruction, use, modification, or disclosure."

i. Defendant Equifax, Inc. is a "business" as defined in Civil Code section 1798.80(a).

ii. In databases that Equifax owns and maintains for the purpose of its business activities, it maintains "personal information," as that term is defined by Civil Code sections 1798.80(e) and 1798.81.5(d)(1), of residents of California. Defendant maintains such personal information without encryption and in unredacted form.

iii. Defendant Equifax "owns" personal information of California consumers who have purchased credit monitoring or other services from Equifax, because such consumers provide personal information to Equifax, which stores such personal information in its computerized databases for the purpose of using it in transactions with the consumers. (Civil Code sections 1798.80(c) and 1798.81.5(a)(2).)

iv. Defendant Equifax also "maintains" personal information of California consumers whose personal information has been provided to Equifax by banks and other financial institutions, and by businesses pursuant to agreements between Equifax and those businesses. (Civil Code section 1798.81.5(a)(2).)

v. As such, Defendant Equifax is a business that "owns, licenses, or maintains personal information about a California resident," and is required by the CRA to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." (Civil Code section 1798.81.5(b).)

vi. The California Legislature has stated: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section [Civil Code section 1798.81.5] is to encourage businesses that own,

//

license, or maintain personal information about Californians to provide reasonable security for that information." (Civil Code section 1798.81.5(a)(1).)

vii. Defendant Equifax has violated Civil Code section 1798.81.5(b), and California public policy as stated by Civil Code section 1798.81.5(a)(1), by failing to maintain and implement reasonable security procedures and practices to protect from unauthorized access, destruction, use, modification, or disclosure the personal information of California residents that Equifax maintains in databases it owns and controls. Equifax has violated this provision of the CRA by its following actions and omissions:

(1) Equifax collected the sensitive personal information of California consumers and maintained that personal information in its databases in unencrypted and unredacted form.

(2) Equifax employed open-source computer code to create its Dispute Portal without implementing processes to keep itself informed of vulnerabilities of that open-source code to unauthorized intrusion;

(3) Equifax knew or should have known by at least March 7, 2017 that the Apache Struts computer code it used to create and operate its Dispute Portal contained a vulnerability that criminals could exploit to gain access to the sensitive personal information that Equifax maintained in its system. Nonetheless, Equifax did not timely or effectively implement the patches or fixes for the March Security Vulnerability that were publicly announced and made available on March 7, 2017.

(4) Nor did Equifax implement any security procedures and practices such as encrypting the personal data in its system, implementing additional layers of security, segmenting the data into separate data bases to prevent intruders from being able to access all of the personal information maintained about each consumer, or otherwise harden its system of personal information databases against unauthorized intrusion and access.

b. Defendant violated Civil Code section 1798.82(a) and (b) by failing to provide timely notice of the data breach to adversely affected California consumers:

i. The Exposed Information Equifax maintained in its computerized databases is "personal information" as defined by Civil Code sections 1798.82(h) and (i).

ii. The CRA requires an entity that conducts business in California and owns or licenses computerized data that includes personal information to disclose any breach of the security of its data system following discovery or notification of the breach in the security of the data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure "shall be made in the most expedient time possible and without unreasonable delay." (Civil Code section 1798.82(a).) The timing of the disclosure required by this subsection may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation, and to permit "any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." (*Id.*)

iii. Defendant Equifax is subject to the disclosure requirements of Civil Code section 1798.82(a) with respect to the personal information it has obtained from customers who have purchased credit monitoring services or other financial management services from Equifax.

iv. The CRA requires an entity that conducts business in California and maintains computerized data that includes personal information that the business does not own to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person." (Civil Code section 1798.82(b).) The timing of the required disclosure may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. (*Id.* at section 1798.82(c).)

v. Defendant Equifax is subject to the disclosure requirements of Civil Code section 1798.82(b) with respect to California consumers' personal information Equifax

//

maintains as computerized data, and which it obtained from banks, other financial entities, and businesses in the course of its business activities.

vi. The March 2017 Data Breach experienced by Equifax constituted a "breach of the security of [Equifax's] system" of computerized data, as defined by Civil Code section 1798.82(g), triggering Equifax's notification obligations under Civil Code sections 1798.82(a) and (b).

vii. The notice of breach required by Civil Code section 1798.82(a) and (b) may be provided as written notice, electronic notice, or by "substitute notice" if the business "demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information." (Civil Code section 1798.82(j).)

viii. Substitute notice requires email notification to affected persons for whom the business has an email address, "conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the . . . business, ..." and "notification to major statewide media." (Civil Code section 1798.82(j).)

ix. Defendant Equifax has not provided written notice to the California residents whose personal information was accessed. Because the number of California residents affected by the Data Breach is in excess of 15 million persons, Equifax may comply with the CRA by providing "substitute notice."

x. In violation of Civil Code section 1798.82(a) and (b), Defendant Equifax failed to provide timely notice of the Data Breach to the consumers whose personal information was accessed:

(1) Equifax knew or should have known as of July 29, 2017 or shortly thereafter that it had suffered a breach of the security of its system of computerized data containing consumer's personal information, but delayed providing notice of the Data Breach to the public or to the

//

affected consumers for six weeks, until September 7, at which time it posted information on its website and issued a press release.

(2) Equifax's delay in providing notification of the Data Breach did not result from a law enforcement agency's determination that the notification would impede a criminal investigation. Equifax's delay in providing notice was not authorized under Civil Code section 1798.82(c).

c. Defendant Equifax violated, and continues to violate Civil Code section 1798(d), by failing to provide to the consumers whose personal information was accessed the information that is statutorily mandated, and by including in the notice that it has provided unauthorized categories of information that are confusing and misleading for consumers:

i. The Data Breach experienced by Equifax was a breach of the security of Equifax's system of computerized databases containing the personal information of California consumers, as defined by Civil Code sections 1798.82(g), (h), and (i). Equifax thus was required by California law to provide those consumers the information mandated by Civil Code section 1798.82(d).

ii. In violation of Civil Code section 1798.82(d)(2)(D), neither the substitute notice Equifax posted on its website on September 7, 2017, nor any of the revised versions of this notice Equifax has posted subsequently, state "whether notification was delayed as a result of a law enforcement investigation," even though that information was and remains available to Equifax.

iii. The notice Equifax posted on its website on September 7, 2017 was not titled "Notice of Data Breach," and did not present the required information in plain language under the five headings specified in Civil Code section 1798.82(d)(1) or under the two headings authorized in Civil Code section 1798.82(d)(3), but instead buried the information required to be provided among a litany of unauthorized headings, including headings of more interest to investors than to affected consumers. An example of such a confusing and unauthorized heading is: "Are Equifax's core consumer or commercial credit reporting databases

impacted?," with the response: "We have found no evidence of unauthorized activity in Equifax's core consumer or commercial credit reporting databases." This information, which does not define what data is included in Equifax's "core consumer or commercial credit reporting databases" is confusing and misleading to California consumers, who might misunderstand the question and answer as indicating that there was no unauthorized activity in databases containing their personal data.

iv. In violation of Civil Code section 1798.82(d)(2)(E), the September 7, 2017 notice did not describe the breach incident as involving the Apache Struts software code, or the March Security Vulnerability, even though Equifax knew this information at the time it posted the notice of breach. Equifax did not publicly provide this information until September 13, 2017, when it confirmed that the "vulnerability was Apache Struts CVE-2017-5638" [the March Security Vulnerability].

v. In violation of Civil Code section 1798.82(d)(2)(C), the September 7, 2017 notice did not include a statement of the date on which notice was given. Revised versions of the notice that Equifax has posted on its website after September 7, 2017 do not include any statement of the date on which notice was initially given.

60. Equifax's unlawful delay in providing notice of the breach to California consumers, and its failure to provide complete, plain and clear information in the delayed notice it eventually posted on its website, prevented the more than 15 million affected California consumers from taking immediate action to protect themselves from the risk of identity theft and fraud resulting from the Data Breach and from Equifax's failure to take reasonable steps to secure these consumers' sensitive and personal data.

61. Defendants' acts and practices as set forth in this Complaint are unfair business practices because they offend established public policy, as expressly stated in Civil Code section 1798.81.5(a)(1), and cause harm that greatly outweighs any benefits associated with those practices. In addition, these business practices are unscrupulous, immoral, and so unfair as to shock the conscience.

//

PRAYER FOR RELIEF

For the reasons set forth above, Plaintiff prays for relief as follows:

1. That, pursuant to Business & Professions Code section 17206, the Court assess a civil penalty in an amount up to two thousand, five hundred dollars for each violation of section 17200 by each of Defendant Equifax, Inc. and Defendants Does 1 through 20;

2. That, pursuant to Business & Professions Code sections 17203 and 17204, the Court award provisional and final remedies against Defendants Equifax and Does 1 through 20, including, without limitation, an injunction prohibiting Defendants from failing to comply with the mandate of Civil Code section 1798.81.5 to implement and maintain reasonable security procedures and practices appropriate to the highly sensitive and personal information about California residents that Defendants own or maintain in their computerized databases; and prohibiting Defendants from failing to provide complete notice to affected California consumers as required by Civil Code section 1798.82;

3. That, pursuant to Business & Professions Code section 17203, the Court award restitution for those California consumers who purchased credit monitoring services from Equifax prior to September 7, 2017;

4. That the Court award costs of suit; and

5. That the Court grant any further and additional relief the Court deems proper.

Dated: September 26, 2017

DENNIS J. HERRERA
City Attorney
RONALD P. FLYNN
YVONNE R. MERÉ
KRISTINE POPLAWSKI
KENNETH WALCZAK

Deputy City Attorneys

By: _____
YVONNE R. MERÉ
Deputy City Attorney

Attorneys for Plaintiff
PEOPLE OF THE STATE OF CALIFORNIA

EXHIBIT 1

Apache Struts 2 Documentation

CHILD PAGES

Security Bulletins

S2-045

Pages / Home / Security Bulletins

S2-045

Created by Lukasz Lenart, last modified by Rene Gielen on Mar 19, 2017

Summary

Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible RCE when performing file upload based on Jakarta Multipart parser
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.3.32 or Struts 2.5.10.1
Affected Software	Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10
Reporter	Nike Zheng <nike dot zheng at dbappsecurity dot com dot cn>
CVE Identifier	CVE-2017-5638

Problem

It is possible to perform a RCE attack with a malicious `Content-Type` value. If the `Content-Type` value isn't valid an exception is thrown which is then used to display an error message to a user.

Solution

If you are using Jakarta based file upload Multipart parser, upgrade to Apache Struts version 2.3.32 or 2.5.10.1. You can also switch to a different implementation of the Multipart parser.

Backward compatibility

No backward incompatibility issues are expected.

Space tools

Workaround

Implement a Servlet filter which will validate `Content-Type` and throw away request with suspicious values not matching `multipart/form-data`.

Other option is to remove the File Upload Interceptor from the stack, just define your own custom stack and set it as a default - please read How do we configure an Interceptor to be used with every Action. This will work only for Struts 2.5.8 - 2.5.10.

```
<interceptors>
    <interceptor-stack name="defaultWithoutUpload">
        <interceptor-ref name="exception"/>
        <interceptor-ref name="alias"/>
        <interceptor-ref name="servletConfig"/>
        <interceptor-ref name="i18n"/>
        <interceptor-ref name="prepare"/>
        <interceptor-ref name="chain"/>
        <interceptor-ref name="scopedModelDriven"/>
        <interceptor-ref name="modelDriven"/>
        <interceptor-ref name="checkbox"/>
        <interceptor-ref name="datetime"/>
        <interceptor-ref name="multiselect"/>
        <interceptor-ref name="staticParams"/>
        <interceptor-ref name="actionMappingParams"/>
        <interceptor-ref name="params"/>
        <interceptor-ref name="conversionError"/>
        <interceptor-ref name="validation">
            <param name="excludeMethods">input,back,cancel
        </interceptor-ref>
        <interceptor-ref name="workflow">
            <param name="excludeMethods">input,back,cancel
        </interceptor-ref>
        <interceptor-ref name="debugging"/>
    </interceptor-stack>
</interceptors>
<default-interceptor-ref name="defaultWithoutUpload"/>
```

8 people like this

No labels

EXHIBIT 2

Apache Struts 2 Documentation

CHILD PAGES

Security Bulletins

S2-046

S2-046

Created by Lukasz Lenart, last modified on Sep 22, 2017

Summary

Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible RCE when performing file upload based on Jakarta Multipart parser
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.3.32 or Struts 2.5.10.1
Affected Software	Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10
Reporter	Chris Frohoff <cfrohoff at qualcomm dot com>, Nike Zheng <nike dot zheng at dbappsecurity dot com dot cn>, Alvaro Munoz <alvaro dot munoz at hpe dot com>
CVE Identifier	CVE-2017-5638

Problem

It is possible to perform a RCE attack with a malicious `Content-Disposition` value or with improper `Content-Length` header. If the `Content-Disposition` / `Content-Length` value is not valid an exception is thrown which is then used to display an error message to a user. This is a different vector for the same vulnerability described in S2-045 (CVE-2017-5638).

Solution

If you are using Jakarta based file upload Multipart parser, upgrade to Apache Struts version 2.3.32 or 2.5.10.1.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

You can switch to a different implementation of the Multipart parser. We have already prepared two plugins which can be used as a drop-in solution, please find them here. You can use them when you are running the Apache Struts 2.3.8 - 2.5.5 (in case of using the default Jakarta multipart parser) or the Apache Struts 2.3.20 - 2.5.5 (when using an alternative jakarta-stream multipart parser).

Another option is to remove the File Upload Interceptor from the stack, just define your own custom stack and set it as a default - please read How do we configure an Interceptor to be used with every Action. This will work only for Struts 2.5.8 - 2.5.10.

```
<interceptors>
    <interceptor-stack name="defaultWithoutUpload">
        <interceptor-ref name="exception"/>
        <interceptor-ref name="alias"/>
        <interceptor-ref name="servletConfig"/>
        <interceptor-ref name="i18n"/>
        <interceptor-ref name="prepare"/>
        <interceptor-ref name="chain"/>
        <interceptor-ref name="scopedModelDriven"/>
        <interceptor-ref name="modelDriven"/>
        <interceptor-ref name="checkbox"/>
        <interceptor-ref name="datetime"/>
        <interceptor-ref name="multiselect"/>
        <interceptor-ref name="staticParams"/>
        <interceptor-ref name="actionMappingParams"/>
        <interceptor-ref name="params"/>
        <interceptor-ref name="conversionError"/>
        <interceptor-ref name="validation">
            <param name="excludeMethods">input,back,cancel
        </interceptor-ref>
        <interceptor-ref name="workflow">
            <param name="excludeMethods">input,back,cancel
        </interceptor-ref>
        <interceptor-ref name="debugging"/>
    </interceptor-stack>
</interceptors>
<default-interceptor-ref name="defaultWithoutUpload"/>
```

2 people like this

No labels

EXHIBIT 3

CVE-2017-5638 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The Jakarta Multipart parser in Apache Struts 2.2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Source: MITRE **Last Modified:** 09/22/2017 View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2017-5638
Original release date: 03/10/2017
Last revised: 09/22/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (legend)
Impact Score: 6.0
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 HIGH
Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource	Type	Source	Name
http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html	Technical Description; Third Party Advisory	External Source	MISC	http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/	Technical Description; Third Party Advisory	External Source	MISC	http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/
http://www.eweek.com/security/apache-struts-vulnerability-under-attack.html	Press/Media Coverage	External Source	MISC	http://www.eweek.com/security/apache-struts-vulnerability-under-attack.html
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html		External Source	CONFIRM	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
http://www.securityfocus.com/bid/96729	Third Party Advisory; VDB Entry	External Source	BID	96729
http://www.securitytracker.com/id/1037973		External Source	SECTRACK	1037973
https://arstechnica.com/security/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/	Press/Media Coverage	External Source	MISC	https://arstechnica.com/security/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/
https://cwiki.apache.org/confluence/display/WW/S2-045	Mitigation; Vendor Advisory	External Source	CONFIRM	https://cwiki.apache.org/confluence/display/WW/S2-045
https://cwiki.apache.org/confluence/display/WW/S2-046		External Source	CONFIRM	https://cwiki.apache.org/confluence/display/WW/S2-046
https://exploit-db.com/exploits/41570	Exploit; VDB Entry	External Source	EXPLOIT-DB	41570
https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=352306493971e7d5a756d51780d57a76eb1f519a	Patch	External Source	CONFIRM	https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=352306493971e7d5a756d51780d57a76eb1f519a
https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=6b8272ce47160036ed120a48345d9aa884477228	Patch	External Source	CONFIRM	https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=6b8272ce47160036ed120a48345d9aa884477228
https://github.com/mazen160/struts-pwn	Exploit	External Source	MISC	https://github.com/mazen160/struts-pwn
https://github.com/rapid7/metasploit-framework/issues/8064	Exploit	External Source	MISC	https://github.com/rapid7/metasploit-framework/issues/8064
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03733en_us		External Source	CONFIRM	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03733en_us
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03749en_us		External Source	CONFIRM	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03749en_us
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03723en_us		External Source	CONFIRM	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03723en_us

https://isc.sans.edu/diary/22169	Technical Description; Third Party Advisory	External Source MISC	https://isc.sans.edu/diary/22169
https://nmap.org/nsedoc/scripts/http-vuln-cve2017-5638.html	Third Party Advisory	External Source MISC	https://nmap.org/nsedoc/scripts/http-vuln-cve2017-5638.html
https://packetstormsecurity.com/files/141494/S2-45-poc.py.txt	Exploit; VDB Entry	External Source MISC	https://packetstormsecurity.com/files/141494/S2-45-poc.py.txt
https://struts.apache.org/docs/s2-045.html		External Source CONFIRM	https://struts.apache.org/docs/s2-045.html
https://struts.apache.org/docs/s2-046.html		External Source CONFIRM	https://struts.apache.org/docs/s2-046.html
https://support.lenovo.com/us/en/product_security/len-14200		External Source CONFIRM	https://support.lenovo.com/us/en/product_security/len-14200
https://twitter.com/theog150/status/841146956135124993	Third Party Advisory	External Source MISC	https://twitter.com/theog150/status/841146956135124993
https://www.exploit-db.com/exploits/41614/		External Source EXPLOIT-DB	41614
https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/		External Source MISC	https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/
https://www.symantec.com/security-center/network-protection-security-advisories/SA145		External Source CONFIRM	https://www.symantec.com/security-center/network-protection-security-advisories/SA145

Technical Details

Vulnerability Type (View All)

- **Input Validation (CWE-20)**

Vulnerable software and versions Switch to CPE 2.2

Configuration 1

OR

- cpe:2.3:a:apache:struts:2.3.5:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.6:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.7:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.8:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.9:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.10:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.11:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.12:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.13:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.14:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.14.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.14.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.14.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.15:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.15.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.15.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.15.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.16:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.16.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.16.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.16.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.17:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.19:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.20:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.20.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.20.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.20.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.21:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.22:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.23:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.24:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.24.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.24.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.24.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.25:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.26:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.27:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.28:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.28.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.29:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.30:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.3.31:*:*:*:*:*:*:*

Configuration 2

OR

- cpe:2.3:a:apache:struts:2.5:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.4:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.5:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.6:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.7:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.8:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.9:*:*:*:*:*:*:*
- cpe:2.3:a:apache:struts:2.5.10:*:*:*:*:*:*:*

Denotes Vulnerable Software

Change History 14 change records found - show changes

EXHIBIT 4

Bulletin (SB17-079)

TLP:WHITE

Vulnerability Summary for the Week of March 13, 2017

Original release date: March 20, 2017

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable buffer overflow / underflow vulnerability in the Primetime TVSDK that supports customizing ad information. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-2997 BID CONFIRM
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK API functionality related to timeline interactions. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-2998 BID CONFIRM
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK functionality related to hosting playback surface. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-2999 BID CONFIRM
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to garbage collection in the ActionScript 2 VM. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-3001 BID CONFIRM
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-3002 BID CONFIRM
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-3003 BID CONFIRM
alienvault -- ossim	The logcheck function in session.inc in AlienVault OSSIM before 5.3.1, when an action has been created, and USM before 5.3.1 allows remote attackers to bypass authentication and consequently obtain sensitive information, modify the application, or execute arbitrary code as root via an "AV Report Scheduler" HTTP User-Agent header.	2017-03-15	7.5	CVE-2016-7955 BUGTRAQ MISC CONFIRM
apache -- struts	The Jakarta Multipart parser in Apache Struts 2.2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.	2017-03-10	10.0	CVE-2017-5638 MISC MISC MISC BID MISC CONFIRM EXPLOIT-DB CONFIRM CONFIRM MISC MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Patch Info
				MISC MISC
azure_dex -- data_expert_ultimate	In Azure Data Expert Ultimate 2.2.16, the SMTP verification function suffers from a buffer overflow vulnerability, leading to remote code execution. The attack vector is a crafted SMTP daemon that sends a long 220 (aka "Service ready") string.	2017-03-10	7.5	CVE-2017-6506 MISC BID EXPLOIT-DB
bitlbee -- bitlbee	Use-after-free vulnerability in bitlbee-libpurple before 3.5 allows remote servers to cause a denial of service (crash) or possibly execute arbitrary code by causing a file transfer connection to expire.	2017-03-14	7.5	CVE-2016-10188 MLIST MLIST BID CONFIRM
bitlbee -- bitlbee-libpurple	bitlbee-libpurple before 3.5.1 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) and possibly execute arbitrary code via a file transfer request for a contact that is not in the contact list. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-10189.	2017-03-14	7.5	CVE-2017-5668 MLIST MLIST BID CONFIRM CONFIRM
cambium_networks -- cnpilot_r200_series_firmware	On Cambium Networks cnPilot R200/201 devices before 4.3, there is a vulnerability involving the certificate of the device and its RSA keys, aka RBN-183.	2017-03-10	10.0	CVE-2017-5859 CONFIRM
embedthis -- goahead	A command-injection vulnerability exists in a web application on a custom-built GoAhead web server used on Foscam, Vstarcam, and multiple white-label IP camera models. The mail-sending form in the mail.htm page allows an attacker to inject a command into the receiver1 field in the form; it will be executed with root privileges.	2017-03-13	9.0	CVE-2017-5675 MISC MISC
f-secure -- software_updater	F-Secure Software Updater 2.20, as distributed in several F-Secure products, downloads installation packages over plain http and does not perform file integrity validation after download. Man-in-the-middle attackers can replace the file with their own executable which will be executed under the SYSTEM account. Note that when Software Updater is configured to install updates automatically, it checks if the downloaded file is digitally signed by default, but does not check the author of the signature. When running in manual mode (default), no signature check is performed.	2017-03-11	9.3	CVE-2017-6466 MISC BID
imagemagick -- imagemagick	Memory leak in the IsOptionMember function in MagickCore/option.c in ImageMagick before 6.9.2-2, as used in ODR-PadEnc and other products, allows attackers to trigger memory consumption.	2017-03-14	7.8	CVE-2016-10252 CONFIRM CONFIRM CONFIRM
imagemagick -- imagemagick	The gnuplot delegate functionality in ImageMagick before 6.9.4-0 and GraphicsMagick allows remote attackers to execute arbitrary commands via unspecified vectors.	2017-03-15	7.5	CVE-2016-5239 MISC MLIST BID
libgd -- libgd	Integer underflow in the _gdContributionsAlloc function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors related to decrementing the u variable.	2017-03-15	7.5	CVE-2016-10166 CONFIRM MLIST MLIST BID CONFIRM
logback -- logback	QOS.ch Logback before 1.2.0 has a serialization vulnerability affecting the SocketServer and ServerSocketReceiver components.	2017-03-13	7.5	CVE-2017-5929 CONFIRM
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	2017-03-16	7.6	CVE-2017-0034 BID CONFIRM
microsoft -- internet_explorer	The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." This vulnerability is different from that described in CVE-2017-0130.	2017-03-16	7.6	CVE-2017-0040 BID CONFIRM
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." This vulnerability is different from those described in CVE-2017-0018 and CVE-2017-0037.	2017-03-16	7.6	CVE-2017-0149 BID CONFIRM
microsoft -- server_message_block	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	2017-03-16	9.3	CVE-2017-0143 BID CONFIRM

EXHIBIT 5

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Section Menu

CVE IDs
- CVEnew Twitter Feed
- Other Updates & Feeds

Request a CVE ID
- Contact a CVE Numbering Authority (CNA)
- Contact Primary CNA (MITRE) – CVE Request web form
- Reservation Guidelines

CVE LIST (all existing CVE IDs)
- Downloads
- Search CVE List
- Search Tips
- View Entire CVE List (html)
- Reference Key/Maps

NVD Advanced CVE Search
- CVE ID Scoring Calculator

CVE Numbering Authorities
- Participating CNAs
- Documentation for CNAs
- Requesting CVE IDs from CNAs
- Become a CNA

Documentation
- About CVE IDs
- Terminology
- Editorial Policies
- Terms of Use

ALSO SEE
- Common Vulnerability Scoring System (CVSS)
- Common Vulnerability Reporting Framework (CVRF)
- U.S. National Vulnerability Database (NVD)

Printer-Friendly View

CVE-ID

CVE-2017-5638 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:41570
- URL:https://exploit-db.com/exploits/41570
- EXPLOIT-DB:41614
- URL:https://www.exploit-db.com/exploits/41614/
- MISC:http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
- MISC:http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/
- MISC:https://github.com/rapid7/metasploit-framework/issues/8064
- MISC:https://isc.sans.edu/diary/22169
- MISC:https://github.com/mazen160/struts-pwn
- MISC:https://nmap.org/nsedoc/scripts/http-vuln-cve2017-5638.html
- MISC:https://packetstormsecurity.com/files/141494/S2-45-poc.py.txt
- MISC:http://www.eweek.com/security/apache-struts-vulnerability-under-attack.html
- MISC:https://arstechnica.com/security/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/
- MISC:https://twitter.com/theog150/status/841146956135124993
- MISC:https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/
- CONFIRM:https://cwiki.apache.org/confluence/display/WW/S2-045
- CONFIRM:https://cwiki.apache.org/confluence/display/WW/S2-046
- CONFIRM:https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=352306493971e7d5a756d61780d57a76eb1f519a

- CONFIRM:https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=6b8272ce47160036ed120a48345d9aa884477228
- CONFIRM:https://struts.apache.org/docs/s2-045.html
- CONFIRM:https://struts.apache.org/docs/s2-046.html
- CONFIRM:https://support.lenovo.com/us/en/product_security/len-14200
- CONFIRM:https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03733en_us
- CONFIRM:https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03723en_us
- CONFIRM:https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03749en_us
- CONFIRM:http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM:https://www.symantec.com/security-center/network-protection-security-advisories/SA145
- BID:96729
- URL:http://www.securityfocus.com/bid/96729
- SECTRACK:1037973
- URL:http://www.securitytracker.com/id/1037973

Assigning CNA

Apache Software Foundation

Date Entry Created

20170129	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20170129)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

BACK TO TOP

EXHIBIT 6

To enroll in complimentary identity theft protection and credit file monitoring, click here.

Cybersecurity Incident & Important Consumer Information

At Equifax, protecting the security of the information in our possession is a responsibility we take very seriously. This is to notify you of a data security incident that may have exposed some of your personal information, including your Social Security number and other identifying information. This site explains the incident and steps Equifax has undertaken to address it. In addition, we provide guidance below on what you can do to protect your personal information.

I. What Happened

On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files. Upon discovery, we acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm which has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.

II. What Information Was Involved

Most of the consumer information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 consumers and certain dispute documents, which included personal identifying information, for approximately 182,000 consumers were accessed. In addition to this site, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. We have found no evidence of unauthorized access to Equifax's core consumer or commercial credit reporting databases.

III. What We Are Doing

Upon learning of this incident, Equifax took steps to stop the intrusion, and engaged an independent cybersecurity firm to forensically investigate and determine the scope. Equifax also engaged the cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

Equifax is focused on consumer protection and has established a dedicated website, www.equifaxsecurity2017.com to help consumers. We have provided a tool on this site for you to determine if your information was potentially impacted by this incident. To find out if you are potentially impacted, please go to www.equifaxsecurity2017.com, and click on "Potential Impact," and enter your last name and last 6 digits of your Social Security number.

We are also offering free identity theft protection and credit file monitoring to all U.S. consumers, even if you are not impacted by this incident. This offering, called TrustedID Premier, includes 3-Bureau credit monitoring of your Equifax, Experian and TransUnion credit reports; copies of your Equifax credit report; the ability to lock and unlock your Equifax credit report; identity theft insurance; and Internet scanning for your Social Security number – all complimentary to U.S. consumers for one year. To find out more information on this complimentary offer and to sign up, please click on the tab "Enroll" on this site. You must complete the enrollment process by November 21, 2017.

IV. What You Can Do

In addition to enrolling in identity theft protection and credit file monitoring, please see the "Identity Theft Prevention Tips" below, and the "State Information" tab of this site. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report. In addition, please monitor your account statements and report any unauthorized charges to your credit card companies and financial institutions.

V. For More Information

Equifax is committed to ensuring that your personal information is protected, and we apologize to our consumers and our business customers for the concern and frustration this incident causes. If you have additional questions, please call our dedicated call center at 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week.

Identity Theft Prevention Tips

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 2000

Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
888-766-0008	888-397-3742	800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

State Attorneys General: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report. Please also visit the "State Information" tab of this site.

EQUIFAX

Return to equifax.com

To enroll in complimentary identity theft protection and credit file monitoring, click here.

« Home

Cybersecurity Incident & Important Consumer Information

Consumer Notice FAQs Potential Impact Enroll TrustedID Premier Contact Us

General FAQs | FAQs for Consumers | FAQs for Investors

– What happened?

We identified a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. We discovered the unauthorized access and acted immediately to stop the intrusion. We promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. We also reported the criminal access to law enforcement and continue to work with authorities.

– When did the company learn of this incident?

We learned of the incident on July 29, 2017, and acted immediately to stop the intrusion and conduct a forensic review.

– Over what period of time did the unauthorized access occur?

Based on our investigation, the unauthorized access occurred from mid-May through July 2017.

– Who and how many people are affected?

This incident potentially impacts approximately 143 million U.S. consumers. We have established a dedicated website, www.equifaxsecurity2017.com, to help U.S. consumers determine if their information has been potentially impacted. As part of our investigation of this application vulnerability, we also identified unauthorized access to limited personal information for certain UK and Canadian residents. We will work with UK and Canadian regulators to determine appropriate next steps.

– What information may have been impacted?

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Criminals also accessed credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers. As part of our investigation of this application vulnerability, we also identified unauthorized access to limited personal information for certain UK and Canadian residents. We have found no evidence that personal information of consumers in any other country has been impacted.

– Are Equifax's core consumer or commercial credit reporting databases impacted?

We have found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

– Is the issue contained?

Yes, this issue has been contained.

- What are you doing to prevent this from happening again?

We have engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

- What steps should I immediately take?

To determine if your personal information may have been impacted and for steps to protect your information, please visit www.equifaxsecurity2017.com. We recommend that consumers be vigilant in reviewing their account statements and credit reports, and that they immediately report any unauthorized activity to their financial institutions. We also recommend that they monitor their personal information and visit the Federal Trade Commission's website, www.ftc.gov/idtheft, to obtain information about steps they can take to better protect against identity theft as well as information about fraud alerts and security freezes.

- Why am I learning about this incident through the media? Why didn't Equifax notify me directly?

Equifax issued a national press release in order to notify U.S. consumers of this incident and has established a website, www.equifaxsecurity2017.com, where U.S. consumers can receive further information.