

STATE OF INDIANA
COUNTY OF MARION

SS:

Marion County Circuit/Superior Court
CAUSE NO. _____

STATE OF INDIANA,)
)
Plaintiff,)
v.)
)
EQUIFAX INFORMATION)
SERVICES LLC,)
EQUIFAX CONSUMER)
SERVICES LLC and)
EQUIFAX INC.,)
Defendants.)

REQUEST FOR JURY TRIAL

COMPLAINT FOR CIVIL PENALTIES, INJUNCTIVE RELIEF, AND RESTITUTION

The State of Indiana, by Attorney General Curtis T. Hill, Jr. and Deputy Attorneys General Douglas Swetnam, Vanessa Voigt Gould, and Michael Eades, petitions the Court pursuant to the Indiana Disclosure of Security Breach Act, Ind. Code chapter 24-4.9-3-3 (“DSBA”) and the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-1 *et seq.* (“DCSA”) for civil penalties, costs, injunctive relief, consumer restitution and other relief.

I. INTRODUCTION

1. This case concerns a data breach at Equifax, one of the world’s largest credit reporting bureaus, between May 13, 2017 and July 30, 2017 that compromised sensitive personal information of 147.9 Million Americans, including 3.9 Million Indiana residents (“the 2017 Apache Struts Breach”). The U.S. House of Representatives Committee on Oversight and Government Reform investigation, published in December 2018, concluded the breach was “entirely preventable.” The committee observed, “Equifax Chief Executive Officer (CEO) Richard Smith embarked on an aggressive growth strategy, leading to the acquisition of multiple

companies, information technology (“IT”) systems, and data . . . [that] brought increasing complexity to Equifax’s IT systems, and expanded data security risks.”¹

2. CEO Smith’s twelve year transformation of Equifax went beyond acquisitions. He purposefully changed the culture of the company to emphasize a laser-like focus on revenue and profit, as he explained:

When I saw where I want to take the company in the future . . . I wanted to be a culture of meritocracy versus tenure so I'm asking people run harder. I don't care how long you've been here it's what did you do for the company yesterday. Some people got burnout and didn't want to go down that path. . . I didn't want to grow one or 3.2 percent a year. We want to do a 10% or more year which required more of people. So, over time people just self-opted out most of the time. We have 10,000 people today roughly around the world and . . . I'd say probably 20% or less of the people who are with us today were with us when we started and that's healthy.²

3. To execute on CEO Smith’s exacting demands, Equifax pursued aggressive cost-cutting measures which included the outsourcing of some of the company’s mission critical systems. To save expenses, the outsourcing contracts understaffed vital functions; further, the service level agreements within the contracts focused entirely on revenue enhancing metrics – like maintaining uptime – while either ignoring patching (software upgrade to fix bugs) and vulnerability remediation, or treating those responsibilities as relatively unimportant. As a result, the company incurred a decade-long information security deficit that accumulated beneath the surface like an iceberg. During CEO Smith’s tenure, the company encountered multiple occasions to change course, when the severity of its information security problems and potential solutions were clearly presented to senior executives and board members. During each of these critical opportunities, senior executives chose revenue over protecting the safety of consumers’

¹ United States House of Representatives Committee on Oversight and Government Reform, Majority Staff Report, 115th Congress, December 2018, p.2. See <https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf> last accessed May 1, 2019.

² <https://www.youtube.com/watch?v=1ZzqUnQg-Us> last accessed April 30, 2019.

sensitive personal information. Throughout this timeframe, Equifax represented to consumers that their information was secure, and that Equifax's payment systems were compliant with Payment Card Industry ("PCI") standards.

4. Perhaps most glaring, the system that was breached contained a payment card processing component that required the company to implement and maintain detailed PCI standards. This was a critical error in judgment. As Visa Chief Enterprise Risk Officer Ellen Ritchie explained, "no compromised entity has yet been found to be in compliance with PCI DSS [Data Security Standard] at the time of a breach," and that continues to be true. From at least 2006, Equifax knew the system involved in the 2017 Apache Struts Breach contained payment card processing, and thus, sensitive information gathered from Equifax's millions of consumers. From at least 2013, Equifax knew the system was storing payment card information in clear text, which was a known violation of the rules. Equifax knew it must be PCI compliant to accept payment cards. It knew PCI certification required Equifax to ensure all networks, applications and other IT technology that connected to, or that could impact the payment card processing system if those other systems were breached needed to comply with the rules. Despite its knowledge, Equifax made a conscious choice to break the rules, and continues to break the rules even today, continuing to expose consumers to risks without warning.

II. PARTIES

5. Plaintiff, State of Indiana, is authorized to bring this action and to seek injunctive and other statutory relief pursuant to Ind. Code § 24-5-0.5-4 and § 24-4.9-4-2.

6. The Attorney General is authorized to bring actions on behalf of the State of Indiana pursuant to Ind. Code § 4-6-3-2.

7. Equifax Information Services LLC is a wholly owned subsidiary of Equifax Inc. that organizes, assimilates and analyzes data used in consumer financial transactions.

8. Equifax Consumer Services LLC is a wholly owned subsidiary of Equifax Inc. that provides consumer-focused credit, financial and security services.

9. Defendant Equifax Inc. is a publicly-traded Georgia corporation with its principal place of business at 1550 Peachtree Street N.E., Atlanta, Georgia. Defendants Equifax Inc. and its wholly owned subsidiaries, Equifax Information Services LLC and Equifax Consumer Services LLC, are hereinafter collectively referenced as “Equifax”.

III. JURISDICTION AND VENUE

10. Defendant Equifax Inc. has been registered to do business in the State of Indiana since December 3, 1919.

11. Defendant Equifax Information Services LLC has been registered to do business in the State of Indiana since June 4, 2001.

12. Equifax was and remains involved in consumer transactions in Indiana, as defined by Indiana Code § 24-5-0.5-2.

13. Equifax is subject to the jurisdiction of an Indiana court pursuant to Ind. Trial R. 4.4(A) (1).

14. Venue is proper in this Court pursuant to Ind. Trial R. 75(A) (10).

IV. FACTS

A. Equifax as a Consumer Credit Reporting Agency

15. Equifax is one of three primary nationwide credit reporting bureaus in the United States and its information is used in nearly every aspect of Indiana residents’ economic lives, impacting whether they can buy a house, buy or lease a vehicle, obtain a credit card or loan,

obtain insurance, or get a job. Further, Equifax's consumer information determines the cost Indiana residents pay for the foregoing transactions.

16. Consumers do not choose to provide Equifax with the majority of sensitive personal data contained in their credit files, nor can consumers prevent Equifax from acquiring and profiting from the sensitive personal data in consumers' credit files.

17. As one of the select entities to operate as a credit bureau, Equifax "organizes, assimilates and analyzes data" on more than 820 million consumers, 91 million businesses, 278 million employee files, 5.75 billion trade credit files, and 201 million public records."³

18. As CEO Smith acknowledged, "When you have the size database we have it's very attractive to others." As one of the three primary credit-reporting agencies, Equifax had, and continues to have a heightened duty to implement and maintain strong security measures to protect that sensitive data.

**B. Equifax's Public Story of the 2017 Apache Struts Breach
Withheld Important Details**

What Equifax Told the Public

19. On September 7, 2017, Equifax issued a press release announcing it had experienced a "cybersecurity incident potentially impacting 143 Million U.S. consumers," and that "the unauthorized access occurred from mid-May through July 2017."⁴

20. Equifax further advised that the information accessed by the unauthorized intruders was primarily names with "Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers." In addition, Equifax revealed that the breach exposed

³ <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832> accessed January 22, 2019.

⁴ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>, last accessed January 19, 2019.

credit card numbers in plain text for approximately 209,000 consumers, and personal identifying information for approximately 182,000 U.S. consumers.

21. Equifax attempted to reassure consumers by stating in their press release that, “[t]he Company has found no evidence of unauthorized activity on Equifax’s core consumer or commercial credit reporting databases.”

22. According to the September 15th press release, the data breach incident involved its online dispute portal. Equifax first noticed suspicious network traffic on July 29, 2017.

23. After taking the dispute portal offline to examine it, Equifax determined the unauthorized intruders (“hackers”) had exploited a known “vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.”

24. The press release stated the intrusion of Equifax’s network occurred from May 13 through July 30, 2017.

25. On October 2, 2017, Equifax announced that a completed forensic review uncovered an additional 2.5 million U.S. customers affected by the data breach, bringing the total number of U.S. Consumers to 145.5 million.⁵

26. Within a period of eleven days in September, Equifax announced that three key executives were retiring: its Chief Information Officer (“CIO”), Chief Security Officer (“CSO”), and CEO Smith.

⁵<https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821> last accessed April 28, 2019.

27. On October 3, 2017, Equifax's Former CEO Smith testified before the House of Representatives Subcommittee on Digital Commerce and Consumer Protection about the 2017 Apache Struts Breach.⁶

28. In his preliminary statement, Former CEO Smith stated, "On March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") sent Equifax and many others a notice of the need to patch a particular vulnerability in certain versions of software used by other businesses. Equifax used that software, which is called 'Apache Struts,' in its online disputes portal, a website where consumers can dispute items on their credit report."⁷

29. Former CEO Smith testified the breach occurred due to, "a combination of human error and technological error." He claimed, "[t]he human error was the individual who is responsible for communicating in the organization to apply the patch did not."⁸

30. Five months after Former CEO Smith's testimony to Congress, and nearly a year after U.S. CERT notified Equifax of the Apache Struts vulnerability, Equifax confessed additional harm. On March 1, 2018, the last possible day for Equifax to submit its Form 10-K to the United States Securities and Exchange Commission ("SEC"), Equifax revealed an additional 2.4 million U.S. Consumers had been impacted by the breach, bringing the total affected to 147.9 million, roughly half the population of the United States. Simultaneous with its 10-K filing, Equifax issued a press release regarding the additional victims.⁹

⁶ <https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Smith-DCCP-Hrg-on-Oversight-of-the-Equifax-Data-Breach-Answers-for-Consumers-2017-10-03.pdf> last accessed April 28, 2019.

⁷ *Id.*

⁸ *Id.*

⁹ <https://investor.equifax.com/news-and-events/news/2018/03-01-2018-140531340> last accessed April 28, 2019 and <https://www.sec.gov/Archives/edgar/data/33185/000119312518065580/d530771d8k.htm> last accessed April 28, 2019.

What Equifax Failed to Disclose:

Executive Compensation Focused Solely on Revenue

31. From 2008, CEO Smith received no increases to his base pay of \$1.45 Million. All modifications to his pay were linked to the performance-based portion of his long term incentives, which were tied to operational earnings and earnings per share. As a result, CEO Smith, and therefore, Equifax, prioritized revenue above all other concerns, including the security of consumers' information.¹⁰

32. Similarly, the pay of Equifax's other senior executives was structured with the same emphasis on performance-based incentives, motivating them to prioritize revenue above all other considerations, including information security.

33. During his first year, CEO Smith received a bonus of \$1,813,630. By 2010, his total compensation had skyrocketed to \$9,804,936.00; \$11,203,711.00 in 2011; \$13,445,099.00 in 2012; \$10,515,558.00 in 2013; \$13,879,675.00 in 2014; \$12,922,711 in 2015, and \$14,964,563.00 in 2016.

34. Equifax's failure to disclose that the emphasis on performance came at the expense of essential information security infrastructure gave consumers a false sense of security.

Outsourcing to Reduce Cost and Increase Profitability

35. One key strategy for reducing cost and increasing profit was an aggressive use of outsourcing to "maintain our profitability in the face of pressure on revenues." Equifax entered a master agreement with Tata Consultancy Services ("Tata"), an India-based IT company, in 2007. Equifax disclosed the risk associated with its outsourcing strategy in its Form 10-K filed with the SEC the following year on February 27, 2008, noting that "operations could be disrupted if we

¹⁰ <https://investor.equifax.com/~media/Files/E/Equifax-IR/documents/presentation/investor-relations-presentation-august-2017.pdf> last accessed April 29, 2019.

do not successfully manage our service providers.” However, the 2008 Form 10-K also stated that “[s]afeguarding the privacy and security of consumer credit information ... is a top priority.” The outsourcing agreement with Tata, which related to the system impacted in the 2017 Apache Struts Breach, demonstrates the falsity of the promised priority of security of consumer information, and the falsity of Equifax’s narrative that the 2017 Apache Struts Breach was an unforeseeable event.

36. The consumer portal Equifax described in its breach announcement was actually part of its Automated Consumer Interview System (“ACIS”) that is used by customer service representatives to access, add, or edit the information maintained in a system called the Automated Credit Report On-line (“ACRO”), Equifax’s primary credit reporting database. ACIS is one mechanism by which Equifax complies with the Fair Credit Reporting Act’s requirement to maintain procedures through which consumers can dispute and correct inaccurate or incomplete information in their consumer reports. 15 U.S.C. § 1681. In 2013, Equifax outsourced the development and maintenance of the ACIS system to Tata.

37. The contract identified the various components of the system for which Tata had responsibility, and included specific identification of the interaction with AnnualCreditReport.com, and the ACRO system, which is the mainframe system Equifax claimed in press releases was not impacted by the 2017 Apache Struts Breach.

38. The contract was based upon a fixed number of Tata’s employees, and limited the capacity to do the required work by the overall capacity of the employees allocated.

39. Under the contract, Equifax had the option to request additional resources to support ACIS, but doing so would increase the cost.

40. Over the next four years, Equifax initiated 22 change requests under the ACIS Statement of Work No. 88, but none of them added resources for remediating vulnerabilities such as the one exploited in the 2017 Apache Struts Breach.

41. In 2014, Equifax outsourced the maintenance and support of the computer servers that hosted the ACIS system to Tata, including the responsibility to implement patches as required, which included the Apache Struts patch.

42. The Service Levels Equifax required of Tata, were focused on maintaining the system's uptime, because downtime could potentially affect Equifax's revenue. For instance, the relevant time requirement for Tata to address server downtime was extremely short, including as little as within 15 minutes for "Priority 1" items.

43. Patching and vulnerability remediation were not part of the Service Level Agreement. A separate paragraph in the contract stated that Tata was required to complete patching within six (6) months, a stark contrast to the fifteen minutes required for items designated as Priority 1 by Equifax.

44. Under the terms of its contract, the Tata contractors managing the ACIS servers affected by the 2017 Apache Struts data breach were not contractually obligated to apply the Apache Struts patch until September 9, 2017, after Equifax announced the data breach to the world.

C. Equifax's Systems were Bound to Fail Consumers

Legacy Systems with Thousands of Vulnerabilities

45. In order to drive revenue and profit, Equifax delayed IT investment, resulting in an accumulation of aging, out-of-service, and difficult to maintain legacy systems.

46. On October 8, 2015, the results of a configuration-patch management audit (“2015 Patch Management Audit”) were presented to senior corporate management, including John Gamble, CFO, Chris Blalock SVP Internal Audit, Dave Webb, CIO, J. Kelley, Chief Legal Officer, and Susan Mauldin, Chief Security and Privacy Officer. The audit revealed that existing controls were “not adequately designed to ensure Equifax systems are securely configured and patched in a timely manner.”

47. At the time of the 2015 Patch Management Audit, Equifax’s patching policy required it to install critical patches within 48 hours, high risk patches within 30 days, and medium risk patches within 90 days.

48. The 2015 Patch Management Audit found there were more than “1,000 known critical, high or medium vulnerabilities on external facing systems (approximately 1150 hosts) and over 7,500 critical and high (excluding medium) vulnerabilities on internal systems (approximately 2,200 hosts). Of those known vulnerabilities, over 75% of the external vulnerabilities and over 93% of the internal vulnerabilities were over 90 days old.”

49. The 2015 Patch Management Audit noted, “One of the factors contributing to the unpatched systems is the large number of legacy systems in the IT environment.” Further, “numerous legacy systems ... are not able to be patched or securely configured; therefore, resulting in weakness to secure against attacks on the system.”

50. In addition to challenges with the number of legacy systems and the weaknesses identified within those systems, Equifax did not have an accurate inventory of its own IT assets. “Lack of asset management controls may result in systems not being scanned periodically for vulnerabilities and also does not allow the ability for IT to monitor/manage the patch levels and

configuration for all system.” Equifax further acknowledged that even if, “one computer in the environment is not patched, it can threaten the stability of the entire environment.”¹¹

51. Despite its official patch management policy, due to cost concerns, senior executives’ response to the stunning number of vulnerabilities was to direct IT staff to develop a plan to remediate the vulnerabilities by December 31, 2016, ***more than 500 days later.***

52. As for the legacy systems, management determined, “[f]or existing legacy UNIX (AIX & Solaris) . . . These environments require manual patching and the ***lack of proper segmentation*** makes scheduling downtime difficult to coordinate. Patching these environments will be best effort with critical patches only.” (Emphasis added).

53. Equifax management, through receipt of the 2015 Patch Management Audit, was aware of key issues with their legacy systems; namely, that (1) there was not proper segmentation, allowing access to multiple systems upon a single unauthorized entry, and that (2) the systems required manual patching, which meant only patches designated as critical would be completed due to concerns about downtime. The large number of outdated or legacy systems contributed to a string of data breaches at Equifax.

Prior Data Breaches

2010, 2012, and 2014 Indiana Data Breaches

54. The Indiana Attorney General’s office received official notifications of Equifax data breaches of Indiana consumers’ information in 2010, 2012, and 2014. See Exhibit A, Exhibit B and Exhibit C.

¹¹ United States Senate Permanent Subcommittee on Investigations Committee on Homeland Security and Government Affairs, “How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach, Staff Report Permanent Subcommittee on Investigations United States Senate https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf

55. Troy G. Kubes, Vice President & Associate Group Counsel for Equifax described the 2014 breach as follows, “On January 31, 2014, the Equifax security team discovered a suspicious pattern of inquiries from a single IP address. We immediately blocked the IP address from any further access. We subsequently determined that the earliest suspicious inquiry from the IP address occurred in April 2013.”

2013 Celebrity Breaches

56. In March 2013, rumors began to circulate that hackers had obtained the credit files of high profile celebrities including First Lady Michelle Obama, Vice President Joe Biden, Former Secretary of State Hillary Clinton, Beyoncé, Jay Z, Mel Gibson, Britney Spears, Hulk Hogan, Arnold Schwarzenegger, Kim Kardashian, Paris Hilton, Ashton Kutcher and current President Donald Trump.¹²

57. On March 12, 2013, Equifax spokesman Tim Klein conceded that high-profile individuals had been impacted, stating, “Equifax can confirm that fraudulent and unauthorized access to four consumer credit reports has occurred.”¹³

2015 Workforce Solutions Data Breach

58. Between January 2015 and March 2015, Equifax employee Cortland Iverson accessed Equifax’s internal network and performed a “hard reset of customer payroll accounts which allowed her to modify customer accounts to obtain direct deposit payments” intended for employees of Equifax’s Workforce Solutions customers. See Indictment-Redacted filed June 22, 2016 in the United States District Court for the Eastern District of Missouri, Case Number 4:16-cr-00260-RWS.

¹² <https://abcnews.go.com/US/obama-authorities-celeb-secret-files-hack/story?id=18707707> last accessed February 2, 2019.

¹³ <https://abcnews.go.com/Politics/equifax-confirms-hackers-stole-financial-data-launches-investigation/story?id=18715884> last accessed February 2, 2019.

59. When Cortland Iverson was indicted on June 22, 2016, the redacted version of the indictment helped to conceal Equifax's identity by describing the company as, "'EWS,' a payroll processing company." *Id.*

60. The 2015 Workforce Solutions breach affected nearly one hundred companies and hundreds if not thousands of employees.

61. Under Indiana law, "Data base owner" is defined as "a person that owns or licenses computerized data that includes personal information." Though Equifax claimed its Workforce Solutions employee data was one of the company's "unique assets," following the Cortland Iverson breach, Equifax failed to timely report its role in the data breach. This forced Equifax's corporate customers to provide their own notice to employees and regulators, including the Indiana Attorney General. See Ind. Code § 24-4.9 *et. seq.*

62. For instance, Allegis Group Inc. ("Allegis") was one of the customers whose employees were victims of the Cortland Iverson data breach. On June 8, 2015, Allegis filed a data breach notice with the Indiana Attorney General. Exhibit D.

63. In its report, Allegis explained steps that had been taken since the data breach to avoid future incidents, including the statement, "Equifax is also performing daily targeted network monitoring for suspicious activity."

2015 Chinese Hacker Data Breach

64. On September 12, 2018, the *Wall Street Journal* reported that in the fall of 2015, Equifax learned that a former employee believed to be an operative for a Chinese entity had improperly accessed and stolen proprietary information from its systems.¹⁴

¹⁴ Aruna Viswanatha and Kate O'Keefe, Wall Street Journal, "Before It Was Hacked, Equifax Had a Different Fear: Chinese Spying," September 12, 2018, <https://www.wsj.com/articles/before-it-was-hacked-equifax-had-a-different-fear-chinese-spying-1536768305> last accessed February 2, 2019.

65. The story explained, “Equifax security officials briefed the then-chief executive, Richard Smith, at a fall 2015 meeting, spreading high stacks of paper across the length of the boardroom table. The voluminous printouts represented what they feared was stolen.”¹⁵

66. Although Equifax initially notified the FBI, the company, “began to worry about legal exposure and how onerous the inquiry could become and eventually reduced its cooperation with law enforcement.”¹⁶ Again, Equifax did not report the breach to appropriate regulators.

2016 Workforce Solutions W-2 Data Breach

67. In 2016, the employees of Equifax’s Workforce Solutions customers, including Allegis, again began experiencing suspicious activity with the W-2 systems, resulting in tax fraud for many employees.

68. The 2016 W-2 system breach involved over one hundred employers and thousands of employees, more than the 2015 Workforce Solutions Breach.

69. Matthew Modica, Equifax’s former Vice President of Global Security, explained that each customer had an employee designated as an administrator and hackers were able to compromise those administrative accounts to exploit the system.

70. Once again, like the 2015 Workforce Solutions breach, Equifax [REDACTED] [REDACTED] and failed to timely notify the Indiana Attorney General as required by law.

71. For instance, The Kroger Co., one of Equifax’s corporate customers, filed a Data Breach Notification Form with the Indiana Attorney General on May 16, 2016, disclosing that 13,283 employees, including 866 Indiana residents, were involved in the data breach. Exhibit E.

¹⁵ *Id.*

¹⁶ *Id.*

72. Equifax considered requiring its corporate customers to change their vulnerable default passwords, but ultimately chose to make the change for new customers only.

2017 Workforce Solutions W-2 Data Breach

73. The 2017 breach was strikingly similar to the 2016 breach. It affected hundreds of employers and thousands of employees.

74. Once again, Equifax failed to report the security breach as required under Ind. Code §24-4.9 *et. seq.* Instead, it devised a scheme to minimize its role in the breaches by filing reports under the name of its subsidiary, Talx, submitting a separate report for each employer affected by the breach, and spreading the reports over a several month period, all in an effort to make the overall size of the breach appear to be smaller than it actually was. In Indiana, Talx sent a notice regarding the University of Louisville on April 20, 2017. Talx sent a notice related to Allegis on May 23, 2017. Talx sent a notice related to Aramark on June 2, 2017. On June 14, Talx sent a notice related to CVS Health. Talx sent a notice related to Whole Foods on July 21, 2017. Talx sent a notice related to Maxim on August 15, 2017. Talx sent a second notice related to Whole Foods on August 28, 2017. See attached Exhibit F, Exhibit G, Exhibit H, Exhibit I, Exhibit J Exhibit K and Exhibit L.

75. Equifax executives were initially advised of the 2017 W-2 breach in April and the internal investigation concluded “sometime after May 26, 2017.” The company’s executive officers would have been aware that the company was in the midst of issuing its disclosures for the data breach on August 1 when Equifax CFO John Gamble sold 6,500 shares of stock, and U.S. Information Solutions President Joseph “Trey” Loughran sold 4,000 shares, and on August

portals, sold 1,719 shares.¹⁷

D. Equifax Failed to Secure Consumers' Sensitive Personal Information

© 2004 Blackwell Publishing Ltd, *Journal of Internal Medicine* 255: 103–110

76. _____

77. [REDACTED]

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

¹⁷ <https://www.npr.org/sections/thetwo-way/2017/09/08/549434187/3-equifax-executives-sold-stock-days-after-hack-that-wasnt-disclosed-for-a-month> last accessed April 29, 2019.

[REDACTED]

[REDACTED]

82. [REDACTED]

[REDACTED]

[REDACTED]

83. [REDACTED]

[REDACTED]

[REDACTED]

84. [REDACTED]

[REDACTED]

85. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

86. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

87. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

88. [REDACTED]

[REDACTED]

[REDACTED]

89. [REDACTED]

[REDACTED]

90. [REDACTED] demonstrates the company's knowledge as to the [REDACTED]

[REDACTED]

[REDACTED]

Failure to Implement Anti-virus Software

91. Equifax failed to install anti-virus software on the servers hosting the ACIS application.

Use of Weak Passwords

92. Equifax failed to follow its own password policies. For instance, the user name and password the Apache Struts hackers used to access the first data base was four lower case letters, and the user name and password both matched the name of the database.

93. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

94. [REDACTED]

[REDACTED]

Failure to Maintain its Certificates

95. At the time of the breach, Equifax used a Network Intrusion/Detection system.

96. In order for Equifax to view and analyze encrypted data entering its network, it relied on Secure Socket Layer Visibility (“SSLV”) appliances.¹⁸

97. The ACIS system, for instance, had an SSLV device to monitor incoming traffic.¹⁹

98. In order to function, the SSLV device required a certificate to decrypt the in-line traffic before reaching the ACIS system.

99. On January 31, 2016, the SSL certificate expired for the ACIS online dispute portal.

100. Equifax failed to update the expired certificate until July 29, 2017, which is what prompted the company to finally discover the 2017 Apache Struts Breach. Between January 31, 2016 and July 29, 2017, Equifax was essentially blind as to the traffic to the ACIS system.

Failure to Implement Effective [REDACTED]

101. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Failure to Properly Manage [REDACTED]

102. [REDACTED]

[REDACTED]

[REDACTED]

¹⁸ House of Representatives Committee on Oversight and Government Reform, The Equifax Data Breach, Majority Staff Report, 115th Congress, December 2018, p. 39 citing Webb Transcribed Interview at 34.

¹⁹ *Id.*

103. The report declared, [REDACTED]

[REDACTED]

[REDACTED]

104. The report continued, [REDACTED]

[REDACTED]

[REDACTED]

105. [REDACTED]

[REDACTED]

[REDACTED]

106. The report continued, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

107. Under [REDACTED], the report indicated, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

108. [REDACTED]

[REDACTED]

109. Under [REDACTED]

110. On [REDACTED]

[REDACTED]

[REDACTED].

[REDACTED] *Security Vulnerabilities*

111. While the hackers were busy stealing the data of 147.9 Million U.S. residents, in mid-June, 2017, [REDACTED]

[REDACTED].

112. [REDACTED]

[REDACTED]

113. The [REDACTED]

[REDACTED]

[REDACTED]

114. In addition, the [REDACTED]

[REDACTED]

[REDACTED]

115. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] *Reveals Longstanding Security Failures*

116. [REDACTED]

[REDACTED]

117. [REDACTED]

[REDACTED]

118. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

119. By declaring its [REDACTED] Equifax knowingly and intentionally gambled with the sensitive personal information of 147.9 Million Americans. Had Equifax followed [REDACTED] no consumers would have been harmed or placed at substantial or imminent risk for identity fraud.

E. Equifax's Scheme or Artifice to Defraud

120. During the period between 2007 and the 2017 Apache Struts Breach, Equifax officers and executives actively engaged in a scheme or artifice to conceal the true state of the company's information security by withholding material information and making false and misleading statements to auditors, regulators, certifiers, investors, the general public and its financial institution customers.

False and Misleading Representations

121. At all relevant times prior to the 2017 Apache Struts Breach, on its Privacy Policy, available through a hyperlink at the bottom of each page of its public website, Equifax represented to the public:

We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.²⁰

122. In addition, between 2008 and 2014, Equifax included a section in its Form 10-K filed with the SEC that included the following language:

Safeguarding the privacy and security of consumer credit information, whether delivered online or in an offline format, is a top priority. We recognize the importance of secure online transactions and we maintain physical, administrative, and technical safeguards to protect personal and business identifiable information. We have security protocols and measures in place to protect information from unauthorized access or alteration. These measures

²⁰ <https://web.archive.org/web/20141006032043/http://www.equifax.com/privacy/> last accessed April 28, 2019.

include internal and external firewalls, physical security and technological security measures, and encryption of certain data.²¹

123. In its “Consumer Privacy Policy for Personal Credit Reports,” accessible at <http://www.equifax.com/privacy/personal-credit-reports>, Equifax represented that it had “reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers'] personal information.”

Equifax Actively Concealed its Information Security Deficiencies

124. In addition to the false representations identified above, Equifax furthered its scheme by attempting to cloak all information security decisions with the false appearance of attorney-client privilege by having Equifax’s Chief Legal Officer supervise the information security function.

125. Equifax sought to conceal its activities with a false accountant-client privilege. Equifax made a point of hiring IT consultants, auditors and certifiers from accounting firms, such as Ernst & Young, [REDACTED], or Habif, Arogeti & Wynne (“HA&W”) and wording the reports in such a manner to imply they were accountant opinions, when in reality they were merely IT reports.

126. Equifax also used Lync to conduct discussions regarding information security, including substantive discussions related to the 2017 Apache Struts Breach response, knowing that the company’s default setting on Lync did not archive chats, and thus would not be preserved for discovery.²²

²¹ See <https://www.sec.gov/Archives/edgar/data/33185/000104746908001839/a2182984z10-k.htm> last accessed February 2, 2019.

²² Senate Report, *Supra*.

127. 18 U.S. Code § 1344 states, “Whoever knowingly executes, or attempts to execute, a scheme or artifice—(1) to defraud a financial institution . . . shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.

128. 18 U.S. Code § 1346 states, “For the purposes of this chapter, the term “scheme or artifice to defraud” includes a scheme or artifice to deprive another of the intangible right of honest services.”

129. 18 U.S. Code § 1349 states, “Any person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.”

Equifax’s Knowing Violation of Payment Card Rules

130. At all times relevant, Equifax’s ACIS system accepted payment by credit cards and debit cards from consumers for security freezes and credit report disclosures.

131. When a customer uses a credit card or debit card (collectively, a “payment card”), the transaction involves four primary parties:

- Equifax, the merchant;
- An acquiring bank contracted with Equifax to process payment cards;
- A card network or payment processor, like Visa or Discover; and
- The consumer’s issuing bank.

132. Processing a payment card transaction involves four major steps:

- *Authorization*: a customer presents a payment card to make a purchase and Equifax requests authorization from the customer’s issuing bank.
- *Clearance*: if the issuer authorizes the transaction, Equifax completes the sale and forwards a purchase receipt to the acquiring bank.
- *Settlement*: the acquiring bank pays Equifax for the purchase and forwards the receipt to the customer’s issuing bank.
- *Post-Settlement or Funding*: the customer’s issuing bank posts the charge to the customer’s payment card account.²³

²³ <https://merchantservices.chase.com/support/faqs/the-basics> last accessed April 29, 2019.

133. At all times relevant to the allegations herein, Equifax's ACIS system accepted payment cards from Visa, MasterCard, Discover, and American Express.

134. For each transaction involving a payment card, the customer, or a customer service representative, would type in his Payment Card Account Number ("PAN") into the online checkout form. Equifax would transmit that data to its iPay credit card application, which in turn would obtain an authorization from Elavon, and following authorization, the transaction would be complete and Equifax stored the card information in the ACIS system in plain text.

135. During a transaction involving a payment card, Equifax collects information from its customers. The information includes the individuals' full names or first initials and last names and the individuals' credit card numbers, debit card numbers, or other financial account numbers along with the expiration dates and other information used to validate the payment (collectively, "Payment Data").

136. The Payment Data was used to process payments for consumer transactions, including transactions between Equifax and Indiana residents.

137. Equifax owned or licensed the Payment Data described above for payment processing purposes.

138. The Payment Data was, at times, maintained or stored on a computer.

139. Visa has established four different levels for businesses who store, process or transmit payment card data. Those merchants with more than 6 Million transactions per year from all channels are considered a Level 1 Merchant.²⁴

140. Since 2010, by virtue of its annual merchant transactions from all channels, Equifax Inc. qualified as a Level 1 merchant. As a Level 1 Merchant, Equifax is required to:

²⁴ https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp last accessed April 29, 2019.

- Annually provide a Report on Compliance (“ROC”) by a Qualified Security Assessor (“QSA”)
- Annually submit an Attestation of Compliance (“AOC”) Form.
- Conduct a quarterly network scan by an Approved Scan Vendor (“ASV”)²⁵

141. In addition to being a merchant, Equifax also qualified as a Level 1 Service Provider under the Payment Card Information Data Security Standards (“PCI DSS”) issued by the Payment Card Information Security Standards Council (“PCI SSC”), an organization formed by Visa, MasterCard, Discover, American Express and JCB.

142. As a Level 1 Service Provider, Equifax was required to complete an “Attestation of Compliance” (AOC) by a PCI QSA every 12 months.

143. Although it was required, Equifax did not provide a PCI Report on Compliance or Attestation of Compliance for 2010, 2011, or 2012.

144. Additionally, Equifax’s contract with Elavon, one of its acquiring banks for the relevant time period, included language requiring Equifax to comply with PCI DSS. Paragraph 16(c) of the contract reads, “Security Program Compliance. You must comply with the requirements of the Payment Card Industry (PCI) Data Security Standard including the Cardholder Information Security Program (CISP) of Visa and the Site Data Protection Program (SDP) of MasterCard, as applicable, and any modifications to, or replacements of such programs that may occur from time to time.”

145. In 2013, Equifax entered into an agreement with Dan Schroeder, Partner in Charge of Information Assurance Services with the accounting firm Habif Arogeti & Wynne (“HA&W”), to conduct its PCI DSS certifications.

²⁵ https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp last accessed February 11, 2019.

146. In 2016 alone, Equifax [REDACTED]

[REDACTED] Equifax was paying Dan Schroeder to consult with them to develop a PCI certification plan, then essentially letting him grade his own homework by performing the certification audits.

147. In addition to the money it received from Equifax for its PCI certifications, and Dan Schroeder's substantial consultant fee, Equifax also gave HA&W the business of "performing security risk assessments for Equifax third party resellers," which involved "testing to determine the deployment of certain controls Equifax requires in their contracts with the resellers."

148. The cozy relationship with HA&W was recognized by Equifax employees. For instance, [REDACTED]

[REDACTED] (Emphasis added).

149. The PCI Security Standards Council defines the proper scope for compliance as:

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.

...

As a rule of thumb, the following guidelines apply:

- Systems located within the CDE are in scope, irrespective of their functionality or the reason why they are in the CDE.
- Similarly, systems that connect to a system in the CDE are in scope, irrespective of their functionality or the reason they have connectivity to the CDE.
- In a flat network, all systems are in scope if any single system stores, processes, or transmits account data.²⁶

²⁶ https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf?agreement=true&time=1549909409814

150. The PCI Security Standards Council recommends

At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of its PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in PCI DSS scope.

151. In 2013, Equifax claimed:

Equifax Inc. has deployed controls, as of August 5, 2013, necessary to comply with PCI DSS Version 2.0, as applicable, for their information systems and supporting management and operational controls relative to their integrated solutions for management of the U.S. ACRO System.

152. Equifax knew the ACIS system was inextricably intertwined with the ACRO system. In fact, retrieving data from the ACRO system was a core ACIS system function. [REDACTED]

[REDACTED]

[REDACTED]

153. The PCI DSS qualifications for Qualified Security Assessors state that the QSA is required to retain the results and related materials from the ROC and AOC.

154. Contrary to that QSA requirement, as one term of its contract with HA&W, Equifax demanded to keep all of the work papers generated as a result of the PCI DSS certifications, which violated PCI SSC rules for Qualified Security Assessors.

155. In the 2013 Report on Compliance ("ROC"), QSA Scott Ritchie claimed he conducted his assessment between June 2013 and August 2013, which coincides with the [REDACTED]

[REDACTED]

156. Had Equifax properly scoped its PCI examination, it should have included the credit card merchant processing component of ACIS, the ACIS system connected to ACRO, as well as the ACRO mainframe, and all of the servers and applications hosting or using copies of

ACRO, such as the ACRO64 database involved in the 2017 Apache Struts Breach, and all other systems that stored or transmitted Payment Data, such as the primary account number of payment cards, and all systems or networks that could impact those systems if they were compromised.

157. In the PCI reports related to the ACRO database in 2013, 2014, 2015, and 2016, Equifax did not meet the PCI standards. Requirement 1.1.5.b, for instance, required the QSA to, “Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.”

158. The QSA noted that Equifax used both Telnet and FTP, which are considered insecure protocols because they transmit data in clear text. The QSA attempted to justify the non-compliance as a business requirement. In truth, Equifax was unwilling to make the changes necessary to upgrade to a compliant system.

159. PCI Requirement 2.2 requires Equifax to:

Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

160. Although Equifax had a patch management policy addressing security vulnerabilities, the 2015 Patch Management Audit demonstrated the company did not follow its own policy.

161. Requirement 3.4 requires Equifax to “Render PAN (Primary Account Numbers, i.e. payment card numbers) unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).”

162. In the ROC, Ritchie conceded, “PAN was not stored in an unreadable format in the environment assessed as part of this scope.” Again, Ritchie attempted to justify the failure to encrypt the data, but in truth, Equifax did not want to make the changes necessary to comply.

163. Following the 2017 Apache Struts Breach, the security firm Kroll was hired to perform a PCI Forensic Investigation (“PFI”). J. Andrew Valentine, the Kroll investigator, found 23,011,017 unique PANs from the ACRO system contained in plain text within the ACIS database.

164. Requirement 5.1 required Equifax to, “Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).”

165. Equifax responded by claiming the requirement was “Not Applicable- Equifax ACRO was not using anti-virus technologies in the assessed environment, as it was not available for the systems in use within the assessed scope.” Anti-virus software was available for the server running the ACIS system, but Equifax did not install it.

166. On [REDACTED]

[REDACTED]

[REDACTED] As of the start of the 2017 Apache Struts Breach, these

[REDACTED] had not been implemented.

167. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

168. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

169. [REDACTED]

[REDACTED]

170. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

171. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

172. [REDACTED]

[REDACTED]

[REDACTED]

173. [REDACTED]

174. [REDACTED]

175. [REDACTED]

176. Rather than bring the appropriate systems within the scope of PCI certification, Equifax's chose to certify only pieces of systems capable of meeting the requirements, and ignore all systems that could not meet PCI standards, treating them as if they did not exist. This

approach essentially pretended each certified application was an island, when in fact they were all connected to, and could be impacted by, non-compliant systems within the U.S. environment.

177. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

178. In addition, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

179. [REDACTED]

[REDACTED]

180. Equifax knew by August 2015 that it had more than 1,000 external vulnerabilities and that the company did not plan to remediate those vulnerabilities before December 31, 2016. Yet Equifax provided the QSA with a copy of its Patch Management Policy, EQ-ITSEC001,

which stated that all critical vulnerabilities would be remediated within 48 hours and all high vulnerabilities would be remediated within 30 days, which Equifax knew to be false.

181. On October 24, 2014, Joseph “Trey” Loughran, President NA Personal Solutions, Equifax Inc. signed an Attestation of Compliance certifying that the Report on Compliance on behalf of Equifax’s Personal Solutions group dated October 17, 2014 was conducted according to PCI DSS requirements and procedures.

182. Under Section 2b. Relationships, the form asks, “Does your company have a relationship with more than one acquirer?” Loughran checked the “No” box. His representation was not true. At the time, Equifax had a relationship with both Elavon and JP Morgan Chase Paymentech, both of which acted as an acquiring bank. Furthermore, the 2014 Report of Compliance failed to mention the ACRO database (the mainframe).

183. By way of contrast, on September 15, 2016, Equifax employee Matthew Modica and HA&W employee Charles Gunnels signed a Report on Compliance that contradicted Loughran’s representation by stating that Global Consumer Solutions included the mainframe.

184. In the 2014 ROC, Loughran further failed to mention the ACIS system or the payment processing component associated with that system. Further, he omitted the fact that the ACRO database is not encrypted, which is another requirement for PCI DSS compliance that Equifax did not meet.

185. In another layer of deception, Loughran, who was an officer of Equifax Inc., provided the Report on Compliance and his Attestation of Compliance, both containing false statements and misrepresentations, to JP Morgan Chase Paymentech, a financial institution, in violation of 18 U.S. Code § 1344; 18 U.S. Code § 1346 and 18 U.S. Code § 1349.

186. As an executive officer, Loughran acted on behalf of Equifax Inc. and the other executive officers engaged in PCI compliance oversight.

187. Similarly, in 2015, Equifax employee Scott Barronton, Vice President, PCI Compliance, signed an Attestation of Compliance on October 15, 2015, certifying that the Report on Compliance dated October 15, 2015 was completed according to PCI DSS requirements and Security Assessment Standards.

188. The Report on Compliance dated October 15, 2015 did not mention the ACRO database. It failed to note the ACRO database stored payment card data without encryption. It failed to mention the ACIS system, or the payment card processing application module, or Equifax's relationship with Elavon, who served as one of Equifax's acquiring banks.

189. Scott Barronton provided both his Report on Compliance and his Attestation of Compliance, both containing false statements and misleading representations, to JP Morgan Chase Paymentech, a financial institution, in violation of 18 U.S. Code § 1344; 18 U.S. Code § 1346 and 18 U.S. Code § 1349.

190. In 2016, Equifax employee Matthew Modica, completed the Report on Compliance for Equifax's Global Consumer Solutions business.

191. As part of his report documentation, Modica added Doc-31, Patch Management Policy, EQ-ITSEC001, which claimed that all critical vulnerabilities would be patched within 48 hours, all high vulnerabilities were to be patched within 30 days and all medium vulnerabilities were to be patched within 90 days.

192. By the fall of 2016 when Modica filled out the Report on Compliance, it had been a full year since the 2015 Patch Management Audit revealed that Equifax had more than 1,000

external vulnerabilities and over 7,500 internal vulnerabilities. Modica knew Equifax Inc. did not comply with its own patch management policy, yet he included the policy in his report.

193. Modica, who was at the time Vice President of Global Security, provided on behalf of Equifax Inc., a copy of his Report on Compliance dated October 25, 2016 and containing what he knew to be false and misleading representations to JP Morgan Chase Paymentech, a financial institution, in violation of 18 U.S. Code § 1344; 18 U.S. Code § 1346 and 18 U.S. Code § 1349.

194. Modica reported directly to Chief Security Officer Susan Mauldin, an officer of Equifax, and was acting on behalf of all the Equifax officers engaged in PCI oversight.

195. In all instances, Equifax made its representations regarding compliance with PCI DSS standards, knowing its representations to be false and misleading. It provided Reports on Compliance and Attestations of Compliance to its financial institution customers, knowing they contained false and misleading information. Equifax did so in order to keep its current customers and data furnishers who required PCI compliance, and to acquire new customers and data furnishers who required PCI compliance.

196. Disturbingly, the PCI certification program was not the only certification deceptively obtained by Equifax to mislead its customers.

ISO27001 False and Misleading Representations

197. On December 21, 2011, EY CertifyPoint, a subsidiary of Ernst & Young, certified Equifax as ISO27001:2005 compliant. At that time, Equifax was an SEC Registrant and an SEC audit client of parent company Ernst & Young.

198. In fact, the actual ISO 27001 certification program was carried out by the Atlanta office of Ernst & Young LLP, “acting as agents of CertifyPoint.”

199. Equifax failed to disclose the obvious conflict of interest in any of its SEC filings.

200. This close, comfortable relationship between Equifax and Ernst & Young LLP is demonstrated by an email written by EY Senior Manager Nick A. Smith e to Gerry E. Boudrea on December 11, 2016, stating:

We wanted to request your commit approval for an upcoming renewal we have for global ISO 27001 certification services for Equifax. We have performed these services for Equifax since 2011, and are putting together a 3-year SOW. Total fees for FY17 would be \$178,000, with the total for the 3 years at approximately \$465,000, and the margin is 67%. **This is not a competitive bid situation –we have a great relationship with their security/ISO team and expect to win this work.** (Emphasis supplied).

201. In its ISO documentation, Equifax failed to disclose that it had outsourced its production environment management to Tata, or that according to its Statement of Work with Tata, patches were not required to be applied earlier than 6 months.

202. Further, [REDACTED]

[REDACTED]

203. In February 2016, GTVM issued a report regarding patching status for Equifax's U.S. and International sites, which indicated that 22 out of 23 sites were "not reported" as to patching status, and only one – Workforce Solutions – reported as "in progress."

204. [REDACTED]

[REDACTED]

[REDACTED].

205. In July 2016, GTVM reported that 22 out of 23 sites were "not reported," with only Workforce Solutions reporting as compliant.

206. Although it is clear Equifax failed to timely remediate vulnerabilities or report on vulnerabilities, it continued to claim that the company followed its patch policy which required

critical patches to be made within 48 hours, high patches within 30 days, and medium patches within 90 days, even though Equifax knew that representation was not true.

207. Following the disclosure of the 2017 Apache Struts Breach on September 7, 2017, Equifax's ISO 27001 certificate was "suspended."²⁷

208. In its Form 10-K filed with the SEC on March 1, 2018, Equifax conceded:

[S]ome of our current and potential customers and the contracts governing certain customer relationships, as well as certain of our data suppliers, require us to maintain International Organization for Standardization ("ISO") certifications, such as ISO 27001 certification, that specify requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system. Due to the 2017 cybersecurity incident, certain of our ISO certifications have been suspended and we will be required to take additional remediation steps to retain such certifications, which efforts may not be successful. Additionally, certain of our payment card industry certifications have been suspended which could result in fines and loss of access to data if we are not able to complete the necessary remediation steps to retain these certifications, which would adversely affect our ability to offer certain products to customers.

False and Misleading Statements in SEC Filings

209. 17 CFR § 240.13b2-2 provides:

- (a) No director or officer of an issuer shall, directly or indirectly:
 - (1) Make or cause to be made a materially false or misleading statement to an accountant in connection with; or
 - (2) Omit to state, or cause another person to omit to state, any material fact necessary in order to make statements made, in light of the circumstances under which such statements were made, not misleading, to an accountant in connection with:
 - (i) Any audit, review or examination of the financial statements of the issuer required to be made pursuant to this subpart; or
 - (ii) The preparation or filing of any document or report required to be filed with the Commission pursuant to this subpart or otherwise.

210. 18 U.S.C. § 1348 provides

Whoever knowingly executes, or attempts to execute, a scheme or artifice—

²⁷ <https://www.sec.gov/Archives/edgar/data/33185/000003318518000011/efx10k20171231.htm> last accessed April 28, 2019.

(1) to defraud any person in connection with any commodity for future delivery, or any option on a commodity for future delivery, or any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78l) or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(d)); or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale of any commodity for future delivery, or any option on a commodity for future delivery, or any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78l) or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(d)); shall be fined under this title, or imprisoned not more than 25 years, or both.

211. In [REDACTED], Equifax senior executives, including CEO Smith, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

212. Despite its knowledge of the risks, in its 10-K filed on February 25, 2015, Equifax failed to disclose the vulnerabilities and cyber risks associated with its outsourcing activity, specifically omitting the fact that the outsourcing contracts with Tata for the maintenance and support of its Solaris servers (including the servers ultimately involved in the 2017 Apache Struts Breach) gave contractors six months to install patches, contrary to the company's official patching policy and accepted practice.

213. [REDACTED]

[REDACTED]

214. [REDACTED]

[REDACTED]

215. Despite its knowledge that the company was not PCI compliant, and further, that its failure to be PCI compliant posed a revenue risk for the company, Equifax failed to disclose that risk in the Form 10-K it filed with the SEC on February 24, 2016.²⁸

False and Misleading Statements to a Congressional Committee Investigation

216. 18 U.S.C. § 1001 provides:

- (a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—
 - (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;
 - (2) makes any materially false, fictitious, or fraudulent statement or representation; or
 - (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry;shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both. If the matter relates to an offense under chapter 109A, 109B, 110, or 117, or section 1591, then the term of imprisonment imposed under this section shall be not more than 8 years.
- (b) Subsection (a) does not apply to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.
- (c) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to—
 - (1) administrative matters, including a claim for payment, a matter related to the procurement of property or services, personnel or employment practices, or support services, or a document required by law, rule, or regulation to be submitted to the Congress or any office or officer within the legislative branch; or
 - (2) any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate.

²⁸ <https://www.sec.gov/Archives/edgar/data/33185/000003318516000037/efx10k20151231.htm> last accessed April 29, 2019.

217. In his testimony before the House of Representatives Committee on Oversight and Government Reform, Subcommittee on Digital Commerce and Consumer Protection, Former CEO Smith failed to disclose that the development and maintenance of the systems which were breached had been outsourced to Tata. He further failed to disclose that the Tata contractors responsible for maintaining and patching the system had in fact received notice of the Apache Struts vulnerability. Further, CEO Smith failed to disclose that Equifax's contract gave Tata six months to install patches and updates.²⁹

F. 2017 Apache Struts Data Breach

218. On March 7, 2017, the Apache Foundation announced the release of Struts 2.3.32 General Availability and Struts 2.5.10.1 General Availability to address a, "Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser." The alert contained a note in bold letters: "**All developers are strongly advised to perform this action.**"³⁰

219. On March 8, 2017 5:06:50 pm the Financial Services Information Sharing and Analysis Center ("FS-ISAC") issued a notice to Equifax and others titled, "Apache Struts Jakarta Multipart Parser Code Execution Vulnerability."

220. On March 8, 2018, the United States Computer Emergency Readiness Team ("US- CERT") issued an alert, notifying recipients that, "The Apache Software Foundation had released security updates to address a vulnerability in Struts 2. A remote attacker could exploit this vulnerability to take control of an affected system." Susan Mauldin, Equifax Chief Security Officer, and multiple other people at Equifax, received a copy of that alert.

²⁹ <https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Smith-DCCP-Hrg-on-Oversight-of-the-Equifax-Data-Breach-Answers-for-Consumers-2017-10-03.pdf> last accessed April 28, 2019.

³⁰ <https://struts.apache.org/announce-2017.html#a20170307-2> accessed on February 5, 2019.

221. On [REDACTED]

222. The Mitre Corporation's list of Common Vulnerabilities and Exposures CVE™ assigned this particular vulnerability with the number CVE-2017-5638, and described it as:

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.³¹

223. On Thursday March 9, 2017, Equifax circulated a copy of the Apache Struts warning to its Global Vulnerability Threat Management ("GVTM") email list, instructing anyone with Apache Struts running on its system to upgrade to the new version within 48 hours.

224. The GVTM list included [REDACTED]

225. On the next day, Friday, March 10, 2017, unknown intruders exploited the Apache Struts vulnerability on the ACIS system, issuing a "whoami" command, which is a known exploit for hackers searching for vulnerabilities.

226. Since the SSLV device had been rendered inoperable because its certificate expired³², Equifax security had no visibility to the fact intruders were exploring the ACIS system.

³¹ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638> last accessed April 29, 2019.

³² See ¶¶ 100-103.

[REDACTED] *Breach*

227. On the next day, Saturday March 11, 2017 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

228. Central Source was one of the modules integrated into the ACIS application. The ACIS application received and processed data received from the AnnualCreditReport.com data base.

229. Equifax employees [REDACTED]

[REDACTED]

[REDACTED]

230. [REDACTED]

[REDACTED]

[REDACTED]

231. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

232. [REDACTED]

[REDACTED]

[REDACTED]

233. [REDACTED]

[REDACTED]

234. [REDACTED]

[REDACTED]

[REDACTED]

Multiple Additional Warnings

235. In addition to the above notifications, multiple other warnings were received by Equifax.

236. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

237. On Tuesday March 14, 2017, Equifax's Countermeasures group prepared to implement changes to the rules in Equifax's intrusion detection system called Snort, to detect Apache Struts exploitation attempts on the intrusion detection and prevention systems

238. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

239. [REDACTED]

[REDACTED]

[REDACTED]

240. [REDACTED]

[REDACTED], and was

factually inaccurate.

241. [REDACTED]

[REDACTED] than the 1,150 servers on which it found known vulnerabilities in the fall of 2015.

242. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

243. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

244. On Friday March 16, 2017, Equifax conducted its monthly Global Threat and Vulnerability Management meeting. The presentation included a description of the Apache Struts vulnerability CVE-2017-5638.

245. [REDACTED]

[REDACTED]

[REDACTED]

246.

247.

Intruders Successfully Breach Equifax Systems

248. On May 13, 2017 the hackers began using a web shell program which is software to enable remote control of the machine, essentially a backdoor.

249. Over the course of the breach, the hackers used approximately thirty web shell programs. According to Mandiant, file integrity monitoring would have detected the creation of these web shells, but the ACIS system did not have file integrity monitoring enabled at the time of the attack.

250. By May 13, the hackers already knew the login and password for the database were both four letters long, and both matched the name of the data base.

251. Equifax maintained this password information on a shared drive containing other user name/password combinations, maintained in clear text, which gave the hackers access to 48 databases due to Equifax's failure to properly segment its network. In total, the hackers were

able to run 9,000 queries against Equifax databases without being detected. The hackers made 265 successful queries that contained enormous amounts of personally identifiable information. The attackers compressed those files and retrieved them from the server using Wget, a common utility that enables users to make web server requests. In total, the hackers were able to steal [REDACTED] related to 147.9 Million Americans and 3.1 Million Indiana residents.

252. The planned “Refresh Date” for the SSLV certificates in Atlanta (where the ACIS system resided) was July 29, 2017.

253. On 29 July 2017, updated the expired certificate and immediately noticed suspicious traffic from an IP address originating from China. They observed traffic in the form of images files related to consumer credit investigations.”

254. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

255. On July 30, 2017, as Equifax investigated the ACIS system, it discovered flaws in the ACIS code rendering the system vulnerable to SQL injection and Insecure Direct Object Reference attacks.

256. The Equifax forensic team quickly determined the exfiltrated data contained Personally Identifiable Information (“PII”).

257. On July 31, Equifax assigned the code name Project Sierra to the incident response efforts.

Equifax Unreasonably Delayed Disclosure of the 2017 Apache Struts Breach

258. Based upon its investigation, by July 31, Susan Mauldin stated, “I felt like I knew at that point PII had been involved in this incident.”

259. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

260. The Vulnerability Assessment team determined that the affected web server had the Apache Struts 2 vulnerability.

261. On August 1, 2017, Graeme Payne briefed CIO Dave Webb regarding Project Sierra (the 2017 Apache Struts Breach). The following day, August 2, 2017, CIO Dave Webb left for a vacation out of the country from August 2 to August 17. During that time, Webb had no communication with anyone at Equifax regarding the data breach.

262. [REDACTED]

[REDACTED]

263. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

264. [REDACTED]

[REDACTED]

[REDACTED]

265. [REDACTED]

[REDACTED]

[REDACTED]

266. [REDACTED] was managed by Tata consultants working under Statement of Work 112. The ACIS development team was composed of Tata contractors working under Statement of Work 88.

267. Equifax's failure to apply the Apache Struts security patch was not due to a communication failure as the company has publicly proclaimed. The company made a conscious decision to outsource these functions to Tata, and the contract with Tata gave it six months to implement patches. Under the terms of the contract, Tata had until September 9, 2017 to apply the patch.

268. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

269. [REDACTED]

[REDACTED]

[REDACTED] :

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
270. [REDACTED]
[REDACTED]
[REDACTED]

271. [REDACTED]
[REDACTED]
[REDACTED] which were all elements of the information stolen in the

2017 Apache Struts Breach.

272. Despite knowing the 2017 Apache Struts Breach involved the personal information of millions of U.S. residents, including 3.9 Million Indiana residents, and despite knowing there may have been vendors on the dark web who were selling that information, Equifax waited six weeks to reveal the data breach with a press release on September 7, 2017.

273. As part of its announcement, Equifax chose to follow alternative notice to Indiana residents by placing a notice on its public website, <http://www.equifax.com>, which directed consumers to a special website Equifax created, located at equifaxsecurity2017.com, to answer consumers' questions and enroll them in the TrustedID program Equifax offered.³³

274. Equifax's disclosure was not in compliance with the Indiana Disclosure of Security Breach Act, because it failed to provide notice without unreasonable delay.

³³ <https://www.equifaxsecurity2017.com/> last accessed April 29, 2019.

Equifax's Bungled Data Breach Response

275. [REDACTED]
[REDACTED]
[REDACTED].

276. [REDACTED]
[REDACTED]

277. On September 9, 2017, Equifax's Twitter account directed consumers to visit securityequifax2017.com which was a phishing site, not the website established by Equifax, misleading countless concerned consumers.

278. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

279. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

280. [REDACTED]
[REDACTED]
[REDACTED].

281. Concerned about their vulnerability to identity theft, and frustrated by the difficulties of trying to deal with Equifax, many Indiana residents spent time and effort trying to guard their financial accounts. Many Indiana residents purchased other credit monitoring services, and also paid to pull multiple copies of their credit reports, resulting in significant financial harm.

282. Ironically, some of the alternative products they purchased, such as Lifelock products, actually paid a fee to Equifax, which lead to Equifax making money from its own data breach.

283. Similarly, Indiana residents who purchased three bureau reports from Experian or Transunion also unknowingly paid a fee to Equifax, which lead to Equifax making money from its own data breach.

PCI Forensic Investigation and Report

284. Following the 2017 Apache Struts Breach, the payment card brands required Equifax to hire a PCI Forensic Investigator to examine the ACIS system involved in the breach.

285. In the November 22, 2017 PFI Final Incident Response Report, Kroll investigator Valentine noted that the ACIS system had never been reviewed for PCI compliance as required by the PCI DSS standards.

286. Out of the twelve PCI DSS requirement categories, Valentine determined that Equifax failed all of the categories he reviewed.

PCI DSS Requirements	Was Requirement Fully Assessed?	In Place	Cause of Breach?	Contribute to breach?	Findings/Comments
Requirement 1: Install and maintain a firewall	No	No	No	No	Firewall configurations were not examined or assessed as part

configuration to protect cardholder data					of this PFI investigation. However, no current network diagram exists detailing connections between the cardholder data environment and other networks, in violation of section 1.1.2.
Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters	NO	No	No	No	Entity did not maintain inventory of system components that are in scope for PCI-DSS, in violation of section 2.4.
Requirement 3 Protect stored cardholder data	No	No	No	No	Entity was storing full PAN in clear text in violation of PCI-DSS section 3.3.
Requirement 4 Encrypt transmission of cardholder data across open, public networks	No	Not Assessed	No	No	Encrypted transmission of cardholder data across public networks was not assessed as part of the PFI investigation.
Requirement 5 Use and regularly update anti-virus software	No	No	No	Yes	Anti-virus software was not installed on the affected Solaris web application servers in violation of PCI DSS section 5.1.
Requirement 6: Develop and maintain secure	No	No	Yes	No	The security vulnerability that was exploited in

systems and applications					order to install a web shell was publicly known with patches available for two months prior to the incident. As per section 6.2, the vulnerability should have been remediated within one month of patch release.
Requirement 7: Restrict access to cardholder data by business need-to-know	No	No	No	No	In this case, were inadvertent storage resulted in the compromise of cardholder data, the entity did not have sufficient policy around the access to that data as it did not know that data existed prior to the compromise (7.1)
Requirement 8: Assign a unique ID to each person with computer access	No	No	No	Yes	The user password for the affected database containing plain text cardholder data was only four characters in length, and not alphanumeric, and matched the username itself, in violation of requirement 8.2.3.
Requirement 9: Restrict physical access to cardholder data	No	Not assessment	No	No	Physical security was not examined or assessed as part of this PFI investigation

Requirement 10: Track and monitor all access to network resources and cardholder data	No	No	No	No	Although Kroll was able to examine relevant web server logs, application logs, and database query logs to determine and understand the scope of intruder access to cardholder data, proxy logs detailing external IP addresses were only available for one month, in violation of section 10.7
Requirement 11: Regularly test security systems and processes	No	No	No	Yes	The affected systems environment had never undergone an external vulnerability scan by an ASV, in violation of section 11.2.
Requirement 12: Maintain a policy that addresses information security	No	Partial Yes	No	No	The client shared its full information security and incident response policy documentation with Kroll.

287. Mr. Valentine testified that Equifax did not permit him to examine how the card data was transmitted from the Equifax environment or the physical server, which is why two of twelve the requirements were listed as “not assessed.”

288. On December 14, 2017, MasterCard notified Elavon that Equifax would need to achieve full compliance with PCI DSS standards within 60 days.

289. On December 19, 2017, Amanda Duggin, the Data Compromise Coordinator for Elavon, sent an email to Gabe Bonfield at Equifax, notifying him that, "MasterCard is requiring the attached Site Data Protection form completed by 1/12/18 and PCI validation completed by 2/12/18. MasterCard has communicated that they are requiring that Equifax validate as level 1 post-breach and complete an onsite QSA assessment."

290. On December 22, 2017 Visa sent a notice to Amanda Duggin informing her, "The investigation concerning the account data compromise involving Equifax (FIT #U.S.-2017-INC:18113) is now complete. Elavon was found to be non-compliant with the Account Information Security Program (AIS) requirements."

291. On December 26, 2017, Amanda Duggin sent Gabe Bonfield an email, advising him that Visa had communicated a deadline for PCI compliance of June 30, 2018.

292. On January 16, 2018, Amanda Duggin sent an email to Equifax employee Shea Geisler, Security Programs, Vice President, informing him that MasterCard approved Equifax's extension request to 7/31/2018.

293. Equifax had no intention of complying with PCI requirements by the card brands' deadlines. Instead, it reverted back to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

294. Following the 2017 Apache Struts Breach, rather than taking the steps to become compliant, Equifax devised a scheme to stall for time, so that [REDACTED] [REDACTED]. It produced a “Mock” PCI DSS Report on Compliance, where the ACIS application was reviewed without consideration to all of the networks and systems to which it was connected. Simply put, Equifax reverted to form and created another one of its improperly scoped and incomplete, non-compliant PCI reports it had been peddling for the prior five years.

295. Under its new scheme, Equifax proposed to complete a true Report on Compliance that considered all the connected systems (as required by the PCI DSS rules) by May 2019.

296. In its Form 10-K filed with the SEC on March 1, 2018, Equifax admitted that following the 2017 Apache Struts Breach announcement, “certain of our payment card industry certifications have been suspended.”

297. From that time, and continuing to the present day, Equifax has continued to accept credit card transactions from consumers, knowing that its systems are not compliant.

298. During 2018 alone, Equifax processed 11,467,429 transactions through JP Morgan Chase Paymentech and 48,637 transactions through Elavon.

G. CAUSES OF ACTION

COUNT I:

EQUIFAX’S FAILURE TO ADEQUATELY SECURE INDIANA RESIDENTS’ PERSONAL INFORMATION CONSTITUTES AN UNFAIR ACT

299. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

300. The DCSA prohibits a supplier from committing “an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations. Ind. Code. § 24-5-0.5-3(a).

301. As a regular part of its business, Equifax sells or otherwise disposes of services or intangibles – and solicits to sell or otherwise dispose of such services or intangibles – both directly to consumers (e.g., credit report sales; credit protection sales; credit report dispute inquiries/communications) and in connection with transactions consumers are entering into with third parties (e.g., extensions of credit related to auto sales and mortgages; credit inquiries for job applications or background checks). Whether transacting business directly with Equifax, or with third parties utilizing the services or intangibles Equifax is providing, the consumers are transacting for personal, familial, agricultural, or household purposes. Equifax regularly engages in consumer transactions under Indiana Code § 24-5-0.5-2(a) (1), and is a supplier under Ind. Code § 24-5-0.5-2(a) (3).

302. In connection with consumer transactions, Equifax engaged in unfair, abusive, or deceptive acts, omissions, or practices causing or resulting in its failure to secure Indiana consumers’ personal and financial information, including, but not limited to, the following acts, omissions, or practices:

302.1. Failing to follow its own policy on patching and remediating
vulnerabilities;

302.2. Failing to replace its certificates before they expired;

302.3. Failing to follow its own policy regarding password complexity or
expiration;

302.4. Failing to encrypt consumer data [REDACTED] and

302.5. Failing to detect the infiltration of its systems for a period of seventy-three days, during which the data of 147.9 million Americans, including 3.9 million Indiana residents was stolen by criminals.

303. Following the announcement of the breach, Indiana residents were unable, in a timely manner, to access Defendants EquifaxSecurity2017.com web site, contact Defendant by telephone or sign up for the credit monitoring offered by Defendant, prompting many residents to purchase other credit monitoring services or credit reports in an effort to protect their financial accounts.

304. As a direct and proximate result of Equifax's failures, 3.9 Million Indiana residents are now more likely to suffer an identity theft crime, and given the sensitive nature of the stolen data, will remain more prone to identity theft crimes for the remainder of their lives which constitutes an unacceptable societal harm.

305. Indiana residents did not choose to provide Equifax with their personal information, and have no ability to prevent Equifax from storing and selling their personal information. As a result, Indiana residents are reliant upon Equifax to implement and maintain reasonable security measures to protect their information from theft and abuse.

306. Equifax's failure to follow its own policies or security standards confers no benefit upon Indiana residents, thus the benefits do not outweigh the harm.

307. For each of the 3.9 Million Indiana residents impacted by the breach, Equifax's failure to protect their personal information constitutes a separate unfair act.

308. Equifax's acts, omissions, and practices are unfair, abusive, and deceptive acts under Indiana Code section 24-5-0.5-3(a).

COUNT II:
EQUIFAX'S MISREPRESENTATION OF ITS INFORMATION SECURITY VIOLATES
THE DECEPTIVE CONSUMER SALES ACT

309. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

310. In connection with consumer transactions, Equifax engaged in unfair, abusive, or deceptive acts, omissions, or practices by misrepresenting the state of its information security systems, including but not limited to, the following acts, omissions, or practices:

- 310.1. Misrepresenting that safeguarding the privacy and security of consumers was a "top priority," in its publicly available Form 10-K filings with the SEC;
- 310.2. Misrepresenting that safeguarding the privacy and security of consumers was a "top priority" in the publicly available privacy policy linked at the bottom of each page on its website;
- 310.3. Knowing and failing to disclose that the company's contract with Tata contained SLAs that only measured uptime performance, contained no security metrics, and permitted Tata to take up to six months to implement a patch;
- 310.4. Knowing and failing to disclose that the company failed to replace its certificates before they expired;
- 310.5. Knowing and failing to disclose that the company failed to follow its own password management policy; and
- 310.6. Knowing and failing to disclose that the company failed to encrypt the sensitive personal information of consumers.

311. The misrepresentations were directed to each Indiana resident for whom Equifax maintained data, including but not limited to, the 3.9 Million residents impacted by the data breach.

312. Equifax's acts, omissions, and practices are unfair, abusive, and deceptive acts under Indiana Code section 24-5-0.5-3(a).

COUNT III:
**EQUIFAX'S MISREPRESENTATION THAT IT COMPLIED WITH PAYMENT CARD
STANDARDS VIOLATES THE INDIANA DECEPTIVE CONSUMER SALES ACT**

313. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

314. In connection with consumer transactions, Equifax engaged in unfair, abusive, or deceptive acts, omissions, or practices by misrepresenting the company's compliance with Payment Card Industry standards, including but not limited to, the following acts, omissions, or practices:

314.1. Misrepresenting to customers that it followed the rules required of all merchants who accept payment card brands by accepting payment cards as a form of payment;

314.2. Misrepresenting to customers that it followed the rules required of all merchants who accept payment card brand by displaying the logos of the payment brands Visa, MasterCard, Discover and American Express on the checkout page of its web site; and

314.3. Knowing and failing to disclose that it failed to comply with PCI DSS standards.

315. Equifax's own bank tells its merchants, "Every time customers give you payment information, they trust you to help protect their card data ..."

316. Prior to the Apache Struts breach, the payment card processing portion of the ACIS system had never been assessed by a Qualified Security Assessor, as required by PCI DSS standards.

317. Since at least 2013, Equifax knew that the ACIS system contained payment card information which was stored in plain text.

318. Equifax reviewed the ACIS system in 2014, 2015, 2016, and 2017 to determine if it complied with PCI DSS standards, and each time it determined that it did not comply.

319. Equifax's acts, omissions, and practices are unfair, abusive, and deceptive acts under Indiana Code section 24-5-0.5-3(a).

COUNT IV:
EQUIFAX KNOWINGLY VIOLATED IND. CODE § 24-5-0.5-3(a)

320. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraph of this Complaint as though fully alleged herein.

321. Equifax knew that it was not adequately securing consumer personal and financial information.

322. Equifax knew that it was misrepresenting its information security.

323. Equifax knew that it was not compliant with PCI payment card data standards.

324. Equifax knowingly violated Indiana Code Section 24-5-0.5-3(a), as asserted in Count I.

325. Equifax knowingly violated Indiana Code Section 24-5-0.5-3(a), as asserted in Count II.

326. Equifax knowingly violated Indiana Code Section 24-5-0.5-3(a), as asserted in Count III.

COUNT V:
EQUIFAX'S CONDUCT CONSTITUTES INCURABLE DECEPTIVE ACTS UNDER
INDIANA CODE §24-5-0.5-2(a) (8)

327. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

328. Equifax committed the Deceptive Acts asserted in Counts I, II, and III as part of a scheme, artifice, or device with intent to deceive. Ind. Code § 24-5-0.5-2(a) (8).

329. Equifax committed incurable deceptive acts under Indiana Code §24-5-0.5-2(a) (8).

330. Equifax knew that it needed to be PCI DSS compliant and that it was solely responsible for said compliance.

331. Equifax misled every Indiana customer involved in a payment card transaction. Indiana customers expected that, as a merchant authorized to accept payment cards, like Visa, MasterCard, Discover and American Express, Equifax met the minimum industry standards to protect payment information, when in fact it did not.

332. Equifax created and furthered a scheme, artifice or device that prioritized revenue over data security and concealed the true state of its deficient information security.

333. Equifax's misleading acts and omissions occurred in each customer transaction in which an Indiana consumer engaged in payment card transaction using one of the Equifax's US sites, including the ACIS application, the Personal Solutions web site, and the Workforce Solutions web site.

334. Each one of the online transactions involving an Indiana resident implicates a misleading representation or omission by Equifax to the consumer. The consumer's payment information was taken and used by Equifax, but, unknown to the consumer, it was not protected or safeguarded by Equifax according to PCI rules.

335. For every transaction involving Indiana residents from 2006 to the present, Equifax took advantage of customers' assumption that Equifax was compliant with industry standards for data protection. The Indiana customers who engaged in payment card transactions with Equifax would not have entered the transaction if they had been warned Equifax did not follow the payment card rules, or that Equifax had thousands of critical, high and medium vulnerabilities on its external web sites, any one of which could result in a data breach.

COUNT VI:
EQUIFAX VIOLATED THE DISCLOSURE OF SECURITY BREACH ACT'S
REQUIREMENT TO NOTIFY INDIANA RESIDENTS AFFECTED BY THE 2016 W-2
BREACH

336. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

337. By engaging in consumer credit transactions in Indiana by owning or licensing the personal information of Indiana residents for commercial purposes, Equifax was and is "doing business in Indiana" as the term is defined by Ind. Code § 24-4.9-2-4.

338. The intrusion and unauthorized acquisition of the personal information described above were "breaches of the security of data," as defined by Indiana Code § 24-4.9-2-2, also known as "data breaches."

339. After discovering or being notified of a data breach, a data base owner shall disclose the breach to an Indiana resident whose personal information may have been acquired by an unauthorized person. Indiana Code § 24-4.9-3-1(a).

340. A data base owner shall make disclosure by mail, telephone, fax, or email.

Indiana Code § 24-4.9-3-4(a). If a data base owner determines that the cost of disclosure will be more than \$250,000, the data base owner may elect to make the disclosure by using both of the following methods:

- a) Conspicuous posting of the notice on the website of the data base owner, if the data base owner maintains a website.
- b) Notice to major news reporting media in the area where the Indiana residents affected by the data breach reside.

Ind. Code 24-4.9-3-4(b).

341. A data base owner must make the notification “without unreasonable delay.”

342. By failing to disclose the 2016 W-2 Breach to affected Indiana residents in accordance with Indiana Code § 24-4.9-3-1(a) or § 24-4.9-3-4, Equifax committed a deceptive act that is actionable by the Attorney General under Indiana Code § 24-4.9-4-1.

COUNT VII:
EQUIFAX VIOLATED THE DISCLOSURE OF SECURITY BREACH ACT’S
REQUIREMENT TO NOTIFY INDIANA RESIDENTS AFFECTED BY THE 2017 W-2
BREACH

343. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

344. By failing to disclose the 2017 W-2 Breach to affected Indiana residents in accordance with Indiana Code § 24-4.9-3-1(a) or § 24-4.9-3-4, Equifax committed a deceptive act that is actionable by the Attorney General under Indiana Code § 24-4.9-4-1.

COUNT VIII:
EQUIFAX VIOLATED THE DISCLOSURE SECURITY BREACH ACT’S REQUIREMENT
TO NOTIFY INDIANA RESIDENTS AFFECTED BY THE 2017 APACHE STRUTS
BREACH

345. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

346. Following its discovery of the 2017 Apache Struts Breach on July 29, 2017, Equifax knew within days the breach was so large, alternative notice would be required, yet it waited nearly six weeks before making its announcement on September 7, 2017.

347. By failing to disclose the 2017 Apache Struts Breach to affected Indiana residents in accordance with Indiana Code § 24-4.9-3-1(a) or § 24-4.9-3-4, Equifax committed a deceptive act that is actionable by the Attorney General under Indiana Code § 24-4.9-4-1.

COUNT IX:

EQUIFAX VIOLATED DISCLOSURE OF SECURITY BREACH ACT'S REQUIREMENT TO MAINTAIN REASONABLE SECURITY PROCEDURES FOR THE 2016 W-2 BREACH

348. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

349. The information stolen in the 2016 W-2 Breach described above is “personal information” as that term is defined by Indiana Code § 24-4.9-2-10.

350. The personal information was not encrypted or redacted as those terms are defined in Indiana Code § 24-4.9-2-5 and 11.

351. Equifax is a “data base owner” as that term is defined in Indiana Code § 24-4.9-2-3. A data base owner shall “implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.” Indiana Code § 24-4.9-3-3.5(c).

352. By failing to comply with multiple PCI DSS requirements and by failing to employ other industry standard security measures as described above, Equifax failed to implement and maintain reasonable procedures to protect and safeguard the personal information of Indiana residents.

353. Equifax knew or should have known that unauthorized acquisition of personal information could lead to identity theft, fraud, or other related harm to affected Indiana residents, as described in Indiana Code § 24-4.9-3-1(a).

354. Equifax failed to adequately protect the Indiana residents whose personal information was exposed by the breach.

355. Equifax knowingly and intentionally failed to comply with Indiana Code § 24-4.9-3-3.5(c), which is a deceptive act that is actionable by the Attorney General. Indiana Code § 24-4.9-3-3.5(e).

COUNT X:

EQUIFAX VIOLATED DISCLOSURE OF SECURITY BREACH ACT'S REQUIREMENT TO MAINTAIN REASONABLE SECURITY PROCEDURES FOR THE 2017 W-2 BREACH

356. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

357. Since 2014, Equifax knew that its Workforce Solutions authentication system was outdated and insecure. By failing to implement appropriate safeguards, Equifax continued to expose the data of Indiana residents to criminal hackers.

358. Equifax knew or should have known that unauthorized acquisition of personal information could lead to identity theft, fraud, or other related harm to affected Indiana residents, as described in Ind. Code § 24-4.9-3-1(a).

359. Equifax failed to adequately protect the Indiana residents whose personal information was exposed by the breach.

360. Equifax knowingly and intentionally failed to comply with Indiana Code § 24-4.9-3-3.5(c), which is a deceptive act that is actionable by the Attorney General. Indiana Code § 24-4.9-3-3.5(e).

COUNT XI:
EQUIFAX VIOLATED DISCLOSURE OF SECURITY BREACH ACT'S REQUIREMENT
TO MAINTAIN REASONABLE SECURITY PROCEDURES FOR THE 2017 APACHE
STRUTS BREACH

361. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs of this Complaint as though fully alleged herein.

362. Equifax knew the data of Indiana residents was stored in plain text, making it subject to theft by hackers.

363. Equifax knew or should have known that unauthorized acquisition of personal information could lead to identity theft, fraud, or other related harm to affected Indiana residents, as described in Ind. Code § 24-4.9-3-1(a).

364. Equifax failed to adequately protect the 3.9 Million Indiana residents whose personal information was exposed by the breach.

365. Equifax knowingly and intentionally failed to comply with Indiana Code § 24-4.9-3-3.5(c), which is a deceptive act that is actionable by the Attorney General. Indiana Code § 24-4.9-3-3.5(e).

H. RELIEF REQUESTED

366. The State requests the Court enter judgment against the Defendants, Equifax, Inc., Equifax Information Services, LLC, and Equifax Consumer Services, LLC, on the Counts described above.

367. The State seeks a permanent injunction, under Ind. Code § 24-4.9-4-2(1), enjoining Equifax and its agents, representatives, employees, successors, and assigns, from:

367.1. Violating its duty pursuant to Ind. Code § 24-4.9-3-3.5(c) to implement
and maintain reasonable procedures, *including taking any appropriate*

corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner; and

367.2. Engaging in potential criminal conduct, including but not limited to, violating the provisions of 18 U.S. Code § 1344; 18 U.S. Code § 1346 and 18 U.S. Code § 1349.

368. The State seeks a permanent injunction, under Indiana Code §24-5-0.5-4(c)(1), enjoining Equifax and its agents, representatives, employees, successors, and assigns, from committing unfair, abusive, or deceptive acts, omissions, or practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a) as alleged in Counts, I, II, and III.

369. The State seeks restitution for the money unlawfully received from the aggrieved consumers harmed by the deceptive acts in Counts I, II, and III of the Complaint pursuant to Indiana Code §24-5-0.5-4(c)(2), in an amount to be determined at trial.

370. The State seeks civil penalties on Counts I, II, III, and IV of the Complaint, under Indiana Code § 24-5-0.5-4(g), for the Defendants' knowing violations of Indiana Code §24-5-0.5-3(a), in an amount to be determined at trial.

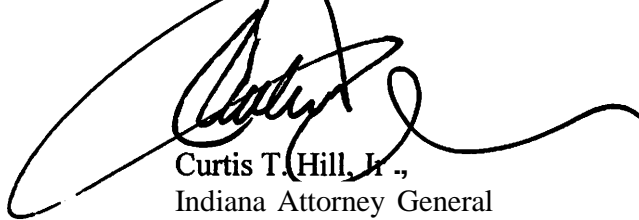
371. The State seeks civil penalties on Counts I, II, III and V of the Complaint, under Indiana Code § 24-5-0.5-8, for the Defendants' incurable deceptive acts as set forth in Indiana Code §24-5-0.5-2(a) (8), in an amount to be determined at trial.

372. The State seeks civil penalties on Counts VI, VII, VIII, IX, X, and XI of the Complaint under Indiana Code § 24-4.9-4-2(2) for the Defendants' violations of Indiana Code §24-4.9-4-1, in an amount to be determined at trial.

349. The State seeks costs, under Indiana Code § 24-5-0.5-4(c) (4) and Indiana Code §24-4.9-4-2(3), awarding the Office of the Attorney General its reasonable expenses incurred in the investigation and prosecution of this action.

350. The State seeks all other just and proper relief.

Respectfully submitted,

A large, stylized handwritten signature in black ink, appearing to read 'C. Hill, Jr.', is written over the typed name.

Curtis T. Hill, Jr.,
Indiana Attorney General
Atty. No. 13999-20

By: /s/Douglas S. Swetnam
Douglas S. Swetnam
Section Chief, Data Privacy & Identity Theft
Atty. No. 15860-49

By: /s/Vanessa L. Voigt-Gould
Vanessa L. Voigt Gould
Deputy Attorney General
Atty No. 26719-49

By: /s/Michael A. Eades
Michael A. Eades
Deputy Attorney General
Attorney No. 31015-49

Office of Attorney General Curtis T. Hill, Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204

REQUEST FOR TRIAL BY JURY

Plaintiff, State of Indiana, by Attorney General Curtis T. Hill, Jr. and Deputy Attorneys General Douglas Swetnam, Vanessa Voigt Gould, and Michael Eades, hereby demands a trial by jury pursuant to Indiana Rules of Trial Procedure 38 and Indiana Constitution Article I Section 20.

By: /s/Douglas S. Swetnam
Douglas S. Swetnam
Section Chief Data Privacy & Identity Theft
Atty. No. 15860-49

By: /s/Vanessa L. Voigt Gould
Vanessa L. Voigt Gould
Deputy Attorney General
Atty No. 26719-49

By: /s/Michael A. Eades
Michael A. Eades
Deputy Attorney General
Attorney No. 31015-49

Office of Attorney General Curtis Hill, Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204