

UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF GEORGIA

**TEAMSTERS LOCAL 443 HEALTH
SERVICES & INSURANCE PLAN, on
behalf of itself and all others similarly
situated,**

Plaintiff,

-against-

**JOHN W. GAMBLE, JR., JOSEPH M.
LOUGHRAN, III, RODOLFO O.
PLODER, RICHARD F. SMITH,
JAMES E. COPELAND, JR., ROBERT
D. DALEO, WALTER W. DRIVER,
JR., MARK L. FEIDLER, G. THOMAS
HOUGH, L. PHILLIP HUMANN,
ROBERT D. MARCUS, SIRI S.
MARSHALL, JOHN A. MCKINLEY,
ELANE B. STOCK and MARK B.
TEMPLETON,**

Defendants,

and,

EQUIFAX, INC.,

Nominal Defendant.

Case No.

**VERIFIED SHAREHOLDER
DERIVATIVE COMPLAINT**

Plaintiffs Teamster Local 443 Health Services and Insurance Plan (“Teamsters Local 443” or “Plaintiff”), by their undersigned attorneys, derivatively and on behalf of Nominal Defendant Equifax, Inc. (“Equifax” or the “Company”), file this Verified Stockholder Derivative Complaint against Defendants Equifax, John W. Gamble, Jr., Joseph M. Loughran, III, Rodolfo O. Ploder, James E. Copeland, Jr., Robert D. Daleo, Walter W. Driver, Jr., Mark L. Feidler, G. Thomas Hough, L. Phillip Humann, Robert D. Marcus, Siri S. Marshall, John A. McKinley, Richard F. Smith, Elane B. Stock and Mark B. Templeton (the “Individual Defendants”) (collectively, “Defendants”) for breaches of their fiduciary duties to the Company. Plaintiff makes the following allegations based upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters, based on the investigation conducted by its attorneys. This investigation included, among other things, a review of the Company’s announcements and press releases; filings made by the Company with the United States Securities and Exchange Commission (“SEC”); corporate governance documents available on the Company’s website; governmental and regulatory investigations of the Company and documents relating thereto; and news reports and other publicly available information about the Company.

I. PRELIMINARY STATEMENT

1. This shareholder derivative action arises from Defendants' breach of fiduciary duties owed to its shareholders in connection with its most recent cybersecurity breach, which was announced to the public on September 7, 2017.

2. Despite warnings as early as March 2016 – when Equifax learned that its subsidiary, Equifax Workforce Solutions, had its website breached – that Equifax was in danger of serious data breaches that could expose to hackers the personal and financial data millions of Americans, Equifax and the other Defendants chose to do nothing to correct their inadequate internal controls over the Company's technology and data security.

3. Due to Defendants' failure to protect against this known risk, on or about July 29, 2017, Equifax discovered an unauthorized intrusion into its massive data files, resulting in unauthorized access to the personal and financial data of nearly half of the American citizenry (the "Data Breach").

4. Rather than immediately announcing the Data Breach, Equifax waited until September 7, 2017 to acknowledge that the Data Breach was discovered on July 29, 2017, potentially impacting approximately 143 million U.S. consumers. This data breach took place between May and July 2017, when cyber criminals exploited a U.S. website application vulnerability to gain access to Equifax files.

5. Incredibly, between the time of the Data Breach and the public disclosure by Equifax, three Equifax executives brazenly sold at least \$1.8 million

worth of shares, as follows: Defendant Gamble, Equifax's Corporate Vice President and Chief Financial Officer, sold shares worth \$946,374 on August 1, 2017; Defendant Loughran, President of Equifax's United States Information Solutions ("USIS") business, exercised options to dispose of stock worth \$584,099 on August 1, 2017; Defendant Ploder, Equifax's President of Workforce Solutions, sold shares worth \$250,458 on August 2, 2017.

6. Equifax failed to secure and safeguard consumers' personal and private information which it collects from various sources in connection with the operation of its business as a consumer credit reporting agency. The information obtained by hackers as a result of the Data Breach includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, Equifax admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

7. Equifax failed to take adequate and reasonable measures to ensure its data systems were protected; failed to disclose to its customers the material fact that it did not have adequate computer systems and security practices in place to safeguard consumers' personal and private information; failed to take available steps to prevent and stop the breach from ever happening; and failed to monitor and detect the breach on a timely basis. As a direct result of Defendants' failures to protect the consumer information they are tasked with safeguarding, the

Company's stock price has plummeted, it is subject to multiple criminal and civil lawsuits, and it faces multiple public inquiries into the Data Breach, all of which have caused the Company to expend, and continue to expend, significant sums of money.

II. JURISDICTION & VENUE

8. Pursuant to 28 U.S.C. §1331 and section 27 of the Securities Exchange Act of 1934 (the "Exchange Act"), this Court has jurisdiction over the claims asserted herein for violations of sections 14(a) and 20(a) of the Exchange Act and SEC Rule 14a-9 promulgated thereunder. This Court has supplemental jurisdiction over the remaining claims under 28 U.S.C. §1367.

9. This Court has jurisdiction over each Defendant named herein because each Defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.

10. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Equifax maintains its principal place of business in this District; (ii) one or more of the Defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the Defendants' primary participation in the wrongful acts

detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Equifax, occurred in this District; and (iv) Defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

III. PARTIES & INTERESTED NON-PARTIES

A. PLAINTIFF

11. Plaintiff Teamsters Local 443 Health Services & Insurance Plan (“Teamsters Local 443”) is a resident of Connecticut and currently is and continuously has been a stockholder of Equifax since prior to May 2017. Plaintiff made a demand for books and records pursuant to O.C.G.A. §14-2-1602 on September 15, 2017. The Company denied Plaintiffs’ request for inspection on October 9, 2017. Thereafter, Plaintiff made a demand pursuant to O.C.G.A. §14-2-742 for the Company to take Suitable Action and address the harm done to it at the hands of the Board of Directors (“Plaintiff’s Demand”). On or about November 27, 2017, Counsel for the Company notified Plaintiff that it formed a purportedly “independent” Committee that is “undertaking a thorough examination of all allegations contained in Plaintiff’s Demand. This “independent” committee is comprised of interested Director Defendants Stock and Hough. The third member of the committee is Scott A. MacGregor. As a result of this Committee’s interestedness, Plaintiff finds it implausible that any conclusion will be fair, just or reasonable.

B. NOMINAL DEFENDANT

12. Nominal Defendant Equifax is a Georgia corporation with its principal executive offices located at 1550 Peachtree Street NE, Atlanta, GA 30309. Equifax common stock trades on the New York Stock Exchange under the ticker symbol “EFX.”

13. Equifax is a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers. Equifax is a consumer credit reporting agency in the United States that gathers and maintains information on over 800 million consumers and more than 88 million businesses worldwide. Along with Experian and TransUnion, Equifax is one of the three largest American credit agencies.

14. Equifax has a large and diversified group of clients, including financial institutions, corporations, governments and individuals. Its products and services are based on comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data.

15. In conducting business, Equifax acquires a substantial amount of information about individual consumers, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic stripe of a card and used to

validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards.

16. Equifax uses advanced statistical techniques and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for their clients. Equifax purports to help consumers understand, manage and protect their personal information and make more informed financial decisions. Equifax also provides information, technology and services to support debt collections and recovery management. Additionally, Equifax is a leading provider of payroll-related and human resource management business process outsourcing services in the U.S.

17. Equifax currently operates in four global regions: North America (U.S. and Canada), Asia Pacific (Australia and New Zealand), Europe (the United Kingdom, or U.K., Spain and Portugal) and Latin America (Argentina, Chile, Costa Rica, Ecuador, El Salvador, Honduras, Mexico, Paraguay, Peru and Uruguay). Equifax maintains support operations in the Republic of Ireland. Equifax also offers branded credit services in Russia and India through joint ventures, has investments in consumer and/or commercial credit information companies through joint ventures in Cambodia, Malaysia and Singapore, and has an investment in a consumer and commercial credit information company in Brazil.

18. Equifax originally was incorporated under the laws of the State of Georgia in 1913, and its predecessor company dates back to 1899. Based in Atlanta, Georgia, Equifax has US \$2.7 billion in annual revenue. Equifax is organized and reports its business results in four operating segments, as follows:

- a. **U.S. Information Solutions (USIS)** — provides consumer and commercial information solutions to businesses in the U.S. including online information, decisioning technology solutions, fraud and identity management services, portfolio management services, mortgage reporting and financial marketing services.
- b. **International** — which includes Equifax’s Canada, Europe, Asia Pacific and Latin America business units, provides products and services similar to those available in the USIS operating segment but with variations by geographic region. In Europe, Asia and Latin America, Equifax also provides information, technology and services to support debt collections and recovery management.
- c. **Workforce Solutions** — provides services enabling Equifax’s clients to verify income and employment (Verification Services) as well as to outsource and automate the performance of certain payroll-related and human resources management business processes, including unemployment cost management, tax credits and incentives and I-9 management services and services to allow employers to ensure compliance with the Affordable Care Act (Employer Services).
- d. **Global Consumer Solutions** — provides products to consumers in the United States, Canada, and the U.K., enabling them to understand and monitor their credit and monitor and help protect their identity. Equifax also sells consumer and credit information to resellers who combine Equifax’s information with other information to provide direct to consumer monitoring, reports and scores.

C. INDIVIDUAL DEFENDANTS – Officers

19. Defendant John W. Gamble, Jr. (“Gamble”) has served as Equifax’s Corporate Vice President and Chief Financial Officer since May 2014. On August

1, 2017 Gamble sold shares worth \$946,374. This transaction was not part of a 10b5-1 scheduled trading plan. Equifax paid Defendant Gamble the following compensation as an executive:

Year	Salary (\$)	Bonus (\$)	Stock Awards (\$)	Option Awards (\$)	Non-Equity Incentive Plan Comp. (\$)	Change in Pension Value and Nonqualified Deferred Comp. Earnings (\$)	All Other Comp. (\$)	Total (\$)
2016	632,243	0	1,244,532	0	758,692	443,000	16,640	3,095,107
2015	609,693	0	1,462,409	0	695,050	266,700	19,792	3,053,644
2014	353,077	0	5,983,154	0	482,526	96,400	163,945	7,079,102

20. Defendant Joseph M. Loughran, III (“Loughran”) serves as President of Equifax’s United States Information Solutions (USIS) business. Prior to being named to this role, Loughran served until July 2017 as the Equifax’s Chief Marketing Officer. Prior thereto, he served as President, Global Consumer Solutions since January 4, 2010. Loughran was also Senior Vice President, Corporate Development from April 2006 to December 2009. On August 1, 2017 Loughran exercised options to dispose of stock worth \$584,099. This transaction was not part of a 10b5-1 scheduled trading plan.

21. Defendant Rodolfo O. Ploder (“Ploder”) has served as Equifax’s President of Workforce Solutions since November 2015. From April 2010 to November 2015, he served as President, U.S. Information Solutions. Prior thereto, he served as President, International, from January 2007 to April 2010. From February 2004 to January 2007, he was Group Executive, Latin America. On

August 2, 2017 Ploder sold shares worth \$250,458. This transaction was not part of a 10b5-1 scheduled trading plan. Equifax paid Defendant Ploder the following compensation as an executive:

Year	Salary (\$)	Bonus (\$)	Stock Awards (\$)	Option Awards (\$)	Non-Equity Incentive Plan Comp. (\$)	Change in Pension Value and Nonqualified Deferred Comp. Earnings (\$)	All Other Comp. (\$)	Total (\$)
2016	500,000	0	785,003	0	600,000	770,000	105,314	2,760,317
2015	462,273	0	944,479	0	554,726	93,800	24,831	2,080,109
2014	-	-	-	-	-	-	-	-

22. Richard F. Smith (“Smith”) has been Chairman and Chief Executive Officer of Equifax since September 2005. Prior to joining Equifax, Smith spent 22 years with GE, holding several president and chief executive officer roles across numerous businesses, including Engineering Thermoplastics, Asset Management, Leasing, and Insurance Solutions. Equifax paid Defendant Smith the following compensation as a director:

Year	Salary (\$)	Bonus (\$)	Stock Awards (\$)	Option Awards (\$)	Non-Equity Incentive Plan Comp. (\$)	Change in Pension Value and Nonqualified Deferred Comp. Earnings (\$)	All Other Comp. (\$)	Total (\$)
2016	1,450,000	0	7,323,095	0	3,045,000	3,027,100	119,368	14,964,563
2015	1,450,000	0	8,315,508	0	3,045,000	0	112,203	12,922,711
2014	1,450,000	0	6,159,236	0	2,345,184	3,815,200	110,055	13,879,675

D. INDIVIDUAL DEFENDANTS – Current Directors

23. L. Phillip Humann (“Humann”) has been on the Equifax Board of Directors since 1992. Humann serves on the Compensation, Human Resources &

Management Succession Committee. In 2016, Humann's total compensation from Equifax was \$263,874.

24. Mark B. Templeton ("Templeton") has been on the Equifax Board of Directors since 2008. Templeton serves on the Audit Committee and Technology Committee. In 2016, Templeton's total compensation from Equifax was \$245,050.

25. Robert D. Daleo ("Daleo") has been on the Equifax Board of Directors since 2006. Daleo is the Chair of the Audit Committee and also serves on the Compensation, Human Resources & Management Succession Committee and Executive Committee. In 2016, Daleo's total compensation from Equifax was \$260,996.

26. Siri S. Marshall ("Marshall") has been on the Equifax Board of Directors since 2006. Marshall is the Chair of the Governance Committee and also serves on the Compensation, Human Resources & Management Succession Committee and Executive Committee. In 2016, Marshall's total compensation from Equifax was \$252,753.

27. Walter W. Driver Jr. ("Driver") has been on the Equifax Board of Directors since 2007. Driver serves on the Governance Committee. In 2016, Driver's total compensation from Equifax was \$238,867.

28. John A. McKinley ("McKinley") has been on the Equifax Board of Directors since 2008. McKinley is the Chair of the Technology Committee and

also serves on the Audit Committee and Executive Committee. In 2016, McKinley's total compensation from Equifax was \$255,409.

29. Mark L. Feidler ("Feidler") has been on the Equifax Board of Directors since 2007. Feidler is the Chair of the Executive Committee and also serves on the Governance Committee and Technology Committee. In 2016, Feidler's total compensation from Equifax was \$255,972.

30. Robert D. Marcus ("Marcus") has been on the Equifax Board of Directors since 2013. Marcus is the Chair of the Compensation, Human Resources & Management Succession Committee and also serves on the Executive Committee and Governance Committee. In 2016, Marcus's total compensation from Equifax was \$241,975.

31. G. Thomas Hough ("Hough") has been on the Equifax Board of Directors since 2016. Hough serves on the Audit Committee and Technology Committee. In 2016, Hough's total compensation from Equifax was \$199,474.

32. Elane Stock ("Stock") has been on the Equifax Board of Directors since January 1, 2017. Stock serves on the Technology Committee.

33. James E. Copeland, Jr. ("Copeland") is a former member of the Equifax Board of Directors. In 2016, Copeland's total compensation from Equifax was \$247,082.

IV. FIDUCIARY DUTIES

A. Duties of the Individual Defendants

34. By reason of their positions as officers, directors, and/or fiduciaries of Equifax and because of their ability to control the business and corporate affairs of Equifax, the Individual Defendants owed and continue to owe Equifax and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Equifax in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Equifax and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interests or benefit.

35. To discharge their duties, the officers and directors of Equifax were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Equifax were required to, among other things:

- a. ensure the Company complied with its legal obligations and requirements, including complying with regulatory requirements by devising and implementing a system of internal controls sufficient to ensure the Company's customers' personal and financial information is protected;
- b. monitor and oversee the system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;

- c. conduct the affairs of the Company in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock;
- d. remain informed as to how Equifax conducted its operations, and upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices as necessary to comply with applicable laws; and
- e. ensure the Company was operated in a diligent, honest, and prudent manner in compliance with all applicable laws, rules, and regulations.

36. The Individual Defendants, because of their positions of control and authority as directors and/or officers of Equifax, were able to, and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein.

37. At all times relevant hereto, each of the Individual Defendants was the agent of each of the other Individual Defendants and of Equifax, and was at all times acting within the course and scope of such agency.

B. Duties of the Board of Directors

38. According to the Notice of the 2017 Annual Meeting of Shareholders and Proxy Statement (the "Proxy Statement"), the Board of Directors of Equifax oversees risk management at the Company. The Board exercises direct oversight of strategic risks to the Company and other risk areas not delegated to one of its committees.

39. The Board of Directors monitors the Company's "tone at the top" and risk culture and oversees emerging strategic risks. On an annual basis, the Board

performs an enterprise risk assessment with management to review the principal risks facing the Company and monitors the steps management is taking to map and mitigate these risks. The Board then sets the general level of risk appropriate for the Company through business strategy reviews. Risks are assessed throughout the business, focusing on (i) financial, operational and strategic risk; and (ii) ethical, legal, privacy, data security (including cybersecurity), regulatory and other compliance risks.

C. Duties of the Audit Committee

40. During the time of the events complained of herein, the Audit Committee included Defendants Daleo, Hough, McKinley and Templeton. The Audit Committee met five times in 2016. *See* 2017 Proxy Statement, at 18.

41. According to Equifax's website, the Audit Committee's primary function is to assist the Board of Directors in fulfilling its oversight responsibilities for: (1) the integrity of the Company's statements and other financial information provided to any governmental body, its shareholders or the public; (2) the Company's systems for complying with legal and regulatory requirements; (3) the independent auditor's qualifications, independence, and performance; (4) the performance of the Company's internal audit function; and (5) the integrity of the Company's internal controls regarding finance, accounting, and auditing, and its financial reporting processes.

42. In addition, according to Equifax's Proxy Statement, the Audit Committee reviews risks related to financial reporting; discusses material violations, if any, of the Company's ethics, legal, regulatory and other compliance policies. The Audit Committee also considers their annual audit risk assessment which identifies internal control risks and drives the internal and external audit plan for the ensuing year. Last, the Audit Committee considers the impact of risk on the Company's financial position and the adequacy of the Company's risk-related internal controls.

D. Duties of the Compensation, Human Resources & Management Succession Committee

43. During the time of the events complained of herein, the Compensation, Human Resources & Management Succession Committee included Defendants Marcus, Daleo, Humann and Marshall. The Compensation, Human Resources & Management Succession Committee met four times in 2016. *See* 2017 Proxy Statement, at 18.

44. According to Equifax's website, the primary function of the Compensation, Human Resources and Management Succession Committee is to assist the Board of Directors in fulfilling its oversight responsibility with respect to: (1) determining and evaluating the compensation of the Chief Executive Officer; (2) approving and monitoring the executive compensation plans, policies and programs of the Company; (3) reviewing and discussing with management the

Compensation Disclosure and Analysis (“CD&A”) to be included in the Company’s annual proxy statement and determine whether to recommend to the Board that the CD&A be included in the proxy statement; and (4) advising management on succession planning and other significant human resources matters. In addition, according to Equifax’s Proxy Statement, the Compensation Committee reviews compensation, human resource and management succession risks.

E. Duties of the Executive Committee

45. During the time of the events complained of herein, the Executive Committee included Defendants Feidler, Daleo, Marcus, Marshall and McKinley. The Executive Committee did not meet in 2016. *See* 2017 Proxy Statement, at 18.

46. According to Equifax’s website, the Executive Committee is authorized by the Bylaws of the Company to exercise all of the powers of the Board in managing the business and property of the Company during the intervals between meetings of the Board of Directors, subject to Board discretion or as limited by applicable laws.

F. Duties of the Governance Committee

47. During the time of the events complained of herein, the Governance Committee included Defendants Marshall, Driver, Feidler and Marcus. The Governance Committee met four times in 2016. *See* 2017 Proxy Statement, at 18.

48. According to Equifax's website, the Governance Committee assists the Board with respect to (1) Board organization, membership, and function, (2) committee structure and membership, and (3) oversight of evaluation and compensation of the Board. In addition, according to the Proxy Statement, the Governance Committee focuses on corporate governance risks, including evaluation of the Company's leadership and risk oversight structure.

G. Duties of the Technology Committee

49. During the time of the events complained of herein, the Technology Committee included Defendants McKinley, Feidler, Hough, Stock and Templeton.

50. According to Equifax's Proxy Statement, the Technology Committee focuses on technology-related risks and opportunities, including data security. The Technology Committee oversees the Company's mitigation of any identified enterprise-wide risks in the following areas: information technology strategy; significant new product lines or technology investments; and the Company's response to external technology-based threats and opportunities.

51. In addition, the goals and responsibilities of the Technology Committee are to monitor the Company's long-term strategy and significant investments in the areas listed below:

- a. information technology long-term strategy in support of the Company's evolving global business needs;
- b. review and present observations to the Board with respect to the annual technology budget;

- c. significant new product development programs (including software initiatives) and new technology investments, including technical and market risks associated with product development and investment;
- d. future trends in technology that may affect the Company's strategic plans, including overall industry trends and new opportunities and threats occasioned by new technologies, especially disruptive technologies;
- e. review the Company's technology investments and infrastructure associated with risk management, including policies relating to information security, disaster recovery and business continuity;
- f. assess the scope and quality of the Company's intellectual property; and
- g. undertake from time to time such additional activities within the scope of the Committee's primary purposes as it may deem appropriate and/or as assigned by the Board of Directors, the Chairman of the Board and Chief Executive Officer.

H. Duties Arising From Equifax's Business Code of Conduct and Ethics

52. During the time of the events complained of herein, Equifax's Code of Ethics and Business Conduct, which applied to all of the Individual Defendants, provided in pertinent part:

Violating relevant laws, regulations or the Code, or encouraging others to do so, exposes the Company to liability and puts our reputation at risk. If an ethics or compliance problem does occur, you are required to report it so that an effective solution can be developed.

* * *

One of our most valuable assets is information. Each of us must be vigilant and protect confidential information. This means keeping it secure, limiting access to those who have a need to know in order to

do their job, and avoiding discussion of confidential information in public areas ... Confidential information includes all non-public information that might be of use to competitors, or harmful to the Company or its customers, if disclosed.

* * *

Our customers and our business partners place their trust in us. We must protect their confidential information. **MAKE SURE YOU:** Learn about the types of information which are given heightened protection by the law and Company policy (such as personally identifiable information, like social security numbers and bank account numbers) and protect them through appropriate means (such as encryption or other types of limited access). Never share confidential information inside or outside the Company except as authorized. Immediately report any loss or theft of confidential information.

* * *

Business partners, government officials and the public need to be able to rely on the accuracy and completeness of our disclosures and business records. Accurate information is also essential within the Company so that we can make good decisions. Our books and records must be clear, complete and in compliance with accepted accounting rules and controls. Employees with a role in financial or operational recording or reporting have a special responsibility in this area, but all of us contribute to the process of recording business results and maintaining records. Each of us is responsible for helping to ensure the information we record is accurate and complete and maintained in a manner that is consistent with our system of internal controls. If you suspect any irregularity relating to the integrity of our records, you need to report it immediately to your supervisor, the Legal Department or the Corporate Ethics Officer.

* * *

Insider Trading

No Equifax employee, officer, director or other “insider” may purchase or sell Equifax securities while in possession of material, nonpublic information relating to Equifax (“insider trading”).

See Equifax, *Code of Ethics and Business Conduct*, https://www.equifax.com/assets/corp/code_of_ethics.pdf (last visited September 13, 2017).

I. Duties Arising from Equifax’s Privacy Policies

53. In addition to their general duties to ensure that systems were in place to safeguard customers’ information to prevent the risk of foreseeable harm to others, the Individual Defendants were at all relevant times obligated to establish systems to safeguard such information by, among other things, rules governing payment card transactions, industry standards, various federal and state laws, and its own commitments, internal policies and procedures.

54. Equifax has continuously acknowledged this legal duty and reassured the public that this duty was being met in the Company’s “Privacy Policy” posted on its website. For example, the policy currently tells the public that Equifax has “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.”

See Equifax, *Privacy*, <http://www.equifax.com/privacy> (last visited September 13, 2017).

V. BREACHES OF FIDUCIARY DUTIES

55. Each Individual Defendant, by virtue of his or her position as a director and/or officer, owed to the Company and to its stockholders the fiduciary duty of loyalty and good faith and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and officers of Equifax, an absence of good faith on their part, and a reckless disregard for their duties to the Company and its stockholders, which the Individual Defendants were aware or should have been aware posed a risk of serious injury to the Company. The conduct of the Individual Defendants who also were officers and/or directors of the Company have been ratified by the remaining Individual Defendants who collectively comprised all of Equifax's Board.

56. The Individual Defendants breached their duty of loyalty and good faith by allowing Defendants to cause, or by themselves causing, the Company to misrepresent its protection of consumer and business data and delay the reporting of the Data Breach, as detailed herein. In addition, as a result of Defendants' course of conduct, the Company is now the subject of consumer class actions and a securities class action alleging securities law violations in connection with the

improper financial reporting. As a result, Equifax has expended, and will continue to expend, significant sums of money.

VI. CONSPIRACY, AIDING AND ABETTING AND CONCERTED ACTION

57. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary liability, the Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

58. During all times relevant hereto, the Individual Defendants, collectively and individually, initiated a course of conduct that was designed to and did: (i) conceal the fact that the Company had experienced massive data breaches; (ii) enhance the Individual Defendants' executive and directorial positions at Equifax and the profits, power, and prestige that the Individual Defendants enjoyed as a result of holding these positions; and (iii) deceive the Company's users and the investing public, including stockholders of Equifax, regarding the Individual Defendants' management of Equifax's operations. In furtherance of this plan, conspiracy, and course of conduct, the Individual Defendants, collectively and individually, took the actions set forth herein.

59. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. During this time, the Individual Defendants caused the Company to fail to disclose the Data Breach, which negatively impacted the Company's performance.

60. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to disguise the Individual Defendants' violations of federal securities laws, breach of fiduciary duties, and unjust enrichment, and to conceal adverse information concerning the Company's operations and future business prospects.

61. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by causing the Company to purposefully, recklessly, or negligently release improper statements. Because the actions described herein occurred under the authority of the Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

62. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing,

substantially assisted the accomplishment of that wrongdoing, and was aware of his or her overall contribution to and furtherance of the wrongdoing.

VII. SUBSTANTIVE ALLEGATIONS

A. Background on Data Breaches

63. Theft of customer data through breaches of retailers' point of sale systems hit the mainstream in 2007, when TJX Companies Inc. ("TJX") admitted in an SEC filing that at least 45.6 million credit and debit card numbers were stolen from its customers over an 18-month period. In addition, TJX disclosed that personal data provided in connection with the return of merchandise without receipts by about 450,000 customers had been stolen. The breach cost the company over \$250 million, including costs related to improving the company's computer system, as well as costs related to lawsuits, investigations and other claims stemming from the breach.

64. In early 2009, payment processor Heartland Payment Systems announced the largest data breach ever at that time to affect an American company. Heartland's breach exposed information from approximately 130 million credit and debit cards to cybercriminals. Malware planted on Heartland's network recorded card data as it arrived from retailers. Because the company processed payments for more than 250,000 businesses across the country, the impact was huge.

65. In April 2011, attackers targeted the Sony PlayStation Network that links Sony's home gaming consoles, as well as Sony Online Entertainment

(“SOE”), which hosts massively multiplayer online PC games, and the Qriocity video and music-streaming service. Initially, Sony said that only the personal information of 78 million PlayStation Network users – login credentials, names, addresses, phone numbers and email addresses – had been exposed, but the tally of compromised accounts rose by 24.6 million when investigators discovered the attackers had also penetrated SOE and Qriocity. The credit-card data of approximately 23,400 SOE users in Europe was also stolen. Following the initial breach disclosure, the PlayStation Network went dark worldwide for more than three weeks.

66. In November 2013, retail giant Target was the target of a cyber-attack that affected more than 41 million of the company’s customer payment card accounts. Cyber attackers gained access to Target’s computer gateway served through credentials stolen from a third-party vendor. Using the credentials to exploit weaknesses in Target’s system, the attackers gained access to a customer service database, installed malware on the system and captured full names, phone numbers, email addresses, payment card numbers, credit card verification codes, and other sensitive data. Along with affecting 41 million customer payment card accounts, the breach affected contact information for more than 60 million Target customers.

67. In September 2014, hardware and building-supplies warehouse retailer Home Depot admitted what had been suspected for weeks. Beginning in

April or May of the same year, “carders” had infected its point-of-sale systems at stores in the U.S. and Canada with malware that pretended to be antivirus software, but instead stole customer credit and debit cards. Fifty-six million payment cards were compromised as a result of this breach.

68. In February 2015, Anthem, formerly known as WellPoint and the second-largest health insurer in the U.S., revealed its customer database had been breached as a result of a cyberattack on its IT system. Stolen data included names, addresses, dates of birth, Social Security numbers, email addresses, employment information and income data. As many as 80 million patient and employee records were exposed.

69. In September 2015, credit reporting agency Experian said that a data breach at one of its business units may have compromised the personal records of about 15 million people including customers of T-Mobile. Hackers appear to have obtained access to an Experian server that hosted the personal information of people who applied for the carrier’s services between September 1, 2013 and Sept. 16, 2015. The information accessed included names, addresses, Social Security numbers, dates of birth, driver’s license numbers, and passport IDs.

B. Equifax Was Aware of Its Vulnerability to Data Breaches

70. The Individual Defendants were – and at all relevant times have been – aware that the information Equifax maintains about its customers is highly

sensitive and could be used for nefarious purposes by third parties, such as perpetuating identity theft and making fraudulent purchases.

71. Because of the sensitivity of the information Equifax maintains, the Individual Defendants are – and at all relevant times have been – aware of the importance of safeguarding the Company’s customers’ information and of the foreseeable consequences that would occur if its security systems were breached, specifically including the risk of massive liability to financial institutions and consumers, as well as potential exposure to criminal and civil liability and loss of reputation.

72. Indeed, as early as in 2001, Equifax realized the importance of protecting consumer privacy. In its annual report, filed with the SEC on March 12, 2002, Equifax stated, “it is the Company’s policy to treat all information with a high degree of security reflecting our recognition of individuals’ privacy concerns.” *See* Equifax 2001 Form 10-K, at 4.

73. Equifax further identified the potential repercussions of a data security breach as a substantial “Risk Factor” for its business in its annual report, filed with the SEC on March 11, 2004, stating: “Security is important to our business, and breaches of security, or the perception that e-commerce is not secure, could harm our business.”

74. In addition to their general duties to ensure that systems are in place to safeguard customers’ information to prevent the risk of loss, the Individual

Defendants were – and at all relevant times have been – obligated to oversee the Company’s compliance, industry standards and various federal and state laws, as well as with the Company’s own commitments, internal policies and procedures.

75. Equifax continuously has acknowledged this legal duty and reassured the public its duty was being met in the company’s “Privacy Policy” posted on its website. Equifax’s policy states: “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 about businesses. Safeguarding the privacy and security of information, both online and offline is a top priority for Equifax.”

76. Despite Equifax’s early claims of protection of consumer information, Defendants did little to safeguard it.

77. According to an October 6, 2017 news article in The Wall Street Journal, titled, “A Warning Shot on Equifax: Index Provider Flagged Security Issues Last Year,” financial company MSCI, Inc. (“MSCI”) warned in August of 2016 that Equifax wasn’t equipped for the “increasing frequency and sophistication of data breaches.” After poring over the Equifax records, MSCI said it found zero evidence that the credit scoring company conducted regular cybersecurity audits or provided training to employees on identifying risks, nor did it have any emergency plans to handle a data breach or leak. Due to these

cybersecurity concerns, MSCI removed Equifax from its stock indices, which evaluate companies based on environmental, social and governance criteria. “If you’re an investor or asset manager and you see these rock-bottom evaluations of Equifax, it had to have given you pause,” Jon Hale, head of sustainability research at Morningstar Inc., told The Wall Street Journal.

78. Then, Equifax disclosed in May 2017 that its subsidiary Equifax Workforce Solutions, a/k/a TALX Corporation (“TALX”), which provides online payroll, HR and tax services, had its W-2 Express website breached. This breach continued from April 2016 through March 2017. Equifax refused to say how many consumers were impacted by the breach, but because this incident exposed the tax and payroll records of its customers’ employees, the victim customers in turn were required to notify their employees as well. Then, five companies that used TALX publicly disclosed data breaches, including defense contractor giant Northrop Grumman; staffing firm Allegis Group; Saint-Gobain Corp.; Erickson Living; and the University of Louisville.

79. Incredibly, Equifax’s TALX division had amazingly lax security: it let customers who use the firm’s payroll management services authenticate to the service with little more than a 4-digit personal identification number (PIN). Identity thieves who specialize in perpetrating tax refund fraud figured out that they could reset the PINs of payroll managers at various companies just by answering some multiple-guess questions — known as “knowledge-based

authentication” or KBA questions — such as previous addresses and dates that past home or car loans were granted.

80. National grocery-chain Kroger, another company which used TALX, also was the target of this type of breach. Once again, Equifax said the identity thieves were able to reset the 4-digit PIN given to customer employees as a password and then steal W-2 tax data after successfully answering personal questions about those employees. In response to these breaches, a fraud analyst with Garner, Inc. noted that, “It’s pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN.”

C. The May-July 2017 Data Breach and Response

81. On July 29, 2017, Equifax’s Security team observed “suspicious network traffic” associated with its online web portal and blocked it.

82. Yet, it was not until a September 7, 2017 press release that Equifax announced on July 29, 2017, the Company discovered a “cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company’s investigation, the unauthorized access occurred from mid-May through July 2017.”

The Company announced that the information obtained by hackers was widespread and detailed, and included “names, Social Security numbers, birth dates, addresses and, in some instances, driver’s license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal

identifying information for approximately 182,000 U.S. consumers, were accessed.” Equifax further stated that it had immediately retained “a leading, independent cybersecurity firm.” That firm -- Mandiant -- “has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted.”

83. On September 26, 2017, the Board of Equifax announced that Richard Smith would “retire” as Chairman of the Board of Directors and Chief Executive Officer, effective immediately.

84. On October 2, 2017, Equifax announced the results of the investigation performed by Mandiant: an additional 2.5 million U.S. consumers potentially were impacted, bringing the total number of persons and entities whose data was exposed in the Data Breach to 145.5 million.

85. Unbelievably, as noted in a “Wired” Blogspot by Ron Fein titled, “Equifax Deserves the Corporate Death Penalty,” more than one week after the Data Breach was disclosed, “a small computer company in Milwaukee noticed that in one Equifax computer system based in South America, customer records could still be accessed by entering the username ‘admin’ and the password ... ‘admin.’”

86. The Defendants continued to fail in their responsibilities even one month after the Data Breach. The website Clark, in an article by Craig Johnson titled “Equifax Data Breach: Embattled credit bureau says it was hacked again,” reported on October 12, 2017 that Equifax confirmed that it was hacked again, this time with a fake Flash installer application. As a result of this announcement, the

stock's price dropped from \$113.10 per share on October 11, 2017 to \$108.81 per share on October 12, 2017.

87. On or about October 16, 2017, as reported on the website CISOMAG, which describes itself as “the handbook for Chief Information Security Officers,” Equifax on October 12, 2017, “temporarily lost a fraud prevention contract worth \$7.25 million with the IRS that it had received on September 29, 2017.” The IRS’s “precautionary measure” put on hold the multi-million-dollar deal after the discovery of the October 12, 2017 incident set forth above. Thus, not only did the Defendants’ malfeasance cost the Company in expenses for legal matters and the decline of its stock price, but it cost Equifax millions of dollars in business deals.

88. As set forth above, Equifax had ample notice of the potential risk associated with a data breach, which as noted in the Company’s annual reports, would subject the Company to litigation, regulatory fines, penalties, reputational damage and loss of business, any of which could have a material effect on its cash flows, competitive position, financial condition or results of operations. During the time of the events complained of herein, the Individual Defendants were well-aware that a data security breach such as the one that occurred on July 29, 2017 was a substantial “Risk Factor” for the Company.

DEFENDANTS' IMPROPER STATEMENTS

89. As set forth above, in the early 2000s, reports of breaches of major retailers' point of sale systems became commonplace and an issue of concern for the Company.

90. In its FY 2008 annual report filed with the SEC on February 26, 2009, Equifax identified the potential repercussions of a data security breach as a substantial "Risk Factor" for its business:

If we are unable to protect our information systems against data corruption, cyber-based attacks or network security breaches, our operations could be disrupted.

...Security breaches of this infrastructure can create system disruptions, shutdowns or unauthorized disclosure of confidential information. If we are unable to prevent such breaches, our operations could be disrupted, or we may suffer financial damage or loss because of lost or misappropriated information.

...Security breaches in connection with the delivery of our products and services via ePORT, our Personal Solutions website, or well-publicized security breaches not involving the Internet that may affect us or our industry, such as database intrusion, could be detrimental to our reputation, business, operating results and financial condition. We cannot be certain that advances in criminal capabilities, new discoveries in the field of cryptography or other developments will not compromise or breach the technology protecting the networks that access our products, consumer services and proprietary database information.

See Equifax 2008 Form 10-K, at 20.

91. The Company's FY 2009, and FY 2010 10-Ks, filed with the SEC on February 23, 2010, February 23, 2011, respectively, all included a similar warning. *See* Equifax 2009 Form 10-K, at 20 and Equifax 2010 Form 10-K, at 16.

92. By the end of FY 2011, the warnings contained in the Company's annual report, filed with the SEC on February 23, 2012, were amended to reflect the Individual Defendants' awareness that the risk of failing to secure a significant amount of customer data was among the top risks facing Equifax and could cause its business and reputation to suffer, as follows:

Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.

...Despite our substantial investment in security measures and business continuity plans, our information technology networks and infrastructure may be vulnerable to damage, disruptions or shutdowns due to attacks by hackers or breaches due to employee error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. The occurrence of any of these events could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could result in legal claims or proceedings, liability or regulatory penalties under laws protecting the privacy of personal information, disrupt operations, and damage our reputation, which could adversely affect our business in lost sales, fines or lawsuits.

See Equifax 2011 Form 10-K, at 17. (Emphasis supplied).

93. By the end of FY 2012, the statements contained in the Company's annual report, filed with the SEC on February 22, 2013 once again were amended to state, in part, as follows:

Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.

... Although we are not aware of any material breach of our data, properties, networks or systems, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations.

See Equifax 2012 Form 10-K, at 17. (Emphasis supplied).

94. The Company's FY 2013, FY 2014, FY 2015, and FY 2016 10-Ks, filed with the SEC on February 28, 2014, February 25, 2015, February 24, 2016, and February 22, 2017, respectively, all included the aforementioned statement. *See* Equifax 2013 Form 10-K, at 16; Equifax 2014 Form 10-K, at 17; Equifax 2015 Form 10-K, at 17; and Equifax 2016 Form 10-K, at 16.

95. On March 25, 2016, Defendants Copeland, Daleo, Driver, Feidler, Humann, Marcus, Marshall, McKinley, Smith and Templeton caused Equifax to file with the SEC a Proxy Statement on Schedule 14A in connection with the 2016 Annual Meeting of Stockholders, held on May 4, 2016 (the "2016 Proxy"). In the

2016 Proxy, Defendants solicited stockholder votes to, among other things, re-elect Defendants Copeland, Daleo, Driver, Feidler, Humann, Marcus, Marshall, McKinley, Smith and Templeton. Defendants issued materially misleading statements with respect to the solicited votes, as follows:

Board Risk Oversight

Our Board oversees risk management at the Company. The Board exercises direct oversight of strategic risks to the Company and other risk areas not delegated to one of its committees.

On an annual basis, the Board performs an enterprise risk assessment with management to review the principal risks facing the Company and monitors the steps management is taking to map and mitigate these risks. The Board then sets the general level of risk appropriate for the Company through business strategy reviews. Risks are assessed throughout the business, focusing on (i) financial, operational and strategic risk, and (ii) ethical, legal, security, regulatory and other compliance risks.

Each business unit and corporate support unit has primary responsibility for assessing and mitigating risks within their respective areas of responsibility. Our CEO and senior leadership team receive comprehensive periodic reports on the most significant risks from these units and from the head of our internal audit department.

* * *

Audit Committee: Reviews risks related to financial reporting; discusses material violations, if any, of Company ethics, legal, regulatory and other compliance policies.

* * *

Governance Committee: Focuses on corporate governance risks, including evaluation of our leadership and risk oversight structure to ensure that it remains the optimal structure for our Company and shareholders.

Technology Committee: Focuses on technology-related risks and opportunities, including information security.

See 2016 Proxy Statement, at 20-21.

96. The 2016 Proxy claimed that: (i) the Board was effective in overseeing Equifax's risk management; (ii) the Audit Committee was effective in fulfilling its oversight responsibilities with respect to material violations of Company ethics, legal, regulatory and other compliance policies; (iii) the Governance Committee was effective in fulfilling its oversight responsibilities with respect to leadership and risk oversight structure; and (iv) the Technology Committee was effective in fulfilling its oversight responsibilities with respect to technology-related risks and information security. These statements were misleading because the 2016 Proxy omitted any disclosures reflecting or acknowledging the Defendants' failure to secure consumer data and the lack of internal controls necessary to prevent data breaches.

97. On March 24, 2017, Defendants Copeland, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton caused Equifax to file with the SEC a Proxy Statement on Schedule 14A in connection with the 2017 Annual Meeting of Stockholders, held on May 4, 2017 (the "2017 Proxy"). In the 2017 Proxy, Defendants solicited stockholder votes to, among other things, re-elect Defendants Daleo, Driver, Feidler, Hough, Humann,

Marcus, Marshall, McKinley, Smith, Stock and Templeton. Defendants issued materially misleading statements with respect to the solicited votes as follows:

Board Risk Oversight

Our Board oversees risk management at the Company. The Board exercises direct oversight of strategic risks to the Company and other risk areas not delegated to one of its committees.

* * *

Board of Directors: Monitors our “tone at the top” and risk culture and oversees emerging strategic risks. On an annual basis, the Board performs an enterprise risk assessment with management to review the principal risks facing the Company and monitors the steps management is taking to map and mitigate these risks. The Board then sets the general level of risk appropriate for the Company through business strategy reviews. Risks are assessed throughout the business, focusing on (i) financial, operational and strategic risk, and (ii) ethical, legal, privacy, data security (including cybersecurity), regulatory and other compliance risks.

* * *

Audit Committee: Reviews risks related to financial reporting; discusses material violations, if any, of Company ethics, legal, regulatory and other compliance policies.

* * *

Governance Committee: Focuses on corporate governance risks, including evaluation of our leadership and risk oversight structure to ensure that it remains the optimal structure for our Company and shareholders.

* * *

Technology Committee: Focuses on technology-related risks and opportunities, including data security.

See 2017 Proxy Statement, at 21.

98. The 2017 Proxy claimed that: (i) the Board was effective in overseeing Equifax's risk oversight; (ii) the Audit Committee was effective in fulfilling its oversight responsibilities with respect to material violations of Company ethics, legal, regulatory and other compliance policies; (iii) the Governance Committee was effective in fulfilling its oversight responsibilities with respect to leadership and risk oversight structure; and (iv) the Technology Committee was effective in fulfilling its oversight responsibilities with respect to technology-related risks and data security. These statements were misleading because the 2017 Proxy omitted any disclosures of the Defendants' failure to secure consumer data and the lack of internal controls necessary to prevent data breaches.

D. Reaction and Public Outcry Over Data Breaches

99. In the face of the disastrous Data Breach and Defendants' misleading statements as set forth above, pushback against Equifax and the Defendants was fierce.

100. On October 3, 2017, Mr. Smith went before the U.S. House of Representatives and was pressed on how a credit bureau of Equifax's size, responsible for safeguarding billions of sensitive records on Americans' financial lives, could have allowed so much data to escape, unnoticed. "How does this happen when so much is at stake?" asked Representative Greg Walden, Republican

of Oregon. “I don’t think we can pass a law that, excuse me for saying this, fixes stupid. I can’t fix stupid.”

101. During the hearing, on multiple occasions, Mr. Smith referred to an “individual” in Equifax’s technology department who had failed to heed security warnings and did not ensure the implementation of software fixes that would have prevented the breach. Equifax previously said that an unpatched software flaw had been to blame for the massive security breach, but on October 3, Mr. Smith went a step further, describing the “human error and technology failures” that turned a single oversight into a data breach that allowed attackers to obtain personal details on nearly half of America’s population.

102. In early March, the Department of Homeland Security sent Equifax and other companies an alert about a critical vulnerability in software that Equifax used in an online portal for recording customer disputes. Equifax sent out an internal email requesting the technical staff fix to the software, but, in effort to lay the blame at an anonymous doorstep, according to Smith, “an individual did not ensure communication got to the right person to manually patch the application.” This human error was compounded by a technical error: the scanning software that Equifax used to detect vulnerabilities failed to find the unpatched hole, he said.

103. In addition, Sen. Elizabeth Warren, D. Mass., forced former Equifax CEO Richard Smith to admit that the credit reporting agency profits from data breaches during the hearing. Warren quoted Smith’s previous description of fraud

as a “huge opportunity for us.” “Now, Mr. Smith, now that information for about 145 million Americans has been stolen, is fraud more likely now than before that hack?” Warren asked. “Yes, Senator, it is,” Smith replied. “So the breach of your system has actually created more business opportunities for you,” Warren said. The result, Warren said, was the Company would have little incentive to invest in security measures to protect consumers’ personal data.

104. Lawmakers also grilled Mr. Smith about the stock sales by Defendants Gamble, Loughran and Ploder, who sold shares worth almost \$1.8 million in the days after the breach was discovered, but before it was disclosed. The sales were approved by John J. Kelley III, Equifax’s chief legal officer, who knew at the time that the company’s technical department had detected suspicious activity on Equifax’s network. Smith, however, described them as “honorable men of integrity” who were unaware of the technical investigation.

E. Equifax Business Has Suffered as a Result of the Breach

105. As set forth above, as a result of the repeated data breaches, on or about October 12, 2017, Equifax lost a fraud prevention contract worth \$7.25 million with the IRS that it had received on September 29, 2017.

106. On October 17, 2017 the Government Accountability Office (“GAO”) rejected Equifax’s appeal of the loss of the contract to provide assistance in preventing identity theft. The GAO conducted a review and concluded that the IRS was justified in shifting the one-year agreement to Experian.

107. Indeed, as set forth on CNBC’s website on September 8, 2017, in an article titled, “Equifax shares plunge the most in 18 years as Street says breach will cost company hundreds of millions,” analysts predicted that the Data Breach will cost the Company hundreds of millions of dollars and “costs could drag on for a number of years[,]” as follows:

“Based on large scale breaches at Target and Home Depot, we [Stifel] believe \$300M-\$325M in gross costs for the breach would not be unreasonable[.]”

* * *

The “significant data breach is likely to cost the company materially, and costs could drag on for a number of years,” analyst Shlomo Rosenbaum [of Stifel] wrote in a note to clients Friday. “We aren’t changing estimates right now because of lack of clarity, **though clearly ours and consensus estimates are too high in the near term.**”

In similar fashion, SunTrust also focused on the negative impact to the company’s credibility with consumers.

“This is clearly a material event, in our opinion. **The breach compromises Equifax’s reputation as a trusted steward of consumer data, and will create a near-term business disruption,** per the company’s public comments,” analyst Andrew Jeffrey wrote in a note to clients Thursday.

(Emphases supplied).

108. On October 24, 2017, as reported on *BBC.com*, the United Kingdom’s Financial Conduct Authority (“FCA”) announced that it would investigate Equifax over the data breach. *BBC.com* reported that “[Equifax] originally believed that fewer than 400,000 British people were affected, but it has now put the figure at

694,000.” *BBC.com* further reported that, “Four groups of UK customers have so far been detailed by the firm: 637,000 whose phone numbers were stolen; 29,000 whose driving licence [sic] numbers were stolen; 15,000 who had some of their Equifax membership details, such as usernames and passwords, stolen; and 12,000 whose email addresses were stolen.”

109. On November 9, 2017, Equifax filed its Form 10-Q for the quarter ended September 30, 2017 (the “September 2017 10Q”). The *Business Insider* of November 11, 2017, set forth the damage to Equifax’s business as detailed in the September 2017 10Q. First, according to the *Business Insider*, “Equifax has no idea how deep the losses incurred by its massive data breach will run.”

110. The article stated that “Equifax doesn’t know how much it’ll cost. ... But it could be big — and ‘have an adverse effect on how we operate our business or our results of operations[,]” quoting the September 2017 10Q as follows:

It is not possible to estimate the amount of loss or range of possible loss, if any, that might result from adverse judgments, settlements, penalties or other resolution of the above described proceedings and investigations based on the early stage of these proceedings and investigations, that alleged damages have not been specified, the uncertainty as to the certification of a class or classes and the size of any certified class, as applicable, and the lack of resolution on significant factual and legal issues.

111. The September 2017 10Q further set forth that the Company could face unknown “Future Costs” associated with the “cybersecurity incident” beyond things like the judgements, penalties and fines, such as: “significant” legal and

other professional services expenses; increased expenses and capital investments for IT and security; increased expenses for insurance, finance, compliance activities, and to meet increased legal and regulatory requirements; and increased costs to provide free services to consumers including “increased customer support costs.”

112. Further, the September 2017 10Q set forth that there would be “other risk factors,” in addition to the legal risks, such as “Our remediation and security and IT enhancement efforts will be costly and may not be effective,” and the Data Breach “has had a negative impact on our reputation” and may have “a long-term effect on our relationships with our customers, our revenue and our business.” The September 2017 10Q also stated that all the lawsuits and investigations by governmental agencies and the courts could seriously adversely impact Equifax’s business:

The governmental agencies investigating the cybersecurity incident may seek to impose injunctive relief, consent decrees, or other civil or criminal penalties, which could, among other things, impact our ability to collect and use consumer information, materially increase our data security costs and/or otherwise require us to alter how we operate our business.

113. On November 27, 2017, Equifax faced a new lawsuit, as the Independent Community Bankers of America (“ICBA”) filed an action against the Company, demanding that Equifax compensate all community banks harmed by the data breach and to improve its security to avoid more damage.

VIII. THE DISCLOSURE OF THE DATA BREACHES WIPES OUT OVER 28.39% OF EQUIFAX'S MARKET CAPITALIZATION

A. Equifax Common Stock Price Declined Precipitously

114. As stated above, on September 7, 2017, Equifax disclosed the data breach. On this news, Equifax's market capitalization fell \$2.35 billion, a 13.68% drop, as Equifax's stock price went from \$142.72 per share on September 7, 2017 to \$123.23 per share on September 8, 2017. Indeed, as of September 15, 2017, Equifax's common stock traded as low as \$92.98 – approximately 35% below where the common stock was trading pre-announcement of the data breach. As of the filing of this Complaint, Equifax is trading at a price of approximately \$119 per share.

B. Equifax Subject to Numerous Lawsuits by Investors and Consumers

115. Federal, state and local government agencies, including the U.S. Department of Justice, the SEC and the U.S. Department of Labor, and state attorneys general and prosecutors' offices, as well as Congressional committees, have undertaken formal or informal inquiries, investigations or examinations arising out of the Company's most recent data breach announced by the Company on September 7, 2017.

116. Further, a number of lawsuits have also been filed by non-governmental parties seeking damages or other remedies related to the Company's

data breach. In fact, as of October 23, 2007, at least twenty-three class action cases have been filed.

IX. DAMAGES

117. As a result of the Individual Defendants' wrongful conduct, Equifax disseminated improper financial statements that misrepresented the Company's knowledge of the data breaches. These improper statements have devastated Equifax's credibility as reflected by the Company's more than 13.68% market capitalization loss following the acknowledgment of the data breach on September 7, 2017. Additionally, Equifax is now the subject of a securities class action alleging securities laws violations in connection with the improper financial reporting.

118. Further, Equifax's failure to timely alert its users of the data breaches violated numerous state laws. Equifax is now subject to consumer class actions that allege it violated these disclosure obligations and that the Company failed to take appropriate steps to keep its users' data safe. The Company will face substantial costs in connection with the consumer and securities class action lawsuits.

119. The Company is now subject to investigations by the SEC concerning the disclosure of the data breaches. Equifax will incur substantial costs in responding to these investigations.

120. Equifax will also likely lose users and the associated revenues from those users, as a result of the data breaches.

121. Equifax also paid substantial compensation to directors and officers that breached their fiduciary duty and violated federal securities laws. The retention of this payment by the Individual Defendants is unfair and unjust.

X. INSIDER SALES

122. Equifax has acknowledged that it discovered the unauthorized access on July 29, 2017, but it has failed to inform the public why it delayed notification of the Data Breach to consumers until September 7, 2017. Instead, Equifax executives took advantage of the delay and sold at least \$1.8 million worth of shares before the public disclosure of the breach as follows: Chief Financial Officer John Gamble sold shares worth \$946,374; Joseph Loughran, President of U.S. Information Solutions for Equifax, exercised options to dispose of stock worth \$584,099; and the Company's President of Workforce Solutions, Rodolfo Ploder, sold \$250,458 of stock on August 2, 2017.

123. On or about September 18, 2017, as reported in *Bloomberg News*, “[t]he U.S. Justice Department[‘s Atlanta office] has opened a criminal investigation into whether top officials at Equifax Inc. violated insider trading laws when they sold stock before the company disclosed that it had been hacked[.]” The news report stated that “[t]he SEC, in its preliminary probe, is looking into what executives knew and when about the data breach, according to the person familiar with that matter.” The DOJ’s investigation is ongoing.

124. As set forth below, Equifax's partisan and non-independent Special Committee (the "Special Committee") regarding this insider trading failed to explain but nevertheless purported to "clear" this insider trading.

125. Information regarding the Data Breach was material and nonpublic information until it was disclosed by Equifax on September 7, 2017. Defendants Gamble, Loughran and Ploder were aware of Equifax's history of data breaches. By virtue of their positions within Equifax, and Equifax's public statement that it "acted immediately to stop the intrusion and conduct a forensic review", Defendants Gamble, Loughran and Ploder were aware of the data breaches that had occurred between May and July 2017, just prior to their stock sales.

126. Defendants Gamble, Loughran and Ploder knew, recklessly disregarded, or should have known, that acting with knowledge of material and nonpublic information was a breach of a fiduciary duty to keep Inside Information confidential.

127. By virtue of the foregoing, Defendants, in connection with the purchase or sale of securities, by the use of the means or instrumentalities of interstate commerce, or of the mails, or a facility of a national securities exchange, directly or indirectly: (a) employed devices, schemes or artifices to defraud; (b) made untrue statements of material fact or omitted to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; or (c) engaged in acts, practices or courses

of business which operated or would have operated as a fraud or deceit upon persons.

128. Defendants thereby violated Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and SEC Rule 10b-5, 17 C.F.R. § 240.10b-5.

129. Plaintiff was an owner of Equifax stock contemporaneously with Defendants Gamble's, Loughran's and Ploder's sale of their Equifax stock.

XI. THE REPORT RELEASED BY THE SO-CALLED DISINTERESTED COMMITTEE INVESTIGATING INSIDER SALES WAS A SHAM

130. On November 3, 2017, Equifax's Board of Directors released a report by the Special Committee that set forth its purported conclusions concerning the insider trading detailed above. Unfortunately for Equifax and its shareholders, the report was led by interested Board members. As set forth in Equifax's November 3, 2017 press release that attached the report, "The Board formed the Special Committee in September to conduct an independent review of various aspects of the cybersecurity incident and the Company's response to it. The report released today relates exclusively to the securities trading matter."

131. The Special Committee was composed of Board members Daleo, Hough and Stock. Two of the three members of the Special Committee -- Daleo and Hough -- are not truly "independent" Directors.

132. As set forth above, Daleo has been on the Equifax Board of Directors since 2006. Daleo is the Chair of the Audit Committee and also serves on the

Compensation, Human Resources & Management Succession Committee and Executive Committee. In 2016, Daleo's total compensation from Equifax was \$260,996. Daleo was not truly independent.

133. As set forth above, Hough has been on the Equifax Board of Directors since 2016. Hough serves on the Audit Committee and Technology Committee. In 2016, Hough's total compensation from Equifax was \$199,474. Hough was not truly independent.

134. As set forth herein, as members of the Audit Committee, Defendants Daleo and Hough were responsible under the Audit Committee Charter in effect during the relevant period for reviewing and approving quarterly and annual financial statements and Equifax's internal controls, as described above. Despite these duties, Defendants Daleo and Hough, as part of the Audit Committee, knowingly or recklessly reviewed and approved improper financial statements. Defendants Daleo and Hough also reviewed and approved Equifax's ineffective internal controls. Accordingly, because Defendants Daleo and Hough face a sufficiently substantial likelihood of liability for breach of their fiduciary duty of loyalty as alleged herein and in other actions against them, they could not possibly be deemed "independent" evaluators of the guilt or innocence of the Insider Defendants.

135. Indeed, the DOJ's ongoing criminal investigation into whether the Insider Defendants violated insider trading laws is and will be a much more

independent determination of their guilt or innocence than that of the already-tainted Special Committee.

136. Furthermore, the findings of the Special Committee itself refute any claim that it was independent. The Special Committee concluded that Gamble “did not have any knowledge of the security incident when he sought preclearance to trade on July 31 or when he executed his cleared trades on August 1.” As set forth above, Gamble, at the time of his trades, had served as Equifax’s Chief Financial Officer since May 2014. It is barely credible that the Company’s CFO only learned of the security breach “on August 10, during a management offsite meeting,” when the Company discovered it on July 28, 2017, with the Company waiting *almost two weeks* to inform its CFO of such a potentially disastrous matter.

137. Similarly, the Special Committee concluded that “Mr. Loughran first learned, at a general level, that a security issue was being investigated in a series of texts, emails, and phone calls he exchanged with members of the Equifax Legal Department on August 13 and 15. Mr. Loughran learned details of the breach on August 22, when he attended the Senior Leadership Team meeting referenced above.”

138. However, it is hard to believe that a person with as much senior executive experience as Loughran was unaware for over two weeks of an event as cataclysmic as the discovery in late July of the massive security breach. At the

time of the discovery, Loughran was President of Equifax's United States Information Solutions (USIS) business – one of three major divisions of Equifax that is responsible, *inter alia*, for providing consumer and commercial information to U.S. businesses. Prior to this role, Loughran was Equifax's Chief Marketing Officer; President of Equifax's Global Consumer Solutions division; and was Senior Vice President, Corporate Development.

139. The Special Committee purportedly determined that Ploder “learned of the security incident on August 22, 2017, when he participated in the Senior Leadership Team meeting referenced above [at which Loughran purportedly learned the details of the breach].” As with Gamble and Loughran, it beggars belief that Ploder would not know for almost three weeks about the discovery of such a devastating event. Ploder, at the time of the discovery, was President of Equifax's Workforce Solutions division since November 2015. Not only is Workforce Solutions one of the three major divisions of Equifax, providing income and employment verification services to Equifax's clients, the data breach occurred at that very division's payroll-related and human resources management unit. It is simply not believable that the head of Workforce Solutions would not be informed immediately of such a major disaster as the data breach *in his own division*. Like Gamble and Loughran, Ploder held many important senior positions prior to being tapped to be President of the Workforce Solutions division: from April 2010 to

November 2015, he served as President, U.S. Information Solutions; and he served as President, International, from January 2007 to April 2010.

140. Daleo and Hough clearly were not “independent” directors sitting on the Special Committee, nor do the Special Committee’s findings indicate that they acted independently.

XII. DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

141. Plaintiff brings this action derivatively in the right and for the benefit of Equifax to redress injuries suffered, and to be suffered, by Equifax as a direct result of violations of the federal securities laws, breach of fiduciary duties, and unjust enrichment, as well as the aiding and abetting thereof, by the Individual Defendants. Equifax is named as a nominal Defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

142. Plaintiff will adequately and fairly represent the interests of Equifax in enforcing and prosecuting its rights.

143. Plaintiff was a stockholder of Equifax at the time of the wrongdoing complained of, has continuously been a stockholder, and is a current Equifax stockholder.

144. The current Board of Equifax consists of the following eleven Individual Defendants: Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton. Plaintiff has not made any demand on the

present Board to institute this action because such a demand would be a futile, wasteful, and useless act, as set forth below.

Demand Is Excused Because Defendants Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton Face a Substantial Likelihood of Liability for Their Misconduct

145. As alleged above, Individual Defendants Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton violated section 14(a) of the Exchange Act by at least negligently making the misstatements and omissions in the 2016 Proxy and 2017 Proxy. Accordingly, demand is excused because a majority of the Board faces a substantial likelihood of liability.

146. Individual Defendants Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton also breached their fiduciary duty of loyalty by making and allowing improper statements to be made in the Company's public statements, including its Annual and Quarterly Reports, and Proxy Statements. In addition, these Board members allowed the Company to delay announcing the data breaches, despite the Company's knowledge of it, exposing Equifax to massive liability in the consumer class actions. Accordingly, demand is futile.

147. As members of the Audit Committee, Defendants Templeton, Daleo, McKinley and Hough, were responsible under the Audit Committee Charter in effect during the relevant period for reviewing and approving quarterly and annual

financial statements and Equifax's internal controls, as described above. Despite these duties, the Audit Committee Defendants knowingly or recklessly reviewed and approved improper financial statements. The Audit Committee Defendants also reviewed and approved Equifax's ineffective internal controls. Accordingly, these Defendants face a sufficiently substantial likelihood of liability for breach of their fiduciary duty of loyalty. Demand upon these Defendants is futile.

148. Plaintiff has not made any demand on the other stockholders of Equifax to institute this action since such demand would be a futile and useless act for at least the following reasons:

(a) Equifax is a publicly held company with over 120 million shares outstanding and thousands of stockholders;

(b) making demand on such a number of stockholders would be impossible for Plaintiff who has no way of finding out the names, addresses, or phone numbers of stockholders; and

(c) making demand on all stockholders would force Plaintiff to incur excessive expenses, assuming all stockholders could be individually identified.

COUNT I

**Against Defendants Copeland, Daleo, Driver, Feidler,
Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock
and Templeton for Violation of Section 14(a) of the Exchange Act**

149. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

150. The section 14(a) Exchange Act claims alleged herein are based solely on negligence. They are not based on any allegation of reckless or knowing conduct by or on behalf of Director Defendants Copeland, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton. The section 14(a) Exchange Act claims alleged herein do not allege and do not sound in fraud. Plaintiff specifically disclaims any allegations of, reliance upon any allegation of, or reference to any allegation of fraud, scienter, or recklessness with regard to the non-fraud claims.

151. Director Defendants Copeland, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton negligently issued, caused to be issued, and participated in the issuance of materially misleading written statements to stockholders which were contained in the 2016 Proxy and 2017 Proxy.

152. The misleading information contained in the 2016 Proxy and 2017 Proxy were material to Equifax's stockholders in determining whether or not to elect Defendants Copeland, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock and Templeton. This information was also material to the integrity of these directors that were proposed for election to the

Board. The proxy solicitation process in connection with the 2016 Proxy and 2017 Proxy was an essential link in the re-election of nominees to the Board.

153. Plaintiff, on behalf of Equifax, thereby seeks relief for damages inflicted upon the Company based upon the misleading 2016 Proxy and 2017 Proxy.

154. Because of the false and misleading statements in the Preliminary Proxy, Plaintiff and the Company are threatened with irreparable harm.

COUNT II

Against the Individual Defendants for Violation of Section 20(a) of the Exchange Act

155. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

156. The Individual Defendants acted as controlling persons of within the meaning of section 20(a) of the Exchange Act as alleged herein. By virtue of their positions as officers and/or directors of Equifax and participation in and/or awareness of the Company's operations and/or intimate knowledge of the false statements contained in the Proxy filed with the SEC, they had the power to influence and control and did influence and control, directly or indirectly, the decision making of the Company, including the content and dissemination of the various statements which Plaintiff contends are false and misleading.

157. Each of the Individual Defendants was provided with or had unlimited access to copies of the 2016 Proxy and 2017 Proxy and other statements alleged by Plaintiff to be misleading prior to and/or shortly after these statements were issued and had the ability to prevent the issuance of the statements or cause the statements to be corrected.

158. In particular, each of the Individual Defendants had direct and supervisory involvement in the day-to-day operations of the Company, and, therefore, is presumed to have had the power to control or influence the particular transactions giving rise to the data breaches as alleged herein, and exercised the same. The 2016 Proxy and 2017 Proxy contain the unanimous recommendation of each of the Individual Defendants to the stockholders to vote in favor of the election of directors. They were, thus, directly involved in the making of these documents.

COUNT III

Against the Individual Defendants for Breach of Fiduciary Duties

159. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

160. The Individual Defendants owed and continue to owe Equifax fiduciary obligations. By reason of their fiduciary relationships, the Individual Defendants owed and continue to owe Equifax the highest obligation of due care, loyalty, and good faith.

161. The Individual Defendants, and each of them, violated and breached their fiduciary duties.

162. As a direct and proximate result of Defendants' failure to perform their fiduciary obligations, Equifax has sustained significant damages. As a result of the misconduct alleged herein, these Defendants are liable to the Company.

163. Plaintiff, on behalf of Equifax, has no adequate remedy at law.

COUNT IV

Against the Individual Defendants for Unjust Enrichment

164. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

165. By their wrongful acts and omissions, the Individual Defendants were unjustly enriched at the expense of and to the detriment of Equifax. The Individual Defendants were unjustly enriched as a result of the salaries, bonuses, and other forms of compensation they received while breaching their fiduciary duties owed to Equifax.

166. Plaintiff, as a stockholder and representative of Equifax, seeks restitution from these Defendants, and each of them, and seek an order of this Court disgorging all profits, benefits, and other compensation obtained by these defendants, and each of them, from their wrongful conduct and fiduciary breaches.

167. Plaintiff, on behalf of Equifax, has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests the following relief:

A. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' violation of securities law, breaches of fiduciary duties, and unjust enrichment;

B. Directing Equifax to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect Equifax and its stockholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for stockholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation and taking such other action as may be necessary to place before stockholders for a vote the following Corporate Governance Policies:

1. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater stockholder input into the policies and guidelines of the Board;
2. a provision to permit the stockholders of Equifax to nominate at least three candidates for election to the Board;
3. a provision requiring immediate disclosure to affected users in the event of a data breach; and

4. a proposal to strengthen Equifax's internal controls over securing consumer and business information within its control.

C. Extraordinary equitable and/or injunctive relief as permitted by law, equity, and State statutory provisions sued hereunder, including attaching, impounding, imposing a constructive trust on, or otherwise restricting Defendants' assets so as to assure that Plaintiff, on behalf of Equifax, have an effective remedy;

D. Awarding to Equifax restitution from the Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Defendants;

E. Awarding to Plaintiff reasonable attorneys' fees, consultant and expert fees, costs, and expenses; and

F. Granting such other and further relief as the Court deems just and proper.

**COHEN COOPER ESTEP & ALLEN
LLC**

By: /s/Steven J. Estep
Steven J. Estep
Georgia Bar No. 250450
sestep@ccealaw.com
Jefferson M. Allen
Georgia Bar No. 010898
Jallen@ccealaw.com

3330 Cumberland Boulevard
Suite 600
Atlanta, Georgia 30339

Telephone: (404) 814-0000
Facsimile: (404) 816-8900

**HACH ROSE SCHIRRIPA
& CHEVERIE LLP**

Frank R. Schirripa

Daniel B. Rehns

112 Madison Avenue, 10th Floor

New York, New York 10016

Telephone: (212) 213-8311

Counsel for Plaintiff and the Class

February 6, 2018

**UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF GEORGIA**

**TEAMSTERS LOCAL 443 HEALTH
SERVICES & INSURANCE PLAN, on
behalf of herself and all others similarly
situated,**

Plaintiff,

-against-

**John W. Gamble, Jr., Joseph M.
Loughran, III, Rodolfo O. Ploder,
Richard F. Smith, James E. Copeland,
Jr., Robert D. Daleo, Walter W. Driver,
Jr., Mark L. Feidler, G. Thomas Hough,
L. Phillip Humann, Robert D. Marcus,
Siri S. Marshall, John A. McKinley,
Elane B. Stock and Mark B. Templeton,**

Defendants,

and,

Equifax, Inc.,

Nominal Defendant,

Case No.


**VERIFIED SHAREHOLDER
DERIVATIVE COMPLAINT**

VERIFICATION AND AFFIDAVIT OF SALVATORE J. ABATE

1. My name is Salvatore J. Abate, I am the Labor Co-Chairman for the Teamsters Local 443 Health Services & Insurance Plan. I am authorized to act on its behalf in this matter, and being duly sworn, deposes and says:

2. I verify that I have reviewed the Verified Shareholder Derivative Complaint (the "Complaint") to be filed in this action and that the facts stated in the Complaint, as they concern my own acts and deeds, are true to my personal knowledge. I believe the facts pleaded in the Complaint on information and belief or investigation of counsel are true.

3. I have not received, been promised or offered and will not accept any form of compensation, directly or indirectly, for prosecuting this action or serving as a representative party in this action except (i) such fees, costs or other payments as the Court expressly approves to be paid to me or on my behalf, or (ii) reimbursement, by my attorneys, of actual and reasonable out-of-pocket expenditures incurred directly in connection with the prosecution of this action.

By: 
Salvatore J. Abate
Labor Co-Chairman
Teamsters Local 443 Health Services &
Insurance Plan

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

TEAMSTERS LOCAL 443 HEALTH SERVICES & INSURANCE PLAN, on behalf of itself and all others similarly situated,

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF New Haven Co., CT
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

JOHN W. GAMBLE, JR., JOSEPH M. LOUGHRAN, III, RODOLFO O. PLODER, RICHARD F. SMITH, JAMES E. COPELAND, JR., ROBERT D. DALEO, WALTER W. DRIVER, JR., MARK L. FEIDLER, G. THOMAS HOUGH, L. PHILLIP HUMANN, ROBERT D. MARCUS, SIRI S. MARSHALL, JOHN A. MCKINLEY, ELANE B. STOCK, MARK B. TEMPLETON, and nominal Defendant Equifax Inc.

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Steven J. Estep and Jefferson M. Allen
Cohen Cooper Estep & Allen, LLC
3300 Cumberland Blvd SE Suite 600
Atlanta, GA 30339 (404) 814-000
sestep@ccealaw.com, jallen@ccealaw.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF
- 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- 2 U.S. GOVERNMENT DEFENDANT
- 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

- | | | | | | |
|----------------------------|----------------------------|---|----------------------------|----------------------------|---|
| PLF | DEF | | PLF | DEF | |
| <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | CITIZEN OF THIS STATE | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 | INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | CITIZEN OF ANOTHER STATE | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 | INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | CITIZEN OR SUBJECT OF A FOREIGN COUNTRY | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 | FOREIGN NATION |

IV. ORIGIN (PLACE AN "X" IN ONE BOX ONLY)

- 1 ORIGINAL PROCEEDING
- 2 REMOVED FROM STATE COURT
- 3 REMANDED FROM APPELLATE COURT
- 4 REINSTATED OR REOPENED
- 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- 6 MULTIDISTRICT LITIGATION - TRANSFER
- 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Sections 14(a) and 20(a) of the Securities and Exchange Act of 1934, and SEC Rule 14a-9. This is a shareholder derivative case against certain directors and officers of nominal defendant Equifax, Inc., for their various breaches related to a massive cyberattack that compromised the private financial and other information of almost half of the American population.

(IF COMPLEX, CHECK REASON BELOW)

- 1. Unusually large number of parties.
- 2. Unusually large number of claims or defenses.
- 3. Factual issues are exceptionally complex
- 4. Greater than normal volume of evidence.
- 5. Extended discovery period is needed.
- 6. Problems locating or preserving evidence
- 7. Pending parallel investigations or actions by government.
- 8. Multiple use of experts.
- 9. Need for discovery outside United States boundaries.
- 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT# _____ AMOUNT \$ _____ APPLYING IFP _____ MAG. JUDGE (IFP) _____
JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK

- 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK

- 110 INSURANCE
- 120 MARINE
- 130 MILLER ACT
- 140 NEGOTIABLE INSTRUMENT
- 151 MEDICARE ACT
- 160 STOCKHOLDERS' SUITS
- 190 OTHER CONTRACT
- 195 CONTRACT PRODUCT LIABILITY
- 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 210 LAND CONDEMNATION
- 220 FORECLOSURE
- 230 RENT LEASE & EJECTMENT
- 240 TORTS TO LAND
- 245 TORT PRODUCT LIABILITY
- 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK

- 310 AIRPLANE
- 315 AIRPLANE PRODUCT LIABILITY
- 320 ASSAULT, LIBEL & SLANDER
- 330 FEDERAL EMPLOYERS' LIABILITY
- 340 MARINE
- 345 MARINE PRODUCT LIABILITY
- 350 MOTOR VEHICLE
- 355 MOTOR VEHICLE PRODUCT LIABILITY
- 360 OTHER PERSONAL INJURY
- 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- 365 PERSONAL INJURY - PRODUCT LIABILITY
- 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 370 OTHER FRAUD
- 371 TRUTH IN LENDING
- 380 OTHER PERSONAL PROPERTY DAMAGE
- 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- 422 APPEAL 28 USC 158
- 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK

- 440 OTHER CIVIL RIGHTS
- 441 VOTING
- 442 EMPLOYMENT
- 443 HOUSING/ ACCOMMODATIONS
- 445 AMERICANS with DISABILITIES - Employment
- 446 AMERICANS with DISABILITIES - Other
- 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- 462 NATURALIZATION APPLICATION
- 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK

- 463 HABEAS CORPUS- Alien Detainee
- 510 MOTIONS TO VACATE SENTENCE
- 530 HABEAS CORPUS
- 535 HABEAS CORPUS DEATH PENALTY
- 540 MANDAMUS & OTHER
- 550 CIVIL RIGHTS - Filed Pro se
- 555 PRISON CONDITION(S) - Filed Pro se
- 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK

- 550 CIVIL RIGHTS - Filed by Counsel
- 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK

- 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK

- 710 FAIR LABOR STANDARDS ACT
- 720 LABOR/MGMT. RELATIONS
- 740 RAILWAY LABOR ACT
- 751 FAMILY and MEDICAL LEAVE ACT
- 790 OTHER LABOR LITIGATION
- 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- 820 COPYRIGHTS
- 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- 830 PATENT
- 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - s/k/h Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK

- 861 HIA (1395ff)
- 862 BLACK LUNG (923)
- 863 DIWC (405(g))
- 863 DIWW (405(g))
- 864 SSDI TITLE XVI
- 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK

- 870 TAXES (U.S. Plaintiff or Defendant)
- 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK

- 375 FALSE CLAIMS ACT
- 376 Qui Tam 31 USC 3729(a)
- 400 STATE REAPPORTIONMENT
- 430 BANKS AND BANKING
- 450 COMMERCE/ICC RATES/ETC.
- 460 DEPORTATION
- 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- 480 CONSUMER CREDIT
- 490 CABLE/SATELLITE TV
- 890 OTHER STATUTORY ACTIONS
- 891 AGRICULTURAL ACTS
- 893 ENVIRONMENTAL MATTERS
- 895 FREEDOM OF INFORMATION ACT
- 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK

- 410 ANTI-TRUST
- 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK

- 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

- CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND \$ _____
- JURY DEMAND YES NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE 44 cases filed, numerous judges DOCKET NO. _____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- 1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.
- 5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.
- 6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):

- 7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. 1:17-cr-04402, WHICH WAS DISMISSED. This case IS IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.

MHC

SIGNATURE OF A ATTORNEY OF RECORD

DATE

2/6/18

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Equifax, Executives Hit with Shareholder Class Action Over Data Breach](#)
